Ius Laboris

Global Human Resources Lawyers

Social Media Guide

A Ius Laboris Publication

Printed: *February 2012*

Nothing stated in this book should be treated as an authoritative statement of the law on any particular aspect or in any specific case. Action should not be taken on the basis of this text alone. For specific advice on any matter you should consult the relevant country representative listed inside. The law is stated as at November 2011.

Is a registered trademark of Ius Laboris scrl

Global
Human
Resources
Lawyers

Social Media Guide

Ius Laboris

Ius Laboris is an alliance of leading Human Resources law practitioners. With more than 2,500 locally qualified lawyers in over 40 countries, the Alliance is able to provide deep local Human Resources law knowledge on a global scale to help clients operating at home or abroad.

Even in an international context, Human Resources law remains steadfastly local. Your employment issues are global, but the solutions will need to be adapted to the local market. Ius Laboris is the only alliance that can provide you with local legal expertise to solve your Human Resources issues on a global scale.

The Human Resources law expertise and experience of Ius Laboris member firms is impressive. Our member firms are consistently ranked among their country's best. Each of our members must be a top-ranking Human Resources or Pensions law firm in their respective locality to be invited to join Ius Laboris. We welcome into our Alliance only firms that possess focused expertise in all disciplines of labour, employment and pensions law. Our lawyers understand the issues and challenges associated with managing a workforce, wherever it is located.

To help you navigate complex Human Resources law issues wherever you operate, our lawyers collaborate closely together. International Practice Groups (IPGs) have been created to further the skill and know-how of our lawyers and to share specific knowledge with clients. The IPGs bring together lawyers from across the Alliance with expertise in key areas of Human Resources law including Data Privacy, Discrimination, Employee Benefits and Tax, Global Mobility, Individual Employment Rights, Occupational Health and Safety, Pensions and Restructuring.

Our IPGs meet regularly and are well placed to coordinate regional and worldwide requests, drawing on each individual lawyer's wealth of experience. Clients using our services will benefit from the ongoing exchange of expertise and knowledge that occurs between members of the Alliance in the IPGs.

For additional information, please visit our website (www.iuslaboris.com) or feel free to contact us:

Ius Laboris

280 Boulevard du Souverain
1160 Brussels
Belgium
T +32 2 761 46 10
F +32 2 761 46 15
E info@iuslaboris.com

Contributors

AUSTRIA
Birgit Vogt-Majarek
Maria Schedle
Kunz Schima Wallentin
Porzellangasse 4
1090 Vienna
Austria
T +43 1 313 74 0
F +43 1 313 74 80
E birgit.vogt@ksw.at
maria.schedle@ksw.at
www.ksw.at

BELGIUM
Nicholas Thoelen
Claeys & Engels
Generaal Lemanstraat 74
2600 Antwerp
Belgium
T +32 3 285 97 83
F +32 3 285 97 90
E nicholas.thoelen@claeysengels.be
www.claeysengels.be

CANADA
Adam Kardash
Bridget McIlveen
Rhonda Shirreff
Heenan Blaikie LLP
Bay Adelaide Centre
P.O. Box 2900
333 Bay Street, Suite 2900
Toronto ON
M5H 2T4
Canada
T +1 416 360 6336
F +1 416 360 8425
E akardash@heenan.ca
bmcilveen@heenan.ca
rshirreff@heenan.ca
www.heenan.ca

COLOMBIA
Ángela Cubides Antolínez
Juan Gilberto Sánchez Cure
Brigard & Urrutia
Calle 70 A No. 4-41
Bogotá
Colombia
T +571 346 2011
F +571 310 0609
E acubides@bu.com.co
jsanchezc@bu.com.co
www.bu.com.co

CYPRUS
George Z Georgiou
Anna Praxitelous
George Z Georgiou & Associates LLC
1 Eras Street, 1st Floor
1060 Nicosia
Cyprus
T +357 22 76 33 40
F +357 22 76 33 43
E george@gzg.com.cy
anna.praxitelous@gzg.com.cy
www.gzg.com.cy

DENMARK
Elsebeth Aaes-Jørgensen
Norrbom Vinding
Amerikakaj
Dampfaergevej 26
2100 Copenhagen
Denmark
T +45 35 25 39 40
F +45 35 25 39 50
E eaj@norrbomvinding.com
www.norrbomvinding.com

ESTONIA
Arne Ots
Ants Nomper
Raidla Lejins & Norcous
Roosikrantsi 2
10119 Tallinn
Estonia
T +372 640 7170
F +372 640 7171
E arne.ots@rln.ee
ants.nomper@rln.ee
www.rln.ee

FRANCE
Anne-Laure Peries
Capstan
1300 avenue Albert Einstein
Stratégie Concept Bât. 4
34000 Montpellier
France
T +33 04 67 15 90 97
F +33 04 67 15 90 91
E alperies@capstan.fr
www.capstan.fr

GERMANY
Jessica Jacobi
Kliemt & Vollstädt
Monbijouplatz 10A
10178 Berlin
Germany
T +49 30 887154 14
F +49 30 887154 20
E jessica.jacobi@kliemt.de
www.kliemt.de

GREECE
Alexia Stratou
Kremalis Law Firm
35 Kyrillou Loukareos
114 75 Athens
Greece
T +30 210 64 31 387
F +30 210 64 60 313
E astratou@kremalis.gr
www.kremalis.gr

INDIA
Manishi Pathak
Kochhar & Co
11th Floor, Tower A, DLF Towers
Jasola
Jasola District Center
New Delhi – 110025
India
T +91 11 4111 5222
F +91 11 4056 3813
E manishi.pathak@kochhar.com
www.kochhar.com

IRELAND
Deirdre Kilroy
LK Shields Solicitors
39/40 Upper Mount Street
Dublin 2
Ireland
T +353 1 661 0866
F +353 1 661 0883
E dkilroy@lkshields.ie
www.lkshields.ie

ITALY
Paola Pucci
Toffoletto De Luca Tamajo e Soci
Via Rovello, 12
20121 Milan
Italy
T +39 02 721 44 1
F +39 02 721 44 500
E spp@toffolettodeluca.it
www.toffolettodeluca.it

LUXEMBOURG
Ariane Claverie
Castegnaro
33 Allée Scheffer
2520 Luxembourg
Luxembourg
T +352 26 86 82 1
F +352 26 86 82 82
E ariane.claverie@castegnaro.lu
www.castegnaro.lu

MEXICO
Rosa Maria Franco
Oscar Arias
Monica Schiaffino
Basham, Ringe y Correa SC
Paseo de los Tamarindos No 400
9th Floor
Bosques de las Lomas 05120
Mexico DF
Mexico
T +52 55 52 61 0400
F +52 55 52 61 0496
E rfranco@basham.com.mx
oarias@basham.com.mx
mschiaffino@basham.com.mx
www.basham.com.mx

NETHERLANDS
Philip Nabben
Tom Mooyaart
Bronsgeest Deur Advocaten
De Lairessestraat 137-143
1075 HJ Amsterdam
Netherlands
T +31 20 305 33 33
F +31 20 305 33 30
E p.nabben@bd-advocaten.nl
t.mooyaart@bd-advocaten.nl
www.bd-advocaten.nl

NORWAY
Claude A Lenth
Advokatfirmaet Hjort DA
Akersgaten 51
P.O.Box 471 Sentrum
0105 Oslo
Norway
T +47 22 47 18 00
F +47 22 47 18 18
E cal@hjort.no
www.hjort.no

PERU
Manuel Bartra
Jose Antonio Valdez
Estudio Olaechea
Bernardo Monteagudo 201
San Isidro
Lima 27
Peru
T +51 1 219 0400
F +51 1 219 0420
E manuelbartra@esola.com.pe
joseantoniovaldez@esola.com.pe
www.esola.com.pe

POLAND
Magdalena Zwolinska
Raczkowski i Wspólnicy sp.k.
ul. Ciasna 6
00-232 Warsaw
Poland
T +48 22 531 52 86
F +48 22 531 52 81
E magdalena.zwolinska@raczkowski.eu
www.raczkowski.eu

PORTUGAL
Bruno Barbosa
Pedro Pinto, Bessa Monteiro, Reis,
Branco & Associados, RL (pbbr)
Av. da Liberdade, nº 110 – 6º
1250 - 146 Lisbon
Portugal
T +351 21 326 47 47
F +351 21 326 47 57
E bruno.barbosa@pbbr.pt
www.pbbr.pt

RUSSIA
Irina Anyukhina
Law Firm ALRUD
2nd floor – 17 Skakovaya Street
125040 Moscow
Russia
T +7 495 234 96 92
F +7 495 956 37 18
E ianyukhina@alrud.ru
www.alrud.com

SPAIN
Fernando Valdés-Hevia
Montserrat Alonso
Sagardoy Abogados
C/Tutor 27
28008 Madrid
Spain
T +34 915 429 040
F +34 915 422 657
E fvh@sagardoy.com
map@sagardoy.com
www.sagardoy.com

SWITZERLAND
Vanessa Rossel
Lenz & Staehelin
Route de Chêne 30
1211 Geneva 17
Switzerland
T +41 58 450 70 00
F +41 58 450 70 01
E vanessa.rossel@lenzstaehelin.com.
www.lenzstaehelin.com

UNITED KINGDOM
Ellen Temperton
Lewis Silkin LLP
5 Chancery Lane
Clifford's Inn
London EC4A 1BL
England
T +44 20 7074 8424
F +44 20 7864 1728
E ellen.temperton@lewissilkin.com
www.lewissilkin.com

USA
Philip Gordon
Littler Mendelson PC
One Tabor Center
1200 17th Street
Suite 1000
Denver CO 80202-5835
USA
T +303 362 2858
F +303 362 8103
E pgordon@littler.com
www.littler.com

EDITOR
Deborah Ishihara
Ishihara & Co Ltd
writing – editing – proof reading
London
England
T +44 20 8549 2772
F +44 20 8549 5455
E deborah@ishihara.co.uk

Contents

Introduction

In the past several years, social media use has grown across the globe at an unprecedented rate, involving hundreds of millions of users of all ages. Because of its worldwide prevalence (more than 800 million users worldwide), Facebook's market penetration provides one means for assessing the relative popularity of social media across the countries covered by this Guide. That market penetration varies significantly as reflected by the following figures: 2.5% in India, approximately 25% in Germany and Mexico, 35% in Belgium, 42% in the United States, 47% in Denmark, and 72% in Colombia. Given these figures, there can be no question that in each of the surveyed countries millions of job applicants and employees use social media.

The meteoric rise of social media raises a range of benefits and challenges for employers across the globe. In the recruitment process, social media facilitate the identification of potential new hires and the collection of information pertinent to the hiring decision. At the same time, social media reveal information about applicants that typically would not become available through more traditional hiring processes. For current employees, social media often provide an efficient means for connecting with customers and prospective customers. However, employees' social media activity can also undermine productivity, expose employers to liability, and damage a company's reputation.

We have prepared this Guide to provide employers, particularly those with multi-national operations, with a basic understanding of the legal framework in 25 countries, affecting an employer's ability to collect information about applicants and employees from social media, to monitor employees' use of social media, and to use information obtained through those efforts to make employment-related decisions. For each country surveyed, the Guide provides information on six subject areas that are critical for employers trying to navigate the intersection of social media and the workplace:

1. Use by Employees: Survey results on the popularity of social media among employees
2. Use by Employers: Survey results on employers' use of social media for marketing purposes and/or for recruiting and case law addressing employers' use of social media for employment purposes

3. Employer Access: Legal restrictions on employers' collection of information posted on social media sites, whether by employees or by third parties about employees
4. Private and Public Information: The legal implications for employers of an employees' decision to post information on a publicly available social media site or on a site with restricted access
5. Consent and Works Council Rights: The circumstances in which employers are and are not required to obtain consent to review social media information and the degree, if any, to which works councils must be involved before an employer can process employees' social media content
6. Data Protection Officers: The role, if any, that internal data protection officers play in an employers' collection and use of employees' social media content for employment purposes

Given the newness of social media, the legal landscape in most of the surveyed countries is almost bare of any guidance specific to social media. None of the surveyed countries, for example, has yet enacted legislation specifically addressing the use of social media for employment purposes. In addition, the surveyed countries have no, or very few, judicial decisions specifically addressing use of social media in the employment context.

This lack of guidance specific to social media does not mean that employers must navigate wholly uncharted waters. As reflected in this Guide, existing laws governing privacy, data protection, and labour relations can be consulted to provide employers with meaningful guidance on how to lawfully collect, monitor, and use employees' social media content. Not surprisingly, these laws can vary significantly across jurisdictions, either in fundamental ways or in their nuances, making it particularly challenging for multi-national employers to adopt social media policies that are uniform across the globe.

Notwithstanding these variations, the Guide does reflect a high level of consistency across the surveyed countries in terms of certain guidelines employers should consider when developing national or multi-national policies addressing the use of social media for employment purposes. These guidelines include the following:

- Employers are generally required to provide notice and/or obtain consent before collecting and using social media information in the background checking process.
- Restrictions on the use of certain categories of information for employment purposes (e.g. race or ethnic origin, disability and genetic composition) apply to information collected through social media.

- Employers potentially face liability for bypassing user-created restrictions on access to social media content, such as a 'friends only' Facebook page, especially if they use false pretenses or coercion to gain such access.
- Information posted on publicly available social media sites typically receives no, or limited, protection under privacy laws but generally continues to fall within the scope of data protection laws and protections against unlawful employment practices.
- Employers generally have significant latitude to take disciplinary action based on an employee's social media activity using the employer's electronic resources during work hours, provided that the employer has implemented a legally compliant electronic monitoring policy.
- Employers in virtually all surveyed countries should be cautious about taking adverse employment action based on an employee's off-duty social media activity using personal electronic resources.

While these general guidelines provide broad parameters for addressing social media in the workplace, employers still should carefully analyse the law in each country where it has employees, for local variations.

Jessica Jacobi (Kliemt & Vollstädt, Germany)
Philip Gordon (Littler Mendelson PC, USA)
Co-Chairs of the Data Privacy IPG

Austria

1. General use of social media sites

1.1 Popularity of social media sites

Facebook is the most popular social networking site, with more than 2.6 million users (Source: Wikipedia). Other popular sites are Twitter with 39,384 accounts (47% of which are active), MySpace, netlog, StudiVZ and Szene1.at (Source: Facebook Ad Planner 21 February 2011) The most popular business network in Austria is Xing. Most users are between 20 and 29 years old. Male users form 51% and female users 49%.

2. Use by employers

2.1 Use of information from social media by employers

There is no specific statistical material available that shows the extent to which employers use these media as a source of information about future or current employees. A survey made by the Austrian Chamber of Commerce in January 2011 showed that 48% of Austrian companies use social media (this was up from 39% in 2010). Facebook, Twitter and Xing are the social networking sites most used by employers. According to this survey 77% reported that they use social networking sites to promote their image. Other objectives according to this survey are the acquisition of new customers and supplier searches, but 23.6% reported that using social media has a positive effect on the recruitment process.

2.2 Case law about use of information from social media by employers

As far as we are aware there is no case law about the use of information from social media by employers.

However, there is doctrine concerning the use of the Internet and emails for private purposes by employees, according to which, if private use of the Internet is permitted, the employer is only entitled to control its use by employees in special circumstances, for example, if the employee is in breach of his or her duties or in breach of the law in general.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

There is no specific applicable law or case law concerning the use of online information by employers, however, the following law applies: the Data

Protection Act (Datenschutzgesetz, 'DSG'); section 16 of the General Civil Code (Allgemeines Bürgerliches Gesetzbuch, 'ABGB'); and the duty of care of the employer to protect the employee against monitoring and selective searching by the employer on social networking sites. According to section 1 of the DSG, where an individual has a legitimate interest in keeping his or her personal data confidential, there is a right that it should be kept confidential.

If an applicant's profile is only accessible to 'friends' the employer is generally not allowed to collect these data.

In general terms, the employer is entitled to collect personal data from social networking sites that are generally accessible, i.e. that can be found via search engines such as Google. However, if these data concern questions which may not be asked by the employer during an interview the employer is not entitled to access such information. This could include questions concerning the financial circumstances of the employee; the employee's political opinions; religious beliefs; sexual life; physical or mental health or condition and they can only be asked if it is in the employer's legitimate interests to do so.

In general the collection of personal data from social networking sites by the employer is only justified if the employer's interests outweigh the interests of the employee. If an employee uses leisure-oriented social networking sites during his or her free time, monitoring of the employee may only be justified if the employee breaches his or her duties. This is because in general, the employer is not permitted to control the behaviour of its employees during their free time. If an employee is utilising employer-owed equipment or networks during working hours the employer's interests will usually outweigh the interests of the employee, especially if the employee uses professionally oriented social media, such as Xing. According to a court decision the employer is permitted to monitor its employees using a detective if the employer has a reasonable suspicion that he or she is in breach of his or her duties.

4. Private and public information

4.1 Treatment of private and public information

A person who posts information on social networking sites considered to be publicly available cannot claim the fundamental right to data protection because the data are public (i.e. generally available). However the right of the employer to collect such information is restricted by the duty of care of the employer and by the principles of data use as specified by the DSG. In particular, data may only be processed for defined, clear and lawful purposes and must not be used in a way which is incompatible with these purposes. Data may only be used inasmuch as they are relevant to the purpose of the processing and do not go beyond this purpose. Data may only be used in a way which preserves their accuracy and, if necessary, they must be updated in accordance with the purpose for which they are being used (see section 3.1 above).

As yet, there is no distinction in law between business and private webpages under Austrian law.

The employee's interest in keeping his or her information private will usually outweigh the interests of the employer. Therefore the employer is not permitted to collect this information and cannot rely on it.

5. Consent and works council rights

5.1 Consent

As far as we are aware, there is no case law concerning whether the posting of private information is considered to constitute consent. Whether the information can be used by employers depends on the balance between the interests of the employer in receiving it and the interests of the employee or future employee in keeping the information confidential.

5.2 Works council rights

The works council may ask the employer for all information that is relevant to vacant positions, but the employer is not required to consult the works council before using social media.

6. Sanctions

6.1 Regulatory authority and sanctions

The Data Protection Act provides for administrative as well as penal sanctions. The administrative sanctions are imposed by the regional administrative authority and the criminal ones by the District Court.

Claims for compensation (in the form of material and immaterial damages) for breaches of the DSG are also possible.

Data controllers who breach data secrecy or refuse to comply with a decision of the Data Protection Commission (Datenschutzkommission) may be liable to a fine. The Data Protection Act provides a fine of up to EUR 25,000, for deliberate or unlawful access to a data application, deliberate breach of data secrecy, or when data are used, not disclosed, not corrected or not deleted in contravention of a legally effective judgment or decision, or if data are deliberately not deleted. A fine of up to EUR 10,000 is provided for non-fulfilment of the reporting obligation, data transmission to another country without the approval of the Data Protection Commission, breach of disclosure or information duties or gross failure to observe security measures.

The use of protected data with the intention of causing damage and making a profit can lead to imprisonment for up to one year.

6.2 How often sanctions are imposed

The sanctions are very infrequently imposed in practice.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are not required by law to appoint a data protection officer, but it is common for larger companies to appoint an employee to take organisational and technical measures in relation to data security and data protection.

Belgium

1. General use of social media sites

1.1 Popularity of social media sites

It is estimated that around 3,850,000 people in Belgium have a Facebook account, which is the equivalent of roughly 35% of the Belgian population. Other sites such as LinkedIn, Twitter and MySpace do not disclose statistics about the number of Belgian subscribers. Yet, according to some sources, LinkedIn has around 530,000 Belgian profiles.

2. Use by employers

2.1 Use of information from social media by employers

Reliable statistics are difficult to find. To our knowledge, no organisation tracks the frequency of usage of social media by employers to monitor future or current employees. According to some sources, 35% of all employers use social media to monitor applicants for employment.

2.2 Case law about use of information from social media by employers

Case law and legal literature concerning the use of information from social media by employers are still rare. They have, however, begun to develop somewhat since 2010.

There was, for example, one case where an employer dismissed an employee for cause because the employee had started an open Facebook group in which he insulted colleagues and the company's management quite aggressively. Although the Labour Court considered that the Facebook group was potentially accessible by all Internet users, it did not accept the dismissal on the basis of the circumstances of the case (e.g. the employee did not know the Facebook group was public; the number of people aware of the group was limited; and the remarks lacked respect but were not too overtly insulting).

In another case the Labour Tribunal made a different decision. This case concerned the manager of a public company that had criticised the company and its management on his Facebook profile immediately after the company had published quite negative yearly results. The Labour Tribunal judged that this employee had been fairly dismissed for cause, taking into account his managerial position, the damage to the company and the timing of the Facebook posts. As the employee's Facebook profile was not private but publicly available, the Labour Tribunal judged that there was no invasion of the employee's privacy.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

There is no specific legislation allowing employers to access and use information obtained via social media.

An employer must respect the privacy of both applicants for employment and its employees. As such, for example, the law states that during the recruitment process, the employer must respect the candidates' privacy and can only collect information that is relevant to the job. Most information available on social media is not considered relevant.

Further, a distinction must be made between monitoring the use of social media during working hours and outside working hours. When monitoring use of internet during working hours, an employer must respect a specific procedure (involving the works council or the union delegation and the need to establish a computer usage policy). That procedure does not apply when an employer monitors the way its employees use social media outside working hours. In the latter case, a balance must be found between an employee's privacy on the one hand and the right of an employer to protect the company from online misconduct on the other. Some companies are beginning to adopt policies concerning the use of social media by employees during their private time (outside working hours).

4. Private and public information

4.1 Treatment of private and public information

There is only very limited case law on whether private information posted on social networking sites is considered to be publicly available, but this will depend on the circumstances or the source of the information. If, for example, the information is posted on a secure website or is only made available to 'friends', it is likely that the information will not be considered to be publicly available.

However, if an employee voluntarily posts information and photos on a non-secured Facebook group or public profile, there is case law to the effect that this information will be considered publicly available and not protected by any right to privacy.

The law does not make a distinction between business webpages and private webpages. We would assume, however, that an individual's expectation of privacy is lower in the case of business webpages, employer-sponsored webpages or blogs than in the case of private webpages.

The law does not make a distinction between information found on search engines and information available to 'friends'. However, we expect that case law will make that distinction.

There is no information as yet about whether data collected by employers from posts by third parties can be used, but it would be risky for an employer to use such information because it may be inaccurate or unreliable.

5. Consent and works council rights

5.1 Consent

In terms of whether the posting of private information is considered to be consent for employers to use the information, case law has decided that by voluntarily posting private information or photos and making them publicly available, the information is no longer private.

5.2 Works council rights

The employer is not required to consult with the works council before using social media posts or content in the recruitment process.

6. Sanctions

6.1 Regulatory authority and sanctions

The most common enforcement tool against an employer that violates privacy protections for an employee's social media activity is a private action brought by the employee against the employer seeking to recover financial compensation and possibly injunctive relief. An employee could also claim that the employer cannot use the information it obtained when monitoring the employee's social media activity.

On rare occasions, a governmental agency, the Belgian Privacy Commission, could commence an administrative action.

6.2 How often sanctions are imposed

To date, there have been only a very small number of instances in which employees or administrative agencies have obtained sanctions against an employer based on the employer's access to, or use of, information on social media sites for employment purposes.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are not required to have a data protection officer, except in limited circumstances unrelated to social media activity.

1. General use of social media sites

1.1 Popularity of social media sites

Social media sites are very popular in Canada. In a recent study on privacy commissioned by the Privacy Commissioner of Canada, over 50% of Canadian respondents reported using social media, such as Facebook, LinkedIn and MySpace (source: Office of the Privacy Commissioner of Canada, dated 31 March 2011). In another study, 76% of employees reported using social media (source: Randstad Workmonitor, 'Social media around the Globe', dated March 2011).

Regarding Facebook specifically, another report showed a membership rate of 49.93% of the population, which is 64.27% of Canada's Internet users (source: Socialbakers, 'Canada's Facebook Statistics', dated 13 October 2011). As of September, 2011, Facebook was calculated to have 16.7 million Canadian users (source: WebMediaBrands, 13 October 2011).

2. Use by employers

2.1 Use of information from social media by employers

Surveys indicate that social media is widely used in the Canadian recruitment process, in particular, for researching candidates who have applied for employment.

One survey revealed that LinkedIn is a 'primary resource' for close to 90% of Canadian recruiters. Further, 87% believe social media has improved their ability to connect to 'passive candidates', with 57% claiming an improvement in quality of hire and 49% claiming a reduction in time-to-hire.

Another survey claims 43% of human resource managers believe social media will entirely replace CVs.

2.2 Case law about use of information from social media by employers

There is case law and literature on various aspects of the use of information from social media by employers. For example, there is case law indicating that employers may be subject to a human rights complaint if they use social networking sites in the recruitment or selection process and (i) obtain information that identifies an applicant as a member of a protected group under human rights legislation, and (ii) subsequently make a hiring decision based on that information.

Other cases have recognised an employer's right to discipline and/or dismiss based on an employees' comments on social media sites, where the comments have been made outside work but relate to work.

To date, there has been limited consideration of social media and collective bargaining rights and/or unfair labour practices.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

The Canadian legal consideration of social media in the workplace generally involves privacy legislation, human rights legislation, and the principles established in common law or arbitral jurisprudence, particularly those principles related to reasonable expectations of privacy.

With respect to privacy legislation, private sector privacy legislation will apply to the personal information practices of employers in Alberta, British Columbia and Quebec, as well as any federally regulated employer (e.g. banks, airlines and telecommunication companies).

When making recruitment decisions, Canadian law generally permits employers to access and rely on information obtained from social media websites. In general, where privacy legislation applies, organisations must give notice to potential employees of the organisation's practices in this regard. Depending on the jurisdiction, consent of the employee may also be required.

Organisations must also be aware that information that reveals an employee's membership of a protected group under human rights and/or labour relations legislation may create liability if a hiring or firing decision subsequently relies on that information.

In general, employers are permitted to monitor employees provided that employees are provided with notice and the practice is reasonable in the circumstances. When evaluating whether monitoring is reasonable, both the Canadian privacy regulatory authorities and the courts have relied on the following four part test (derived from Canadian labour arbitral jurisprudence): whether (i) the surveillance is demonstrably necessary to meet the specific need; (ii) it is likely to be effective in meeting that need; (iii) the loss of privacy is proportional to the benefit gained; and (iv) there is a less privacy-invasive way that the employer could achieve the same end.

In October 2011, the Office of the Information and Privacy Commissioner of British Columbia released Guidelines for Social Media Background Checks outlining the privacy risks associated with the use of social media to screen and monitor current and prospective employees. Such risks include: the collection of potentially inaccurate personal information; the collection of too much or irrelevant personal information; and the over-reliance on consent for the collection of personal information that may not be reasonable in the circumstances.

In the case of dismissing for online conduct, information from social media websites can support an employer's decision to dismiss as long as the online misconduct relates to a legitimate work-related interest. Notice and a policy on potential dismissals for online conduct will assist an employer in this regard.

4. Private and public information

4.1 Treatment of private and public information

In some cases, the courts in Canada have provided a greater degree of protection for personal information posted on social networking sites in cases where the individual has limited (e.g. by way of privacy controls) the number of people that can access that information.

The law in Canada does not make a distinction between business webpages and private webpages. Under Canadian privacy legislation, Canadian privacy regulatory authorities have stated that 'information collected about individuals is personal information or personal employee information and is subject to privacy laws, whether or not the information is publicly available online or whether it is online but subject to limited access as a result of privacy settings or other restrictions'.

Assuming privacy legislation would apply, an organisation would only be able to collect and/or use information about an individual posted by third parties in accordance with such legislation, including the consent and/or notice requirements relevant in the jurisdiction.

5. Consent and works council rights

5.1 Consent

Under the common law, consent for an employer to use information and/or photos posted online is supplanted by the employee's reasonable expectation

of privacy in the circumstances. This is a sliding scale, with publically available information having little expectation of privacy, and private information having a high expectation.

The analysis is similar in jurisdictions with privacy legislation. Where personal information and/or photos have been posted and made public by the employee, collection, use, or disclosure of such information without additional consent is generally permitted, provided doing so is reasonable in the circumstances and the employee is aware (by way of a notice and/or privacy statement) that this could occur.

An employer's ability to make use of personal information posted to social media websites is restricted by human rights and labour relations laws which prohibit the use of such information for discriminatory and/or anti-union purposes.

As noted above, depending on the jurisdiction, consent of the employee may be required for the use of personal information by an employer. In most cases, notice would be sufficient to meet this requirement.

5.2 Works council rights

The employer may be required to seek approval or consult with the trade union regarding monitoring social networking activity, if required under the collective agreement or if this is standard procedure between management and the union relevant in the jurisdiction.

In Canada there are no works councils. However approximately 30% of the Canadian workforce is unionised. An employer's use of social media must be consistent with the relevant provisions of the collective agreement.

6. Sanctions

6.1 Regulatory authority and sanctions

Canadian privacy legislation is enforced by the privacy commissioner in the applicable jurisdiction.

Under federal law, a formal complaint must be investigated, subject to limited exceptions. The Commissioner will issue a Letter of Finding and if applicable, recommendations for compliance. The finding may be made public at the discretion of the Commissioner. A complainant (but not the organisation subject to the compliant) may appeal to the Federal Court and the court has broad authority, including to order a correction of the organisation's practices and to award damages to the complainant.

Under the provincial legislation in Alberta and British Columbia, an investigation may be elevated to a formal inquiry by the Commissioner, resulting in an order. Organisations are required to comply with an order within a prescribed time period or apply for judicial review. Similarly, in Quebec, an order must be obeyed within a prescribed timeline.

6.2 How often sanctions are imposed

There have been numerous investigations (and Letters of Findings) under both federal and provincial privacy legislation. In more limited circumstances, orders have been issued by the provincial regulatory authorities.

More recently there has been an increase in the number of judicial decisions in the privacy arena.

7. Data protection officers

7.1 Requirement for data protection officer

Organisations in Canada that are subject to Canadian privacy legislation must have a data protection officer responsible for compliance with the legislation.

Colombia

1. General use of social media sites

1.1 Popularity of social media sites

According to a survey on social media usage, 4,519,320 people in Colombia have a Facebook account. It has also been established that Colombia has more users on Facebook (72.6%) than any other Latin American country. Thanks to smartphones and the facility to download applications, other sites such as Twitter, LinkedIn and Flickr are also gaining in popularity.

2. Use by employers

2.1 Use of information from social media by employers

There are no statistics available about the extent to which employers use social media as a source of information about future or current employees. It is not common in Colombia to use these media in the recruitment process.

2.2 Case law about use of information from social media by employers

Despite the popularity of social media pages, there is no case law or legal literature about the use of information taken from social media by employers.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

In Colombia there is no labour law specifically regulating the access or use of employee information by employers.

Access is regulated by the general laws on data protection. The Colombian legal framework has three main sets of rules in this regard. First, decisions made by the Colombian Constitutional Court regarding data protection and privacy (of which there are now hundreds). Second, Law 1266 of 2008 ('Law 1266'), which specifically regulates 'financial personal data', namely data that are collected and administered by any person or entity for purposes of credit risk assessment. Third, Congress approved last December a general law regulating the collection, administration and transfer of all other types of personal data (the 'New Data Protection Law'), with the exception of financial personal data. Because the New Data Protection Law will regulate what are considered to be fundamental rights in Colombia, it must be reviewed by the

Constitutional Court before enactment. If the Constitutional Court declares it constitutional, it will be enacted within between one to eight weeks. The Court has recently issued a press release declaring that with the exception of a few articles the law has passed the constitutional test. However the text of the decision has not yet been published. We estimate that the test will be published before the end of this year.

The rules (both existing and prospective) create several obligations for 'users' of personal data, depending on the role each person assumes. In general terms, employers must comply with the principles that the Constitutional Court has set forth and this applies to both future and existing employees. Of these, it is worth mentioning the following:

- Freedom principle: Personal Data may only be collected, processed or transferred with the free, express and prior consent of the data subject.
- Purpose: Personal data may only be collected and processed for an explicit, pre-determined and legitimate purpose. The data subject must be informed of the purpose and the collection and/or use must be within the scope of that purpose.
- Restricted circulation: Personal data may only be circulated within the parameters of the freedom and purpose principles, which means within the legal entity that has legitimately obtained the information. Any transfer to other entities, even if affiliated, must be done with the prior consent of the data subject.
- Necessity: Only personal data that are specifically required for the purpose may be collected.
- Accuracy of the data: Personal data stored in databases must be accurate, complete, exact, up-to-date, verifiable and comprehensible. Recording of information that is partial, incomplete, fragmented or that is likely to cause error is not permitted.
- Time limits: Personal Data must only be stored for as long as they are useful for the purpose for which they were collected.
- Security: Personal data must be handled using technical measures that guarantee their safety and the integrity of the records as a whole.
- Confidentiality: All individuals and legal entities that have access to personal data must guarantee their confidentiality at all times.

There is no applicable law or rule regarding reliance on the information. However, we consider that it would be unlawful to dismiss an employee on the basis of information available on social networking sites.

4. Private and public information

4.1 Treatment of private and public information

Private information posted on social networking sites is not considered to be publicly available and it remains protected under the law.

No distinctions are made between business and private webpages and no distinctions are made between information taken from search engines and information only available to 'friends'.

The use of private information posted on social networking sites with or without the consent of the data subject is unlawful. In this situation a third party who posts information that is subsequently used by the employer might also be at risk, as this act would also be considered unlawful.

5. Consent and works council rights

5.1 Consent

The act of posting private information is not considered to be an expression of consent by the data subject for the current or future employer to use the information.

5.2 Works council rights

There is no specific regulation in the Colombian Labour Code providing information or participation rights for works councils with regard to information.

6. Sanctions

6.1 Regulatory authority and sanctions

In Colombia, the sanctions for non-compliance with the rules and/or law on data protection are penalties and fines. There is no specific value for these and they will depend on the decision of the entity imposing the sanction.
Under Law 1266, the public entity responsible for imposing sanctions is the Financial Superintendence (Superintendencia Financiera). Under the New Data Protection Law, the responsible entity will be the Superintendence of Commerce and Industry (Superintendencia de Industria y Comercio).

The public entity that imposes the sanction has the power to enforce it.

6.2 How often sanctions are imposed

We have no specific data as to how often sanctions are imposed.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are not required to have a data protection officer.

Cyprus

1. General use of social media sites

1.1 Popularity of social media sites

There is no official survey regarding the popularity of social media sites. However, according to the Eurostat Press Office, 76% of Cypriot Internet users aged 16-24 use the Internet to post messages to chat sites, blog and network, whilst only 37% of Internet users aged 25-54 use the Internet for such purposes.

2. Use by employers

2.1 Use of information from social media by employers

Reliable statistics are difficult to find and to our knowledge, no organisation tracks the frequency of usage of social media by employers to monitor either prospective or current employees.

2.2 Case law about use of information from social media by employers

There is no up-to-date case law covering the use of information from social media at this point.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

The Processing of Data (Protection of Individuals) Law of 2001, as amended (the 'Law') does not impose any restrictions on employers accessing information about an employee from a publicly available social network page.

According to the Law, where data are collected from third parties the employer must notify the data subject (who might be an employee or an applicant, for example) and inform him or her in an appropriate and explicit way of the purpose of processing and the employer's identity.

A number of firms monitor Internet use and have policies that either restrict employees' access to certain websites (e.g. social network sites) or state that they can only be used during lunch hours or that excessive use that affects the employees' performance can amount to a disciplinary offence.

It is advisable for the employer to offer the data subject the opportunity to discuss and explain the information posted on his social network page and his or her actions.

Further, the law of Cyprus contains a number of anti-discrimination provisions prohibiting certain forms of discrimination. An employer must offer employment and advancement opportunities to all individuals irrespective of race, colour, marital status, religion, sex, national or ethnic origin, age or disability.

According to law an employer must give prior notification to employees of the means of electronic surveillance used in the workplace and the employer has the discretion to prevent personal use of the Internet by disabling access to certain websites. The employer does not have the right to access employees' personal emails or listen to the content of his or her telephone communications. The employee retains his or her right to privacy.

However, if the employee is using social networking pages during working hours and that affects or delays the quality of his or her work, this might constitute a reason for dismissal without compensation (provided fair warnings and a right to a hearing have been given).

4. Private and public information

4.1 Treatment of private and public information

Information posted on social media which is unrelated to work, where the data subject has given his or her consent, are considered to be publicly available unless the data subject takes steps to restrict access to the information.

Cyprus law makes no distinction between business webpages and private webpages. The level of protection provided is equal and the same provisions regarding the rights and obligations apply.

However, personal data cannot be processed for the purposes of direct marketing or the provision of services, unless the data subject notifies his or her consent to the Commissioner for Personal Data Protection in writing.

Further, Cyprus law applies to any processing of personal data where this is performed (a) by a data controller established in the Republic of Cyprus or in a place where Cyprus law applies by virtue of public international law; or (b) by a data controller not established in the Republic for the purposes of the processing of personal data and the data controller makes use of means, automated or otherwise, situated in the Republic, unless such means are used only for the purpose of transmission of data through the Republic.

Information from search engines may be used by the employer but information available only to 'friends' cannot, as it is restricted by the employee.

There are no rulings about information posted by third parties. However, according to the Law, where data are collected from third parties the employer must notify the data subject and inform him or her appropriately and explicitly of the purpose of the processing and the employer's identity.

Anti-discrimination and labour laws would also apply so as to limit the employer's ability to use the information for employment purposes. An employer must offer employment and advancement opportunities to all individuals irrespective of race, colour, marital status, religion, sex, national or ethnic origin, age or disability.

5. Consent and works council rights

5.1 Consent

Personal data are any information relating to an individual who can be recognised from those data, and photographs are included. 'Consent' is defined in the Law as being any freely given, express and specific indication of the data subject's wishes, which is clearly expressed and informed and by which the data subject consents to the processing of personal data concerning him or her. Therefore, the employer can use the information only if the data subject has been notified of the reasons for the processing and has given his or her unambiguous consent.

The Law states that if data are collected from third parties the employer must notify the data subject of its identity and inform him or her appropriately and explicitly of the purpose of processing.

5.2 Works council rights

The matter of who to hire is at the employer's discretion and the works council has no information or participation rights.

However, the employer should notify and consult with the trade unions in relation to the processing of employee data.

6. Sanctions

6.1 Regulatory authority and sanctions

The sanctions for non-compliance are both civil and criminal.

Civil sanctions may be imposed by the Commissioner for Personal Data Protection and these include: (a) a warning and the setting of a deadline for rectifying a breach; (b) fines of up to EUR 8,453; (c) the temporary or permanent withdrawal of the Commissioner's permission to collect personal data, where such permission has been granted; (d) the permanent revocation of a licence; and (e) an order to cease processing and/or destroy data.

The court may impose fines of up to EUR 8,453 and up to five years' imprisonment.

Every individual has the right to apply to the competent court for an injunction for the immediate suspension or cessation of an act or decision affecting him or her involving the processing of data, if the purpose of the processing was to assess, in particular, his or her efficiency at work, financial solvency, credibility and behaviour in general. The data subject has the right to seek compensation in such circumstances.

In the event that the data controller does not comply with obligations arising under the laws of Cyprus, the Commissioner for Personal Data Protection may impose the following administrative sanctions depending on the seriousness of each violation:

- a warning with a specific time-limit for termination of the contravention;
- a fine of up to EUR 8,453;
- temporary revocation of a licence;
- permanent revocation of a licence;
- the destruction of a filing system or the cessation of processing and the destruction of the relevant data.

If an offence is committed for which no other penalty is expressly provided, it is punishable with imprisonment for a term not exceeding five years or with a fine not exceeding EUR 3,417 or both.

6.2 How often sanctions are imposed

The Commissioner for Personal Data Protection often investigates complaints submitted to his office and also launches his own investigations. However, no criminal proceedings for contraventions of the Law have been reported to date.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are not required to appoint a data protection officer.

Denmark

1. General use of social media sites

1.1 Popularity of social media sites

According to a recent survey on social media usage, 2.6 million people in Denmark have a Facebook account (approximately 47% of the population). According to Wikipedia, about 500,000 Danes (approximately 9% of the population) have a LinkedIn account. Other sites such as Twitter and Flickr are also gaining in popularity.

2. Use by employers

2.1 Use of information from social media by employers

According to a survey from 2011, two-thirds of Danish companies use social media to create value for their businesses. This figure includes marketing and product development and is thus not limited to recruitment.

To our knowledge, there are no specific statistics available about the extent to which employers use social media as a source of information about future or current employees, but the figure is without doubt rising.

2.2 Case law about use of information from social media by employers

Despite the popularity of social media in Denmark, only very little case law exists regarding employers' use of information from social media.

In one industrial arbitration case, a security guard was summarily dismissed as a result of the posting of critical statements about the employer on her Facebook wall, which was available only to friends. The arbitrator found that dismissal with notice would have been justified, but summary dismissal was not, because of the lack of prior warning.

Legal literature only deals very briefly with the subject, as matters stand.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

In general, employers (i.e. data controllers) may process personal data on an applicant or employee (data subject) that originate from social media.

Data controllers must, however, at all times comply with the Danish Data Protection Act (the 'Act'). The Act stipulates that data must be processed fairly and lawfully in accordance with the specific rules on data processing. The processing operations permitted under the Act depend on the nature of the data, with sensitive and semi-sensitive personal data requiring a greater level of protection.

In recruitment, employers are under a duty to inform job applicants that data have been collected.

If an employer wishes to monitor employees' Internet usage at work, including social networking sites, the employer must inform them that their online conduct will be monitored before such monitoring begins.

In cases of dismissal, the employer will generally be able to use data posted on social networking sites if this is relevant and necessary to the dismissal. It might also be possible to dismiss an employee on the grounds of online misconduct.

4. Private and public information

4.1 Treatment of private and public information

As mentioned above, only very limited case law exists regarding employers' use of information from social media. However, whether such information and/or photos can be said to be publicly available (and thus less well protected) may depend on the number of people who have access to the information and/or photos.

The Act applies to the processing of personal data by automatic means and does not distinguish between private, business-related or employer-sponsored webpages. As a result, the level of protection is the same for all webpages.

Nor does the law distinguish between data that can be found by a search engine or only made available to 'friends' or close contacts. However, it might have certain practical importance because in some circumstances the Act allows data controllers (i.e. the employer) to process sensitive data that have been made public by the data subject (i.e. the employee).

Employers must give fair processing information to applicants and employees, in other words, they must inform them of the types of data being processed and the purpose of the processing, and, in addition, explain how their data will be used. This applies if the data being processed have been posted by third parties.

5. Consent and works council rights

5.1 Consent

The posting of private information is not necessarily considered to be consent. Under the Act, data may be processed with the data subject's consent. However, if the data subject has not been asked to consent, but the data are publicly available, the employer will, in many cases, be held to be justified in processing the data, but it will depend on the circumstances of each case. However, note that the employer's use of the data must also be relevant and necessary.

5.2 Works council rights

There are no information or participation rights for works councils in relation to information on social media, although under some collective agreements it may be a requirement that works councils be informed beforehand of the process if certain types of data regarding the employees are collected. However, typically, that would be in relation to monitoring employees and would not apply to job applicants or social media.

More generally, employers must give fair processing information to applicants and employees regarding personal data processed about them and this includes informing them of the types of data being processed and the purpose of the processing, and also explaining how their data will be used.

6. Sanctions

6.1 Regulatory authority and sanctions

Under the Act, data controllers must compensate any damage caused by data processing in breach of the Act unless it is established that such damage could not have been averted even if the data had been processed with the required diligence and care.

Any person who commits an offence in connection with the processing of data on behalf of private individuals or bodies may be fined or imprisoned for up to four months, at the discretion of the courts.

The Danish Data Protection Agency is authorised, amongst other things, to:

- enter and inspect (without a court order);
- issue (public) opinions;

- criticise data controllers for failure to comply with the Act or the Agency's opinions;
- report non-compliance to the police (and it is then for the police to decide whether to take action).

Data subjects are also entitled to claim compensation for injury to feelings or reputation under the Danish Liability for Damages Act.

Generally, there have been very few cases of sanctions being imposed by a court against a data controller. The fines that have been imposed range from DKK 5,000 to DKK 25,000 (i.e. EUR 670 to EUR 3,350). Similarly, compensation has been awarded in very few cases, but has amounted to DKK 25,000 (i.e. EUR 3,350).

6.2 How often sanctions are imposed

The Agency often issues opinions and criticises data controllers, but, as mentioned, there have been only very few instances of fines being imposed for non-compliance with the Act and the ones that have, have been small.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are not required to have a data protection officer.

Estonia

1. General use of social media sites

1.1 Popularity of social media sites

There is no official information on how may users of Facebook there are in Estonia, but according to information available on the Internet, it seems to be over 250,000 people – and growing. (For the purposes of comparison, the population of Estonia is about 1.3 million). Therefore, it is fair to say that Facebook is very popular. Other social media sites such as LinkedIn, MySpace and Twitter are also quite popular, but not as widely used as Facebook.

2. Use by employers

2.1 Use of information from social media by employers

There are no reliable statistics about the use of social media by employers seeking information on future or current employees, but it is widely known in practice, that employers often 'google' and receive information from the Facebook and other social media sources on both current and prospective employees. However, employers must inform employees about such research and employees must be informed of the results, including where and why the data were collected and who did the research.

2.2 Case law about use of information from social media by employers

There is no case law on the use of social media by employers. The Estonian Data Protection Inspectorate recently released a comprehensive written opinion on data protection matters in employment relationships, which is widely used by both employers and employees, as it is a practical 'handbook' that is helpful in interpreting the law.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

The law permits employers to access and rely upon all information about an employee that is made publicly available by the employee, e.g. on Facebook, You Tube and other Internet sites. Employers may not use coercion or fraudulent means to gain access to an employee's social media posts or content, where the employee has taken steps to secure the information or otherwise keep it private.

However, employers must inform employees of the collection of data, the results of it, who the processor of the personal data is and for what purpose the research has been done. The same applies to future employees.

The employer may ask for information from a previous employer only with the consent of the employee.

The employer has the right to monitor Internet usage (including social media) only if the employee has given his or her consent and the monitoring is specifically permitted by law or is necessary for performance of the employment agreement. In the latter case, the employer must ensure that the monitoring is proportionate having regard to the objective it is used to achieve.

4. Private and public information

4.1 Treatment of private and public information

Information that is disclosed to an unspecified group of recipients is considered to be information that has been made publicly available.

Information posted on social media sites which is unrelated to work will be considered to be publicly available and not subject to privacy protection, unless the employee has taken steps to restrict access to it (for example, by using a password-protected social media site or privacy settings to restrict access to 'friends').

Estonian law does not make any distinction between business and private webpages. All are subject to the same protection and if the employee has disclosed information on the Internet, the employer acquires the right to acquaint himself with it.

The law does distinguish between information available from search engines and that only available to 'friends' in that the employer may only use information that has been made publicly available by employee. If the employer is not a 'friend' or 'close contact', which it usually is not, then it is not entitled to such information.

As the law does not specifically regulate information posted by third parties, the general rule is that the employee may process this information, but must inform the (future) employee that it has done so and allow him or her to comment and correct any inaccuracies. In general terms, it would seem risky for an employer to utilise information posted by a third party about an employee because it may be inaccurate or unreliable.

5. Consent and works council rights

5.1 Consent

The employer can use information posted by the employee, not necessarily because this constitutes consent, but because, by voluntarily posting the private information or photos and making them publicly available (e.g. via Facebook), the information is no longer considered private and no longer enjoys protection under privacy laws. For that reason, no consent is needed. The employer must, however, still inform the employee that it has collected the information and the purpose of doing so.

5.2 Works council rights

In terms of workplaces that are unionised, the employer is not required to consult with the union before using social media posts or content in the hiring process. Only the employee has the right to such information.

6. Sanctions

6.1 Regulatory authority and sanctions

The most common enforcement tool against an employer that violates privacy protection in relation to an employee's social media activity would be a private lawsuit filed by the employee against the employer seeking to recover financial damages. Compensation for moral harm is relatively rare and in employment cases even rarer. Infringements of personal data processing rules may also result in an administrative action and a fine, which may be imposed by the Data Protection Inspectorate to a maximum amount of EUR 32,000.

Sanctions are enforced by the court, the Data Protection Inspectorate (for administrative procedures) and by bailiffs (if the debtor fails to fulfil the court's or Data Protection Inspectorate's decision).

6.2 How often sanctions are imposed

To date, there have been only a very small number of instances in which employees or administrative agencies have obtained sanctions against an employer based on the employer's access to, or use of, information on social media sites for employment purposes.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are not required to have a data protection officer. However, having one does enable the company to avoid the necessity to register itself as a processor of sensitive personal data, if such data are processed as part of its activities (e.g. hospitals).

France

1. General use of social media sites

1.1 Popularity of social media sites

According to recent surveys 25 million French people are registered on one or several social media sites and 10 million visit them on a daily basis. Most social media users are registered on several social media sites, such as Facebook, Twitter, Viadeo (which is a professional social networking site similar to LinkedIn) or LinkedIn. Viadeo claims to have 30 million visitors, with four million of them in France. We do not have any figures for Twitter, which claims to have had 200 million visitors globally in 2011, but we do know that around 20 million French people are registered on Facebook, with eight million of them using it daily, notably at the workplace and during working hours.

2. Use by employers

2.1 Use of information from social media by employers

Reliable statistics are difficult to find. According to Burston-Marsteller, 79% of large international companies favour using social networking as a form of communication; 65% of them would use Twitter and 54% of them Facebook (http://bmfrance.burstonmarsteller-online.eu). Most specialists think that at least 30% of employers regularly utilise social media for hiring or recruiting purposes. There are no official statistics in France, notably because job applicants must normally be informed prior to recruitment of all measures and techniques used to recruit them and of all information that may be collected in the recruitment process (Articles L. 1221-8 and L. 1224-9 of the Labour Code). Moreover, the works council must be informed of the recruitment techniques prior to their use (Article L.2323-32 of the Labour Code). In practice, social networks have only been heavily used by human resources departments for the last three years. Nevertheless, in the near future, it is likely that every CV will be systematically compared to the profile of the applicant and to his or her 'reputation' based on information collected on the Internet. To our knowledge there has been one significant case where an employer terminated an employee's contract for social media-related misconduct (the Industrial Tribunal in Boulogne Billancourt,19 November 2010, held that disparagement of the employer via Facebook was misconduct justifying dismissal).

2.2 Case law about use of information from social media by employers

Employers must exercise caution when using data collected on social media, and also when disciplining for social media-related conduct. According to recent case law (Supreme Court, 9 February 2010), provided the employer has given prior notice to employees, it can monitor all Internet usage during

working hours done using IT equipment provided by the employer for work, Such Internet usage is considered to be for professional reasons and therefore, the employer can access it without the presence of the employee. In France, there is a conflict between freedom of thought and expression; the protection of privacy; and the need to protect the public image of the organisation.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

As mentioned, the employer is permitted to access to information from social media when making recruitment decisions, provided it has individually informed the applicants concerned and has also collectively informed the works council of this recruitment method.

During employment, the employer is permitted to monitor the use of social media sites via the Internet during working hours using equipment or networks owned or controlled by the employer at the workplace. It is only if the employee is using emails and expressly specifies in an email that it is 'confidential', 'private' or 'personal' that the employer is not permitted to access it (this is the principle of secrecy of correspondence).

The Industrial Tribunal in Boulogne Billancourt ruled on 19 November 2010 that the employer is permitted to dismiss employees for online misconduct.

Nevertheless, judges in France are reluctant to consider there to be an abuse of freedom of expression, based solely on a description of the employer online.

IT policies applicable to companies may be a guideline to enable judges to consider the potential abuse of freedom of expression. How the case of an employee who has posted a comment on the Internet is perceived also depends on the sector of activity and on the nature of the employee's job.

4. Private and public information

4.1 Treatment of private and public information

Information posted on social media sites which is unrelated to work cannot be used for professional reasons by the employer, if the posting takes place outside working hours and outside the workplace, as this will be considered to be an aspect of the private life of the employee.

Nevertheless, there is a possibility that the information could justify dismissal by the employer if it can be shown to have damaged the company's reputation. This would be done, not as a disciplinary action for misconduct as such, but as a dismissal for personal reasons based on the consequences of the behaviour.

Private webpages are protected by restricted access, which mean they are not (in theory) accessible to the employer, unlike business web pages. There is no specific regulation of business webpages.

The law does not distinguish as such between information found by search engines and information only available to 'friends' or close contacts but the recent case law referred to above seems to make a distinction between restricted access and less restricted access on Facebook.

In general, there is no restriction for the employer on the use of use search engines. On the other hand, if the employer 'disguised' itself as a 'friend' in order to enter a social media network and gain access to private data, this would be unlawful in France, as it would be considered to be entrapment of the employee.

There is no authority on information posted by third parties as yet, but we would expect that publicly available information could be used, whilst secured information could not. However, we do not recommend the use of information posted by a third party, as it may not be reliable.

5. Consent and works council rights

5.1 Consent

The employer can use information posted by employees, not necessarily because the employee's posting constitutes consent, but because, by voluntarily posting the information or photos and making them publicly available, the information is no longer considered private and no longer enjoys protection under privacy law.

Nevertheless, if the employer uses the information in the context of the employment relationship, it cannot use it for external purposes (e.g. by making it public) without the formal consent of the employee pursuant to the 'right of image'.

An employee's consent for the employer to access information on a password-protected or otherwise restricted social media site, would eliminate

any potential claims he or she had based on privacy law. However, the employee could argue that the consent was not fully informed, which would enable him or her to bring an action. Other relevant law, such as anti-discrimination and labour law could also limit the employer's ability to use information.

5.2 Works council rights

The works council must be provided with information before the employer may collect or use data posted on social media sites.

6. Sanctions

6.1 Regulatory authority and sanctions

If an employer violates privacy protection, the employee could bring an action against the employer and seek damages. In addition, the fact that the employer could not use the information collected whilst in breach of privacy rules would act as a sanction. The French authority that fights discrimination (the 'Défenseur des Droits') could intervene, even in a law suit and the body responsible for the protection of all individual personal data (the Commission Nationale Informatique et Liberté, the 'CNIL') could impose a fine on employers that do not comply with data protection law.

The courts can enforce any court judgment made against an employer.

6.2 How often sanctions are imposed

There are no statistics about how often sanctions are imposed. However, there have been numerous cases in which the employer has been prevented from using data collected in breach of privacy law.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are not legally required to have a data protection officer.

Germany

1. General use of social media sites

1.1 Popularity of social media sites

As of June 2011, an estimated 25% of Germany's population, i.e. 20 million, have a Facebook account. Other popular sites are the VZ-networks (17.5 million users), Xing (4.5 million), MySpace (4 million), LinkedIn (800,000), and Twitter (600,000).

According to a survey from April 2011, German users of social network sites:

- make their profile information available to:
  - friends only: 41%
  - certain friends only: 8%
  - members of the respective network: 28%
  - all Internet: 21%

- share the following information:
  - name: 77%
  - age: 76%
  - portrait picture: 60%
  - relationship status: 57%
  - work: 46%
  - party and holiday pictures: 25%
  - address: 8%
  - sexuality: 4%

2. Use by employers

2.1 Use of information from social media by employers

A 2010 survey of 1,500 HR managers showed that 45% of German companies do research on job applicants by using search engines. A further 21% of them research business-related social networking sites such as LinkedIn, while 17% look for information on social networking sites such as Facebook and StudiVZ.

2.2 Case law about use of information from social media by employers

There is case law about the use of information from social media sites by employers. The cases mainly concern the use of the Internet at the workplace for private reasons by employees (supervised by the employer). Other than in extreme cases, a warning is necessary before an employee may be dismissed.

In May 2011, Daimler complained about a Facebook group and contacted employees who 'liked' a comment on the page that called the Daimler CEO a liar. Daimler said it learned about the comment from a third party rather than from spying on employees. Daimler did not, however, take legal steps against the employees.

There is literature on the question of who owns an employee's Facebook and Xing information (including access to the site) if the employer has asked the employee to use social media for networking or other business purposes. There is consensus that such information belongs solely to the employer, provided the employee received the information on behalf of the employer.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

During recruitment, employers who wish to collect personal data from social network sites need an employee's or applicant's written consent. Otherwise, the collection of the data must be either necessary for the employer to enable it to decide whether an employment relationship should be established or terminated or how it should be conducted.

Therefore, the collection of personal data from social networking sites found using search engines such as Google is justified unless the employee's interests outweigh those of the employer. Given that the employee or applicant published the information himself and thereby gave consent for it to be found using search engines, collection of the data by the employer is usually justified.

By contrast, if personal data is only accessible to other members of a social networking site, it is not generally accessible and the collection of such data is prohibited unless they are taken from business-related social network sites.

During employment, information posted on social media sites can only be monitored if it can be found on the Internet using search engines such as Google.

Regarding termination for online misconduct, there is still little case law on dismissal decisions by employers based on social media information. This is probably because in German law, even if an employee insults the manager or employer, say, on Facebook, a warning is usually necessary before the employee may be dismissed. However, there is an account of a court proposing the

termination of an employment contract in order to settle a case where a trainee simulated an illness when in fact she was in Spain (the Labour Court of Düsseldorf, 25 August 2011). This was known because she posted pictures of her holiday on Facebook.

4. Private and public information

4.1 Treatment of private and public information

Whether the information is protected depends on whether:

- it is generally accessible, i.e. can be found using search engines;
- it is only accessible to other members of a given social networking site;
- it is only accessible to 'friends';
- it can only be found on third party profiles.

In other words, whether the employee's interest in keeping such information private outweighs the interests of the employer.

At the time of writing, there is no explicit differentiation between private and publicly available information. In 2010 however, the German Government did announce amendments to the Federal Data Protection Act that have yet to be enacted. The law will differentiate explicitly between social and professional networking sites to the following effect:

- Research done by employers on social networking sites will be restricted by law.
- Employers will be obliged to collect personal data directly from the employee or applicant.
- Personal data that are 'generally accessible', (i.e. can be found on the Internet, in newspapers, etc.), may be collected by the employer if the employee or applicant was given prior warning, e.g. through the job advertisement. For example, an employer may still research on the Internet in order to ascertain whether an employee's behaviour on professional network sites is not bad for business.
- If an employee or applicant so requests, the employer must inform him or her about the collection of personal data on him or her.
- all personal data must be deleted or returned to the applicant if an employment relationship is not entered into.

If an applicant's or employee's profile information is only accessible to 'friends', an employer would first need to send or accept a 'friend request'. Employers would be prohibited from simply collecting such information unless it was necessary for 'professional reasons'.

It will not normally be possible to collect personal data found on third party profiles (e.g. guest books, groups and photo albums) from social or professional networking sites. Therefore, an applicant will probably not expect potential employers to collect data from third parties, especially because it is not likely to be reliable. Moreover, the employee may even be unable to control information posted by third parties. Accordingly, his or her right to privacy outweighs the employer's interest in collecting the personal data for professional reasons.

5. Consent and works council rights

5.1 Consent

If an employee publishes private information and/or photos, thus making them 'generally accessible', he or she would usually be considered to have taken into account their availability, meaning that the employer's collection of such data will normally be justified.

5.2 Works council rights

In businesses with more than 20 employees, the works council (if one exists in the company) must be fully informed before an employee is hired, i.e. the employer is required to provide the works council with all information relevant to the open position to enable the works council to get a full picture of all applicants. In addition, the works council has participation rights for all employee behaviour issues including the use of social media at the workplace. This means that the employer must negotiate an agreement with the works council prior to implementing a social media policy.

6. Sanctions

6.1 Regulatory authority and sanctions

Compliance with data protection law is enforced by the local Data Protection Authority, as the supervising institution. Each of the 16 German States has a local Data Protection Authority. These Authorities may:

- enter and inspect the premises of a data controller during business hours;
- inspect business documents and personal data that have been saved as well as the programs used for saving personal data;
- impose measures to cease the unlawful processing of personal data or technical or organisational faults;
- impose a penalty payment that is payable if breaches continue ('Zwangsgeld');
- impose a fine ('Geldbuße') of up to EUR 300,000 or, in severe cases, initiate criminal proceedings which could lead to imprisonment (for up to two years);
- in severe cases, prohibit the data processing altogether (i.e. if the abovementioned measures or fines have not worked).

Employers may be required to inform employees and the authorities if personal data have been unlawfully transferred or disclosed to third parties.

6.2 How often sanctions are imposed

According to the Federal Commissioner for Data Protection and Freedom of Information, German agencies still lack the resources to monitor and sanction all violations. At the time of writing, there are no statistics available on how often sanctions are imposed. Among the sanctions reported in the news are a fine of EUR 137,500 on a drugstore chain and a fine of EUR 36,000 on a discounter. Both employers collected data on employees' sickness. At the time of writing, however, there is no published case law on employers' misconduct with regard to social network sites (e.g. an employer that monitors employees' use of Facebook at the workplace).

7. Data protection officers

7.1 Requirement for data protection officer

In order to avoid the need to notify the local Data Protection Authority in advance of all processing of data, employers with more than nine persons who process personal data within the organisation are required to appoint a Data Protection Officer.

The Data Protection Officer may be any person who has the knowledge and reliability of character necessary under German law to fulfil his or her tasks. Either an internal or external person may be appointed. The Data Protection Officer enjoys a higher level of legal protection against termination, which means that he or she may not be terminated unless for severe cause.

The task of the Data Protection Officer is to ensure compliance with the provisions for the protection of personal data in the Federal Data Protection Act and other statutes. In order to facilitate this, the Data Protection Officer must become involved in any projects involving the processing of personal data in good time. The Data Protection Officer must inform those responsible for processing the data about the protections of personal data that exist in law.

Although not required by law, it is advisable that companies consult their Data Protection Officer in addition to the works council prior to implementing a social media policy.

Greece

1. General use of social media sites

1.1 Popularity of social media sites

According to recent surveys, more than four million people possess social media accounts in Greece, with Facebook having over three million users, i.e. 30.59% of the population. Other sites such as LinkedIn, MySpace and Twitter do not provide statistics concerning the number of subscribers, although it is fair to say that they are experiencing continuous growth.

2. Use by employers

2.1 Use of information from social media by employers

Although reliable sources of statistics are hard to come by, it is clear that about 30 to 33% of employers frequently use social media sites as a source of information about candidates. It should be mentioned that LinkedIn is widely used for hiring and recruiting employees for senior management (approximately 50%) and middle management (approximately 35%).

2.2 Case law about use of information from social media by employers

As the use of information on social media sites constitutes a recent practice for Greek employers, no disputes relating to this have been recorded and there is no legal literature about it.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

The law permits employers to access information from social media sites about prospective or current employees if it is publicly available and not secured or otherwise kept private. The use of such information is permitted if it i) directly relates to the framework of the employment relationship and the work; ii) concerns the privacy and personality of the employee; and iii) does not contain sensitive personal data such as racial or ethnic origin, political opinions, religious beliefs or sexual orientation.

As far as the dismissal of an employee based on such information is concerned, the Athens Court of First Instance recently made a notable ruling (Decision 34/2011) that dismissal for, inter alia, visiting social networking sites during working hours is not abusive and is fully lawful. Relevant also is Decision 37/2007 of the Hellenic Data Protection Authority, which held that

the processing of an employee's Internet search history (revealing visits to pornographic sites) is unlawful. This decision is a strong indicator that the processing of information gathered from social media sites will be considered contrary to the Law on Data Protection and, as such, may not be grounds for a lawful dismissal.

4. Private and public information

4.1 Treatment of private and public information

Private information and/or photos that have been posted on social networking sites are considered publicly available but it is important to weigh up any rights infringement associated with the publication of the information against the principle of proportionality. However, according to the law on Personal Data Protection (2472/1997), information and/or photos are characterised as personal data and can be used only if the data subject has given consent or the law provides otherwise.

At the time of writing, there is no differentiation between private and publicly available information as far as data protection is concerned.

Note that it would be risky for an employer to utilise information about an employee which has been posted by a third party because the information may be inaccurate or unreliable. The posting of information by third parties without consent is, in any event, unlawful.

5. Consent and works council rights

5.1 Consent

According to Greek law, the consent of the data subject should be a clear, explicit and specific statement of fully informed willingness. Accordingly, the simple posting of private information is not considered consent for others to use it.

5.2 Works council rights

There are no obligations to allow participation by works councils in Greece.

6. Sanctions

6.1 Regulatory authority and sanctions

Breaches of the Law on the protection of personal data in the field of employment relations (the 'Law') can result in administrative sanctions imposed by the Hellenic Data Protection Authority, as well as penal sanctions imposed by the courts.

The Data Protection Authority may impose administrative sanctions for breach of duties arising from the Law and any other regulation on the protection of individuals from the processing of personal data on data controllers or their representatives (e.g. the CEO of the data controller). The penal sanctions imposed by the Greek courts are set out in Article 22 of Law 2472/1997.

6.2 How often sanctions are imposed

The Hellenic Data Protection Authority has recently imposed a fine of EUR 20,000 on an organisation for serious breaches of the rules on processing employees' personal data. The Data Protection Authority has the power to impose such fines without a court order.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are required by law to appoint a data protection officer. The data controller is, in most cases, the same person as the employer or head of department either formally or in practice. The data controller must take appropriate organisational and technical measures to ensure data security.

India

1. General use of social media sites

1.1 Popularity of social media sites

Facebook and LinkedIn are quite popular in India. According to Internet World Stats (http://www.internetworldstats.com/asia.htm) there were 100 million Internet users in India as of December 2010, which amounts to an 8.5% market penetration. Of these 29.5 million are Facebook users (as at 30 June 2011), which is a penetration rate of 2.5%.

2. Use by employers

2.1 Use of information from social media by employers

There is no information available about the extent to which employers use media as a source of information about future or current employers. However, it is likely that both Facebook and LinkedIn are becoming increasingly popular as part of the recruitment process.

According to the Employment News Weekly, the corporate world is using forms of social recruitment for staff, whereby social networking websites are used to locate and recruit suitable candidates for their organisation. Employers visit social networking websites to search the profiles of candidates with relevant and suitable skill-sets. People looking for jobs may use these social and professional networking sites to enhance their careers and boost their job searches.

However, according to the Economic Times, about 42% of employers have found content on social networking sites that has led them not to hire prospective candidates.

2.2 Case law about use of information from social media by employers

No reported case law or legal literature about use of information from social media by employers is available.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

The law permits employers to access and rely upon all information concerning prospective employees that is publicly available and/or consented to by them. However, employers should verify the information before relying on it.

An employer may not use any unlawful means to gain access to the social media posts or content of an employee or prospective employee if he or she has taken steps to secure the information or otherwise keep it private. However, an employer may monitor its employees' social media use even with respect to private content if the employee is utilising employer-owned or controlled equipment or networks and the employer has a clearly-written computer usage policy informing employees to the effect that they have no right to privacy in their usage of company systems and that such usage may be monitored at any time by the employer.

An employee can also be dismissed for online misconduct if this is in violation of company policy.

4. Private and public information

4.1 Treatment of private and public information

Any information available for public view or in the public domain would be considered as public information, while information which is available for a select group or is not in public domain would be considered to be private information.

At the time of writing, there is no distinction between business and private webpages. However, if an employer maintains a private webpage which has restricted and password protected access, then the information would not be considered to be information in the public domain. Indian law provides protection for information posted on an employer-sponsored webpage which can be accessed only by authorised personnel.

The law is not well-developed in terms of distinguishing between sources of information from the Internet. However, information available on search engines is considered to be public information and it therefore might not be protected.

In the case of information made available to friends and close contacts only, the provider of information is required to take adequate precautions and safeguards to prevent that information from being placed in the public domain.

Information concerning a person but posted without his or her knowledge or consent can be collected but should not be relied upon.

5. Consent and works council rights

5.1 Consent

Any private information which is posted on a public forum is general information available to the public and it can be accessed by a future or current employer without consent.

However, in accordance with data privacy rules, 'personal and sensitive information' may only be collected following receipt of consent. It must also only be used in accordance with those rules and must be protected by the employer.

5.2 Works council rights

There are no rights for works councils to receive information or to participate where an employer wants to use information posted on social media before inviting a job applicant.

6. Sanctions

6.1 Regulatory authority and sanctions

The Adjudicating Officer, as appointed under the Information Technology Act, has powers to adjudicate claims for damages of up to INR five million (approximately EUR 75,000).

Non-compliance may amount to a criminal offence, in which case this could be prosecuted in a criminal court.

6.2 How often sanctions are imposed

As and when there is non-compliance, sanctions are imposed, but information about this is not in the public domain and we cannot therefore provide any indication about the frequency of sanctions.

7. Data protection officers

7.1 Requirement for data protection officer

Every organisation is required to appoint a systems administrator. The duty of the systems administrator is to ensure that proper security measures are maintained on computer networks, so as to ensure adequate safeguarding of the data and information available within the organisation.

Ireland

1. General use of social media sites

1.1 Popularity of social media sites

According to Internet World Stats, there are approximately 1.9 million Facebook users in Ireland as of March 2011, which amounts to approximately 41.5% of the population. According to the Irish Internet Association there are 353,000 Irish users of LinkedIn. There are 245,000 Irish users of Twitter based on figures released by Ipsos MRBI. Statistics released by Comscore, reveal that 84.2% of all Irish Internet users used social networks in December 2010, up 8.1% on December 2009, with the average Irish person spending 18 hours and 7 minutes online each month.

2. Use by employers

2.1 Use of information from social media by employers

Reliable statistics in this area are very limited in Ireland. However, recent surveys indicate that many Irish employers are using social networking sites to monitor employees who are absent on sick leave. One of these surveys indicated that 83% of employers have monitored employees' Facebook statuses to check whether employees were truly ill. The result was that 67% of companies disciplined staff for bogus illnesses.

Another recent survey by Eurocom Worldwide in association with Irish agency Simpson Financial and Technology PR suggests that 38% of Irish technology companies examine social media profiles to determine the suitability of potential employees.

2.2 Case law about use of information from social media by employers

Employers must exercise caution when imposing discipline based on social media-related conduct and a number of cases are instructive. Anyone seeking to rely on information in disciplinary matters should seek advice on the most recent case law.

In one recent case an employee was dismissed for posting derogatory comments about her manager on the social networking site, Bebo. Although the employer was found to have followed fair procedures, the Employment Appeals Tribunal held that the sanction of dismissal was not proportionate. While the comments were disrespectful, inappropriate and damaging they were not gross misconduct. In another case, a college computer lecturer was dismissed for claims in his online blog that the president of one of Ireland's largest universities was the son of a Nazi. In that case the lecturer received a

significant award due to a lack of appropriate procedures in the dismissal process.

Data protection law in Ireland applies to personal data gathered, regardless of where they are sourced. If employers gather information about employees from social media then they must comply with such laws. Some of the guidance notes from the Data Protection Commissioner should be considered before gathering employee information.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

The law permits employers to access and rely on all online information about an employee or prospective employee that the person has made publicly available, where the clear implication of the person making the data available is that he or she gives implied consent to their use for this purpose. The exception to this principle is personal data that are categorised as sensitive data, including relating race, disability and union membership.

From a data protection point of view, the employer should be open about where information about the employee or prospective employee is sourced and what it will be used for. An employer may not use coercion or fraudulent means to gain access to a person's social media posts or content where the person has taken steps to secure the information or otherwise keep it private.

An employer may monitor its employees' social media use if the employee is utilising employer-owned or controlled equipment or networks provided that the employer is doing so for legitimate purposes, has complied with privacy, constitutional and data protection laws and the employer has a clear, well-written and legally compliant computer usage policy informing employees that such monitoring may take place. Regard should also be had to data protection guidance issued by the Data Protection Commissioner from time to time. If the employer has obtained consent to the use of personal data in the case of disciplinary procedures or dismissal, and the use of the data is proportionate and legitimate, it may be used in that context.

4. Private and public information

4.1 Treatment of private and public information

Publicly available information can, in certain circumstances, be used by employers for legitimate purposes provided the use complies with data protection law.

Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. Irish law provides that all personal data must be processed fairly and it does not distinguish between business information about a person and private information in terms of the level of protection. However it will be easier for an employer to claim that the employer has implied employee consent to use information posted on public, business webpages than on personal, private webpages.

Aside from the issue of implied consent which can arise in certain circumstances (see below) Irish data protection law does not distinguish between information that can be found by search engines and information that is only available for 'friends'.

Information, however it is made available or created, which relates to an individual is considered to be personal data and is subject to the provisions of Irish data protection law. If the individual to whom the data relate has not posted the information, it is highly unlikely that an employer could be considered to be processing it with the consent of the data subject. In order to make use of this information the employer would have to ensure it is processed for a legitimate purpose, that it is entitled to gather and process the data notwithstanding that the employee has not given consent and that the use of it does not prejudice the rights and freedoms of the employee. It can be difficult to rely on the narrow legal exceptions to the principles that the employee must be told what data are gathered about him or her, and where the data came from.

Employers need to be particularly cautious in the case of sensitive personal data, where additional conditions must be satisfied in order to gather and make use of the data.

5. Consent and works council rights

5.1 Consent

Where an employee posts information on the understanding that it will be made available only to a restricted group of users, such as friends and family, it is not likely that this action would be considered to be consent to employer use under Irish data protection laws. However, knowingly posting information that will be publicly available without limitation to any users of the website, could amount to implied consent to use of that information under Irish law. Regard would have to be given to all of the circumstances relating to the post, including the terms and conditions of use of the website to which the post is made.

For sensitive personal data (including information relating to a person's sexuality, race, or political or other beliefs), employers would need to be satisfied that the person has given their explicit consent to their information being used or has taken deliberate steps to make their information public. Public posting of the information on a website would not be sufficient to constitute explicit consent.

5.2 Works council rights

There are no relevant works council information or participation rights, unless such rights are specifically set out in collective agreements between the relevant employees and the employer.

6. Sanctions

6.1 Regulatory authority and sanctions

Breaches of Irish data protection laws are generally dealt with by the Data Protection Commissioner. The Commissioner has powers to investigate complaints made by data subjects, to audit businesses and to issue enforcement notices to those in breach of Irish data protection laws, requiring them to take the steps necessary to comply.

There are a large number of offences applicable for failure to comply with data protection law. The maximum fine on summary conviction for such an offence is set at EUR 3,000. For convictions on indictment, the maximum penalty is a fine of EUR 100,000. In addition directors, managers, secretaries or other officers of an organisation which has committed an offence are also guilty of that offence, if it is proved to have been committed with their consent or connivance or to be attributable to any neglect on their part.

If the Commissioner investigates a complaint, is satisfied there has been a breach of Irish data protection laws and is unable to resolve the issue amicably, he can issue a decision as to whether Irish data protection laws have been contravened. Decisions can be appealed within 21 days, and the decision of the court is final. The Commissioner has no power to award compensation, however.

Data subjects can also bring a civil action against data controllers in circumstances where non-compliance with Irish data protection laws has resulted in both a breach of duty owed to the data subject and harm suffered by the data subject. Actions of this nature are rare in practice.

6.2 How often sanctions are imposed

In practice, complaints by data subjects and/or investigations conducted by the Commissioner are frequently resolved out of court. Data controllers will often be required, for example, to make changes to their data protection policies, business structures and contracts in order to satisfy the Commissioner. They may also be required to make a donation to a charitable organisation.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are not required to have a data protection officer under Irish data protection laws. However, organisations that are required to register with the Office of the Data Protection Commissioner must provide the name of an officer, which will then appear on the public register, and act as a contact point for the public and the Commissioner. In practice, this person often deals with data protection issues arising within the organisation, such as data subject access requests, registration and general compliance.

Italy

1. General use of social media sites

1.1 Popularity of social media sites

According to research, 18 million people in Italy have a Facebook account. Italy is the ninth biggest holder of Facebook accounts.

Other sites such as LinkedIn, Twitter and MySpace do not disclose statistics about the number of Italian subscribers.

2. Use by employers

2.1 Use of information from social media by employers

Reliable statistics are difficult to find, given that under Italian law, the monitoring of employees using social media as source of information is not permitted.

To our knowledge, no organisation tracks the frequency of usage of social media by employers for monitoring current employees. However, we are aware of at least three or four cases of termination as a result of comments made on Facebook.

2.2 Case law about use of information from social media by employers

There is no case law on the misuse of information collected via social media. However, the Data Protection Authority has issued guidelines concerning the monitoring of employees through social media.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

According to Italian law employers must not use employee data and information in any way, if they are not relevant to employees' attitudes towards their jobs or to their skills.

The law permits employers to access and rely on any information about an employee that is publicly available unless it relates to a protected characteristic, such as race or disability, or a protected activity, such as union organising.

The same rules apply to job applicants and information that is not relevant to the job may not be used in any event.

By contrast, the monitoring of employees during working hours via the Internet is forbidden by law. The employer's Internet policy must be authorised or agreed with the unions.

An employer may not use coercion or fraudulent means to gain access to an employee's social media posts or content where the employee has taken steps to secure the information or otherwise keep it private. However, an employer may monitor its employees' social media use even with respect to private content if the employee is utilising employer-owned or controlled equipment or networks and the employer has a clear, well-written computer usage policy informing employees that they have no right to privacy in their usage of company systems and that such usage may be monitored at any time, even with certain restrictions, by the employer.

Few cases of dismissal based on social media information have been registered and they mainly relate to the misuse (or use against company policies) of the Internet (including Facebook) during working hours.

4. Private and public information

4.1 Treatment of private and public information

The law permits employers to access and rely on any information about an employee that is publicly available unless it relates to a protected characteristic, such as race or disability, or a protected activity, such as union organising.
However, the employer cannot use the employee's information if it is not relevant to employees' attitudes towards their jobs or to their skills.

Italian privacy law does not provide any distinction between different types of webpages, irrespective of the employee's consent, the employer cannot use the employee's information if it is not relevant to employees' attitudes towards their jobs or to their skills.

In the same way, Italian privacy law does not provide any distinction between information on search engines and information only for 'friends'.

Other law, such as anti-discrimination law would also apply to information posted on an employer-sponsored webpage.

There is no case law or literature on the use of postings by third parties by employers. However, as mentioned, the employer cannot use the information found if it is not relevant to employees' attitudes towards their jobs or to their skills.

5. Consent and works council rights

5.1 Consent

Irrespective of the employee's consent, the employer cannot use the employee's information if it is not relevant to employees' attitudes towards their jobs or to their skills. If the information is relevant, the employee's posting will constitute implicit consent to disclose the information. However, note that anti-discrimination law may, in any case, limit the employer's ability to use the information, even if it is relevant.

5.2 Works council rights

In general terms, the monitoring of employees' current activity via the Internet is forbidden and all Internet policies must be authorised by the Labour Inspector or agreed with the unions.

6. Sanctions

6.1 Regulatory authority and sanctions

In terms of sanctions, the employee could bring a claim before the Employment Court for damages.

The employee could also bring a claim before the Data Protection Authority in order to obtain an injunction on the employer not to use the data and to retract all action taken based on processing in breach of the law.

The Data Protection Authority and the Employment Court could also impose administrative sanctions, such as fines, and even criminal sanctions.

The courts would enforce any court-issued judgment against an employer resulting from litigation. The courts also would enforce any sanctions imposed by the Data Protection Authority against an employer.

6.2 How often sanctions are imposed

At the time of writing, we have no information about any cases in which employees or the Data Protection Authority have obtained sanctions against an employer based on the employer's access to, or use of, information on social media sites for employment purposes.

Nevertheless, actions brought under data protection law are increasing rapidly, and can be seen as a new trend.

7. Data protection officers

7.1 Requirement for data protection officer

The employer must appoint a data protection officer to be responsible for data processing. His or her duties are to check and ensure compliance with the data protection rules and all related laws.

Luxembourg

1. General use of social media sites

1.1 Popularity of social media sites

According to the President of the National Commission for Data Protection (Commission Nationale pour la Protection des Données, 'CNPD'), in an article of 11 May 2011, about 180,000 Facebook accounts were active amongst the Luxembourg population. This is relatively significant in relation to the number of resident households, i.e. a little over 200,000. This means that there is almost one Facebook account per household in the country.

Moreover, it appears that mobile Internet users spend an average of 2.7 hours a day on social networks.

2. Use by employers

2.1 Use of information from social media by employers

Statistics on the use of social networks by Luxembourg employers are difficult to find. However, during a meeting on 31 March 2010 with the trade union Lëtzebuerg Chrëschtleche Gewerkschafts Bond ('LCGB'), the CNPD confirmed that, in practice, many employers use social media in order to collect information about employees or job applicants.

2.2 Case law about use of information from social media by employers

At the time of writing, neither the Legislator nor the courts have taken a stance on the lawfulness or otherwise of the use of information collected by employers via social media sites.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

The legislation does not provide rules specifically applicable to employers accessing information disclosed by an employee on social media sites.

However, the generic regulatory framework on individual data and privacy protection applies. Data processing must:

- be lawful and done in accordance with specific purposes;
- be processed fairly;

- comply with the related security and privacy provisions;
- be subject to prior declaration to, or approval from, the CNPD, according to the circumstances (prior approval is necessary for monitoring employees using technical means at the workplace).

As far as the recruitment process is concerned, the employer must comply with all the above-listed conditions Moreover, the processing should not include 'sensitive data' such as, notably, the applicant's race, political and/or religious views, health or sexual orientation.

The law does not prohibit employers from relying on information found on social networks to hire or reject a job applicant. However, the employer would never be allowed to use sensitive information, in order to make its decision, even if these had been collected via a public site, since this could be considered discriminatory. In practice, however, it would be for the data subject to prove that the information collected influenced the employer's decision.

In Luxembourg, 'monitoring' means any activity which is carried out using technical means and consists of observing, collecting or recording in a 'non-occasional' manner, the personal data of one or more persons, concerning behaviour, movements, communications or the use of electronic computerised systems. Therefore, a manual search of social media, even performed regularly, would not be considered as 'monitoring', and should be permitted. Employers should, however, not use fraudulent means to access the data.

If social media or websites are monitored permanently by the employer using technical means, for example specific spy software, in such a way as to allow the employer to extract information whenever needed, this would not be permitted.

As long as the information is publicly available, there is no legal constraint to prevent the employer at least accessing the information.

As for reliance on the information, the generic principle of good faith in the employment relationship and in personal data processing is relevant. According to this principle, the employer would not be allowed to use dishonest, disloyal or fraudulent means of accessing such information. The fraudulent access to an employee's personal data would deprive the employer of the right to use those data afterwards. Indeed, this would constituent an infringement of the employee's private life and privacy and of the generic principles of loyalty and good faith in the employment relationship and personal data processing.

In order to justify a dismissal, the online misconduct would have to be evidenced by information collected in compliance with the applicable legislation (i.e. in compliance with privacy rules, personal data processing and the right to a private life).

4. Private and public information

4.1 Treatment of private and public information

As regards the protection of employees' private life and private correspondence, information posted on social networking sites will be considered to be public only if it is available to a large number of people. If so, the data will be less well-protected.

As regards personal data protection, as long as private information posted on social networking sites is covered by the legal definition of 'personal data', it will automatically fall within the ambit of personal data protection. Thus, even though it is publicly available, any data processing would have to comply with the law.

The law of 1982 on the protection of private life and correspondence does not distinguish between the different sources from which personal data can be taken and makes no distinction between business and private webpages, for example. The only criterion is capacity to identify an individual via those data. However, a parallel can be drawn, in that the law prohibits the intentional infringement of the privacy of others by viewing or sending words spoken in private, or images of a person who was in a place not accessible to the public, or messages sent or submitted in a sealed envelope. Business webpages could be considered as not being private places within the meaning of the law. Employer-sponsored webpages should make clear the privacy rules applicable on the website.

The law does not distinguish between information that can be found by search engines and information that is only available to 'friends' or close contacts. However, these criteria may be ruled on in future. This point is also relevant to the question of access by lawful means.

As regards sensitive data (i.e. racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, including genetic data), one of the authorised exceptions under the Data Protection Act ('DPA') in addition to the data subject's consent, is that the data have been clearly made public by the data subject. Therefore, sensitive data relating to an applicant or employee could not be used by an employer if they had been posted by a third party.

For non-sensitive data, the usual conditions for processing apply. For example, the processing of information which has been posted by third parties could be deemed lawful if it is necessary in pursuance of the legitimate interests of the data controller. However, an applicant or employee can always invoke the protection of his private life and, where applicable, his correspondence, to challenge a decision taken by the employer on these grounds. It should be borne in mind, however, that there is always a risk that information taken from third parties may be unreliable.

5. Consent and works council rights

5.1 Consent

The law does not expressly address the issue of whether the posting of information by employees constitutes consent for employers to use it. However, once made clearly public, personal data are accessible to any current or future employer and can be used, provided the employer processes the data fairly and lawfully, acts without discrimination and ensures the protection of private life (e.g. the employer should consider whether the information found on a social media site should have a real or objective impact on the (future) employment relationship).

5.2 Works council rights

There are no works council information or participation rights.

6. Sanctions

6.1 Regulatory authority and sanctions

The national regulatory body, the CNPD, is empowered by law to sanction data protection non-compliance. Hence, the CNPD is entitled to:

- issue warnings to a failing data processor;
- lock up, erase or destroy data which is being processed in breach of the law;
- temporarily or permanently forbid fraudulent data processing;
- order publication of sanctions imposed on a failing data processor in an official journal.

The CNPD cannot issue fines or criminal sanctions. However, it may notify the legal authorities of any offences of which it is aware and a criminal court could impose criminal sanctions.

The above sanctions are administrative decisions and hence immediately enforceable by their recipient. However, administrative sanctions can be challenged before the administrative courts, which will issue a ruling. If the sanction is upheld it will be enforced in the same way as any other court ruling.

Criminal sanctions are generally a prison sentence of between eight days and one year and a fine of between EUR 251 and EUR 125,000, or one of these penalties. The court hearing the case may also order the cessation of all processing or communication which is contrary to the provisions of the law, subject to a financial penalty.

6.2 How often sanctions are imposed

There are some cases relating to unlawful data processing but none of them addresses the situation where an employer uses personal data posted on social networking media. There are no statistics on the frequency of sanctions imposed in practice. Nonetheless, the annual report issued by the CNPD for 2008 reveals that 63 complaints were filed in 2008 against an average of 32 per year between 2003 and 2007.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are not required to appoint a data protection officer. If there is one, the data protection officer is responsible for establishing and forwarding to the CNPD a register listing the processing operations carried out by the data controller, with the exception of those exempt from notification. Processing carried out by the data controller (other than employee monitoring at the workplace) is exempt from the obligation to notify, if the data controller appoints a data protection official.

The data protection officer should consult the CNPD if in doubt about the compliance of processing under his supervision.

The powers of the data protection officer are as follows:

- investigative powers to ensure the data controller is in compliance with the DPA;
- a right to be informed by the data controller and a right to inform the data controller of what needs to be done to comply with the DPA.

Mexico

1. General use of social media sites

1.1 Popularity of social media sites

According to the social media statistics portal socialbakers.com, the total number of Facebook users in Mexico has reached 28,963,320. Statistics show that Facebook penetration in Mexico is at 25.75% of the country's population and at 94.65% of the number of Internet users.

The LinkedIn demographics for 2011 show that this site has 1.2 million users in Mexico.

It is clear that the importance and penetration of social networks in Mexico is increasing fast.

2. Use by employers

2.1 Use of information from social media by employers

Reliable statistics are difficult to find, but a recent survey carried out by the web site zonajobs.com shows that 45% of Mexican companies use social media as a source of information when hiring personnel.

The most common social networks used for these purposes are Facebook (87%), LinkedIn (36%) and Twitter (27%).

There are no specific statistics showing how often employers make decisions about current employees based on information available in social media.

2.2 Case law about use of information from social media by employers

There is no case law as yet, since the Federal Law on the Protection of Personal Data held by Private Parties (the 'Law') is quite recent and its secondary regulations have not yet been finalised or published. In addition, the Federal Institute for Access to Public Information and Data Protection ('IFAI') has not yet heard any legal actions in relation to this. From January 2012 data subjects will be able to exercise access, rectification, cancellation and objection rights as well as to file data protection proceedings with the IFAI.

To our knowledge, there is no specific legal literature in this regard.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

Our interpretation of the Law is that it does not restrict employers from accessing and relying on any information about an employee or applicant that is publicly available or provided by the employee or applicant, as long as the employee or applicant is duly informed.

When making recruitment decisions the employer must observe all of the data protection principles established in the Law. In this sense, the employer must use fair and legal means to gain access to an applicant's social media posts or content and must clearly inform the applicant of the personal data that it intends to process, the origin of the data and the purposes of the processing.

The general rule is that the employer must obtain the employee's consent to monitor private information, but it is our view that an employer may monitor its employees' social media use if the employee is using employer-owned or controlled equipment or networks and the employer has previously made available to the employee a clear computer usage policy or any other policy by which employees are informed that there can be no expectation of privacy in their usage of the company's systems and that such usage may be monitored at any time by the employer.

During the employment it is also possible to access public information and base employment decisions on that information as long as no discriminatory action is taken against the employee.

In terms of dismissals, the employer will be able to use data posted on social networks only if the use of such data is permitted by law, and provided that the information or the online misconduct is, without doubt, attributable to the employee.

It should be pointed out that the Federal Labour Law does not regulate employers' monitoring activities.

4. Private and public information

4.1 Treatment of private and public information

The Commissioners of the IFAI have stated that social networking sites such as Facebook will not automatically be considered to be publicly available sources.

However, it is our opinion that this particular issue will be solved once the IFAI, the Federal Administrative and Tax Court and the Circuit Courts of Appeal begin to hear these kinds of cases.

The Law does not make a distinction between business, private or employer-sponsored webpages and the nature of the data included on them. However, a publicly available source is a database on which data may be accessed by any person, without any requirement except, where appropriate, payment of a fee.

It is our opinion that the question of whether a distinction should be drawn between private and public information is likely to be determined by the IFAI, the Federal Administrative and Tax Court and the Circuit Courts of Appeals, though this has not yet occurred.

The Law does not make any distinction between information from search engines and information only available to 'friends' but it is one of the reasons why the IFAI Commissioners have stated that if information is only available to 'friends' and prior consent or authorisation has been granted by the data subject to allow these close contacts access to his or her account, this authorisation confirms that the shared information is not publicly available.

If a third party who posts data is considered to be using the data exclusively for personal use and without the purpose of disclosure or commercial use, the processing of such data will not be covered by the Law. However, this will only apply if the processing is done, for example, by a friend of the data subject, in which case there would be no need for the consent of the data subject to the processing, as it would be for domestic and personal purposes.

On the other hand, if the information is being posted by third parties (which may not fit within the meaning of domestic use) without the knowledge or consent of the employee and the employer would like to process the information, it must first inform the employee of this and request consent to the processing. It is important to note, however, that third party posted information may be unreliable, since it could be posted, for example, by an individual who intends to damage the image or reputation of another.

The purpose of the Law is to protect personal data held by private parties, to ensure that it is processed in a legitimate, controlled and informed way which protects the privacy and the right to informational self-determination of individuals, independently of the origin or source of the data.

All data controllers must adhere to the principles of legality, consent, notice, quality, purpose, loyalty, proportionality and accountability under the Law, even if the data have been obtained by a third party.

5. Consent and works council rights

5.1 Consent

The posting of private information would not necessarily be taken as consent to the use by employers of information posted by employees. The consent of the data subject must be clearly given prior to the processing of its personal data by the employer.

The Law defines 'publicly available source' as 'those databases on which data may be accessed by any person, without any requirement except, where appropriate, payment of a fee.'

In this regard, the IFAI has stated that social networking sites such as Facebook will not automatically be considered to be publicly available sources.

5.2 Works council rights

In Mexico there are no information or consultation obligations and there is no need for the employer to inform the union if an employer wants to use information posted on social media before inviting a job applicant.

6. Sanctions

6.2 How often sanctions are imposed

Violations of the Law are punishable by the IFAI by means of:

- warnings or fines ranging from 100 to 320,000 days' worth of Mexico City's minimum wage;
- in the event of repeated breaches, an additional fine may be imposed ranging from 100 to 320,000 days of Mexico City's minimum wage;
- with regard to violations involving the processing of sensitive personal data, the sanctions may be doubled.

Mexico's City minimum wage is of MXN 59.82 (EUR 3.28).

6.2 Regulatory authority and sanctions

Sanctions have not yet been imposed in practice. From January of 2012 data subjects will be able to exercise access, rectification, cancellation and objection rights as well as to file data protection proceedings with the IFAI, which may result in the imposition of sanctions.

7. Data protection officers

7.1 Requirement for data protection officer

The Law provides that all data controllers must designate a person or department responsible for personal data, who/which will process the access, rectification, cancellation and objection applications filed by data subjects and enhance the protection of personal data within the company.

Netherlands

1. General use of social media sites

1.1 Popularity of social media sites

An estimated 3.5 to 4.5 million people in the Netherlands have an active Facebook account, which is equivalent to at least 21% of the population. Around one million Facebook users also have an application for their mobile phone. About 50% of all Facebook users log in on a daily basis. Only Hyves (Dutch version of Facebook, with an estimated 5.5 million active accounts) is more popular than Facebook. LinkedIn is estimated to have 2 to 2.5 million users (15% of the population), with Twitter having 200,000 users. A study of social networking usage in the Netherlands (comScore, Inc., London, 26 April 2011) reveals that the Netherlands ranks first worldwide for penetration of LinkedIn and Twitter (more than one in four Dutch internet users visit these sites during the course of a month).

One remark: reliable statistics are difficult to find, as most social media providers do not disclose their statistics. Moreover, if they do, the basis on which the figures are calculated may differ (e.g. the difference between the total number of accounts and the number of 'active' accounts; and the meaning of the term 'active' account).

2. Use by employers

2.1 Use of information from social media by employers

Reliable statistics are difficult to find and are being tracked mostly by HR support organisations, rather than employers. The results vary widely and claim that up to 70% of employers utilise social media for recruitment purposes. They say that 20% of employers have rejected a future employee as a result of information found about that person on the Internet.

2.2 Case law about use of information from social media by employers

At the time of writing, there is hardly any case law on this matter and virtually no published court decisions. There are some known cases which settled out of court.

There are known examples of messages having been left on social media that have proved that employees who reported sick were not telling the truth. In one case, an employee had reported sick because he had back pains. The suspicious employer checked the employee's Hyves account and found out that the employee had been dancing at a concert. A similar case was that of a football player who was found on a picture at a concert just after he

reported sick for a friendly match of the national Dutch football team, claiming he had concussion. In another case, an employee who reported sick in the morning was seen by her colleague on Facebook later that day drinking wine on a terrace. There have also been examples of negative statements on social media sites that have cost job applicants/employees their jobs. For example, an applicant who wrote on Twitter that 'Cisco has just offered me a job! Now all I have to do is balance the vast salary against doing work I hate' – was denied the job.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

The general rules under the Dutch Personal Data Protection Act (Wet Bescherming Persoonsgegevens, the 'WBP') are that personal data must:

- be processed fairly, lawfully and carefully;
- be obtained only for specified and lawful purposes and must not be processed in any manner incompatible with those purposes;
- be adequate, relevant and not excessive in relation to the purposes for which they are processed;
- not be kept longer than is necessary for those purposes;
- be accurate and kept up-to-date;
- be processed in accordance with the rights of the employees;
- be protected against unauthorised or unlawful processing and against accidental loss and damage; and
- not be transferred to a country outside the EEA unless that country has an adequate level of protection or other strict requirements are met.

Personal data may only be processed with the employee's consent. If there is no consent, processing may be done only if the information is necessary for:

- the execution of a contract with the employee, or to comply with a request by the employee to contract;
- compliance with a legal obligation;
- the protection of a vital interest of the employee;
- compliance with a statute by a managing body or the managing body that is provided with the personal data;
- representation of a justifiable interest of the processor or a third party to whom the data are disclosed, except where the interests or the fundamental rights of the employee, especially his or her right to protection of privacy, prevails.

To process sensitive personal data fairly and lawfully, additional requirements must be met, partly depending on the type of sensitive personal data.

It is generally accepted that employers may access and rely upon all information about employee and candidates for jobs that is publicly available unless it relates to a protected characteristic such as race or disability, or a protected activity, such as union organising.

In the employment context the general requirements are that: the employer must obtain explicit consent and/or the employee must have made the data public him/herself; the processing must be necessary to establish, exercise or defend a legal right in law and the processing must be necessary because of an important general interest. In addition, suitable measures must be taken to protect the personal life of the employee and the processing must be based on a legal obligation or on an exemption by the Dutch Data Protection Committee (the 'College Bescherming Persoonsgegevens', the 'CBP').

An employer may not use fraudulent means to gain access to an employee's social media posts or content if the employee has taken steps to secure the information or otherwise keep it private. The extent to which an employer may monitor its employees' social media use, including private content, will depend on the computer usage policy in place. Most policies aim not to forbid all use of the Internet and/or social media sites but aim to regulate how much usage is permitted and the conditions of that usage.

Whether an employee could be dismissed based on social media information depends on what the information is and whether or not it may be used. Given that many social media pages are publicly accessible and unlikely to involve evidential issues, we are of the view that employers will be entitled to dismiss employees (for urgent cause) based on information found on social media.

4. Private and public information

4.1 Treatment of private and public information

Information posted on social media sites that is unrelated to work will be considered publicly available and not subject to privacy protection under Dutch law unless the employee takes steps to restrict access to the information (e.g. by using a password-protected social media site or privacy settings to restrict access to 'friends only'). As noted above, other Dutch laws, such as anti-discrimination laws, may impose restrictions on the use of publicly available information for employment purposes.

There is no distinction in Dutch law between business webpages, employer-sponsored webpages and private webpages. The WBP protects the processing of personal data, i.e. any information relating to an identified or identifiable natural person and the level of protection of each type of personal data must be established based on the general rules as set out in section 3.1 above.

In addition, the law makes no distinction between information from search engines and information available only to 'friends', but search engine information will be usable by employers, whereas, information only available to 'friends' generally will not.

In terms of the use of information posted by a third party, the general rule that publicly available information can be used, while secured information cannot, would be likely to apply. However, it would be risky for an employer to utilise information about an employee which is posted by a third party because the information may be inaccurate or unreliable.

5. Consent and works council rights

5.1 Consent

The employer can use information posted by the employee not necessarily because it constitutes consent, but because, by voluntarily posting the private information or photos and making them publicly available, the employee no longer enjoys protection under privacy law. Because no expectation of privacy still exists, consent is not required. Consent is not defined in the WBP. However, the definition under the Data Protection Directive is that consent must be informed and freely given. Although recommendable, there is no requirement for consent to be in writing.

The CBP has indicated that the extent to which consent can be relied on by an employer is limited. The CBP considers that it will, in some cases, be difficult to establish that consent has been freely given by employees, because of the balance of power.

An employee's consent for the employer to access information on a password-protected or otherwise restricted social media site would eliminate any claim by the employee for protection under Dutch privacy law. However, other Dutch laws, such as anti-discrimination and labour laws, may limit the employer's ability to use the information.

5.2 Works council rights

Works councils have certain general rights under the Dutch Works Council Act ('Wet op de Ondernemingsraden'). The Works Council Act requires the employer to ask for the consent of the works council to any intended decision to determine, amend or withdraw general regulations regarding the protection of personal data of employees (e.g. a privacy policy). As soon as such a general policy is in place and as long as the employer acts in line with that policy, there is no further role for the works council.

6. Sanctions

6.1 Regulatory authority and sanctions

The CBP imposes the sanctions provided under the WBP. The following sanctions may apply:

- an investigation into compliance with the WBP, with which the responsible party must to co-operate;
- enforcement of an administrative order if the responsible party does not co-operate;
- imposition of an administrative penalty (if a responsible party has breached the WBP, the maximum penalty is currently set at EUR 4,500 for each element of non-compliance);
- criminal proceedings against the responsible party, in which case the penalty may be substantially higher;
- imprisonment;
- publication of the outcome of an investigation (if there is a public interest in doing this).

The practical sanctions, such as entering and inspecting are enforced by the CBP. In the case of threatened imprisonment, the CBP will work with the Public Prosecutions Department.

Fines are imposed by the CBP and can be challenged in a formal objection procedure and a court procedure.

6.2 How often sanctions are imposed

During its first years of existence, the CBP used to be mainly an advisory body. However, over the last years it has changed its focus from advising to enforcement of the WBP. Therefore, more and more sanctions are being

imposed every year. For example, in 2009 the CBP imposed an incremental penalty payment of EUR 120,000 on a Dutch hospital as the hospital had failed to draft a risk inventory of its information security systems on time, despite being ordered to do so by the CBP.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are not (legally) required to appoint a data protection officer ('Functionaris Gegevensbescherming'), but they can volunteer to do so. The data protection officer will see to it that data processing within the organisation complies with the WBP. Should a code of conduct for data processing be in place in the organisation, the data protection officer will also ensure compliance with that code (Article 25 WBP).

Dutch law prescribes that a data protection officer can (after consultation with the CBP) make recommendations to the organisation as to how it can improve data processing. Other duties of the data protection officer are: the handling of complaints, reporting and informing.

Norway

1. General use of social media sites

1.1 Popularity of social media sites

According to a recent survey on social media usage, 2.53 million people (March 2011) in Norway have a Facebook account (approximately 50% of the population) and 420,000 people (January 2011) have a LinkedIn account. Other sites such as Biip and Twitter are also gaining in popularity.

2. Use by employers

2.1 Use of information from social media by employers

To our knowledge, there are no specific statistics available in Norway about the extent to which employers use social media as a source of information about future or current employees, but there are some statistics from Sweden that we think are relevant also for Norway. According to a Swedish survey from 2011, 32% of Swedish companies use Google in their recruitment procedures. In the same survey 20% of Swedish companies use Facebook, Twitter or LinkedIn.

2.2 Case law about use of information from social media by employers

Despite the popularity of social media in Norway, only very little case law regarding employers' use of information from social media exists.

In a court case from 2009, two fishermen were dismissed for alcohol consumption during shore leave and for denying the matter to the employer afterwards. A photo of the fishermen drinking beer in the local pub was posted on Facebook. The employees did not object to the employer's use of the photo as evidence on which to base the dismissals were based. However, the dismissals were found to have been unjustified because of the employer's failure to follow its formal dismissal procedure.

The legal literature deals only very briefly with these issues.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

In general, employers (i.e. data controllers) must comply with the Norwegian Personal Data Act (the 'Act') in processing personal data about a job applicant

or employee (i.e. the data subject) where these originate from social media sites. The collection of non-sensitive personal data is exempt from the general duty of data controllers to report to the Data Inspectorate. However, the employer must: (1) have a justifiable basis for collecting personal data (e.g. it has the consent of the employee or the collection of the data is necessary to safeguard a justifiable interest); and (2) ensure that data are processed fairly and lawfully in accordance with the rules on data processing. The processing operations permitted under the Act depend on the nature of the data and sensitive and semi-sensitive personal data require a greater level of protection; and (3) the employer is obliged to inform the data subject about the information being collected from other sources by it, such as information from social media sites.

Employers have a general duty to not base their decisions on discriminatory reasons, such as race and sexual orientation. However, this duty is not specific to information collected from social media sites.

If the employer wishes to monitor employees' Internet usage at work, it follows from Chapter 9 of the Norwegian Working Environment Act (the 'WEA') that such measures can only be used if it has a justifiable reason for doing so and the monitoring does not place disproportionate strain on the employee. The employer must also comply with the Act by ensuring that it has a specific reason for the monitoring and must report what it is doing to the Data Inspectorate. Further, the employer must discuss all control measures with the employees' elected representatives before implementing the measures.

If an employer wishes to dismiss an employee based on information gleaned from social networking sites, it can do so provided the information is relevant and necessary as part of the dismissal and the processing is in compliance with both the Act and the Civil Procedure Act.

It might also be possible to dismiss an employee on grounds of online misconduct if the misconduct qualifies as a justifiable reason for the dismissal.

4. Private and public information

4.1 Treatment of private and public information

As mentioned above, only very limited case law regarding employers' use of information from social media sites exists. Our view as to whether information posted on social media sites could be said to be publicly available (and thus less protected) is that this could depend on the number of people who have access to it. However, this does not reduce the employer's obligation to act in accordance with the Act.

The Act does not distinguish between private and business-related webpages, or indeed, employer-sponsored webpages. As a result, the level of protection is the same for all webpages if an employer collects information from such sites for business purposes.

The Act applies to the processing of personal data by automatic means and thus does not distinguish between whether data can be found by a search engines or is only available to 'friends' or close contacts.

Employers must give fair processing information to applicants and employees, i.e. it must inform them of the types of data being processed and the purpose of the processing, and explain how their data will be used. This also applies if the data being processed have been posted by third parties. The employer also has an obligation to ensure the quality of any data collected by it. Third party information should therefore be treated with caution, as it may not be reliable.

5. Consent and works council rights

5.1 Consent

Under the Act, personal data may be processed with the data subject's consent. If the data subject has not been asked to consent but the data are publicly available, the employer will normally be justified in processing the data in any case, depending on the circumstances of the case. Posting private information and/or photos will generally not be considered as consent to the use of the information by a future or current employer.

In any event, the employer is obliged to inform the data subject about the information being collected from other sources by it, such as information from social media sites.

5.2 Works council rights

Employers must give fair processing information to applicants and employees regarding the personal data being processed about them. This would include informing them about the types of data being processed and the purpose of the processing, and explaining how their data will be used. Collective agreements may also contain relevant rights and obligations.

6. Sanctions

6.1 Regulatory authority and sanctions

Any person who commits an offence in relation to the processing of data on behalf of private individuals or organisations may be fined or imprisoned for up to three years, at the discretion of the courts. An organisation that commits such an offence may be fined.

The Norwegian Data Inspectorate, for its part, is authorised to:

- keep a register of all personal data processing reported by data controllers;
- handle applications for licences, receive reports and assess whether to give instructions to data controllers;
- ensure compliance with the Act by data controllers and correction of any errors;
- give advice on how to avoid breaching the Act;
- enter and inspect (without a court order).

The Norwegian Data Inspectorate can also impose a penalty for breach of up to (currently) NOK 790,000 (i.e. EUR 98,750), and/or a daily compulsory fine pending compliance.

In practice, there have been very few cases in the Norwegian courts of sanctions being imposed by a court against a data controller. The fines that have been imposed range from NOK 5,000 to NOK 20,000 (i.e. EUR 645 to EUR 2,583). Similarly, compensation has been awarded in very few cases and has amounted to NOK 5,000 (i.e. EUR 645).

6.2 How often sanctions are imposed

The Data Inspectorate made 135 'controls' in 2010. These are the Data Inspectorate's means of regulating compliance with the Act. Controls can either be random spot-checks or in response to information received by the Data Inspectorate of an alleged breach.

Of these controls, 48 serious breaches of the Act were revealed. The Inspectorate gave instructions in 96 of the cases. In at least 4 of the cases, the Inspectorate fined the data controller. The fines were in the range NOK 5,000 to NOK 75,000 (i.e. EUR 645 to 9,884).

7. Data protection officers

7.1 Requirement for data protection officer

Companies are not required to have a data protection officer.

Where data protection officers are appointed, they are charged with improving compliance with the Act within the company. However, the company itself will remain responsible for all processing of personal data.

Peru

1. General use of social media sites

1.1 Popularity of social media sites

Facebook is the social media site with the most penetration in Peru, with 3.7 million people having a Facebook account, representing 12.3% of the Peruvian population. Other sites visited are Twitter, Slideshare, Google+ and LinkedIn. There are 539,000 people with a Twitter account, representing 1.8% of the population. Slideshare has 640,000 users and Google+ has 93,000. Peruvians spend 4.9 hours per month on social media sites and users are increasing each year.

2. Use by employers

2.1 Use of information from social media by employers

There are no statistics regarding the use by employers of social media sites to recruit future employees.

However, employers may find these sites a useful source of information to find out about their current and future employees' behaviour, tastes, preferences and job search interests.

2.2 Case law about use of information from social media by employers

There is no case law or literature about the use of information from social media sites by employers.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

Employers may at any time access personal data about future or current employees posted on social media unless they are addressed only to a restricted list of friends and the employer is not included.

If the employer uses social media sites restricted to friends to breach future or current employees' privacy, the future or current employee may initiate a criminal process for breach of privacy, as contained in Article 154 of the Criminal Code. The employer may be subject to imprisonment if he or she reveals a 'private act'. By Article 154 it is unlawful to breach the privacy of personal or family life by observing, listening to or registering a fact, word, text or image, using instruments, technical processes or other means (i.e., recording a video or uploading a video). The action will only be effective if the data controller (the employer) can be identified. If not, the action will fail.

Employers must comply at all times with the recent Peruvian Law on Personal Data Protection (the 'Law'), which states in Article 1 that the purpose of the Law is to guarantee the fundamental right to protection of personal data based on point 6 of Article 2 of the Political Constitution of Peru, by means of its proper treatment, within a framework of respect for the other fundamental rights contained therein, including good reputation, privacy and honour.

If data obtained by an employer is held on a restricted page available only to certain friends, the employee may allege that his or her privacy has been breached, as Article 13.4 of the Law states that communications, telecommunications, informatic and other systems that are of a private character or for private use, may only be opened or intercepted with the consent of the employee or by order of the court. Personal data obtained in breach of this Article lack legal effect, that is, cannot be used against the employee in an administrative proceeding, including civil or criminal trials.

Personal data may only be processed with the consent of the employee, unless there is authoritative law in this regard, relating, for example, to health or where the personal data derive from a professional relationship of the data controller and its disclosure is necessary for its compliance with the contractual relationship. Consent must be prior, informed, express and unequivocal.

If the employer wishes to monitor employees' Internet usage at work, including social media webpages, the employer must inform the employee that his or her online conduct will be monitored before the monitoring begins.

The Constitutional Tribunal has held that an employee who was dismissed when the employer opened personal emails she had received on her work computer should be reinstated. This suggests caution should be exercised when contemplating dismissing employees on similar grounds.

4. Private and public information

4.1 Treatment of private and public information

Private information posted on social networking sites is considered to be publicly available. However, if the employer accesses information that is restricted to a group of friends in which the employer is not included, the employer may be subject to imprisonment pursuant to Article 154 of the Criminal Code. See section 3.1 above.

The Law does not distinguish business and private webpages and therefore information contained on these websites is considered of public interest and not protected unless the company restricts its access to 'friends only'.

Information found via search engines is available to the public and therefore no consent is required. If available to 'friends only', those not included in the list need the consent of the data subject.

If the data subject does not consent to the employer processing information posted by third parties, he or she can file a claim arguing violation of Article 154 of the Criminal Code.

5. Consent and works council rights

5.1 Consent

The posting of private information is not considered to be consent. Under the Law, data may only be processed with the data subject's specific consent to that processing. However, consent is not required from the data subject if the personal data come from a publicly available source and the employee has agreed to their posting on that source.

Consent is sufficient as long as the processing of the data is done in a way that respects the fundamental rights of data subjects under the Political Constitution of Peru.

5.2 Works council rights

Works councils have no information or participation rights where an employer wants to use information posted on social media before inviting a job applicant.

6. Sanctions

6.1 Regulatory authority and sanctions

The National Authority for the Protection of Personal Data, an office attached to the Ministry of Justice (the 'DPA') will be the competent authority for the protection of personal data and the protection of the rights and obligations established in the Law and a regulation (the 'Regulation') which will be made pursuant to the Law. The Law has been enacted but only certain articles are in force until the Regulation is published. Therefore, the DPA has not yet been created.

The articles of the Law that impose administrative fines for infringements of the Law are not yet in force. The sanctions will be in force once the Regulation has been published and the competent authority created.

No sanctions have yet been imposed under the Law but the courts will apply Article 154 of the Criminal Code and this allows for the possibility of imprisonment for breach of privacy.

6.2 How often sanctions are imposed

No fines have been imposed for non-compliance with the Law and there are no records regarding the application of Article 154 of the Criminal Code, as far as we are aware.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are not required to have a data protection officer.

Poland

1. General use of social media sites

1.1 Popularity of social media sites

Based on unofficial statistics, there are over six million people in Poland who have a Facebook account and according to the most recent survey, 51% of Polish residents spend at least one hour on Facebook every day.

2. Use by employers

2.1 Use of information from social media by employers

There are no reliable statistics about employers' use of social media. To our knowledge, no organisation tracks the frequency of usage of social media by employers to monitor current employees.

2.2 Case law about use of information from social media by employers

Under Polish law employers cannot gain access to social media information by controlling or monitoring employees' Internet activities. Such controlling can be introduced only when it is justified by special circumstances and its scope must be restricted to what is necessary to meet the employer's justifiable aims (e.g. an increase in productivity or the prevention of the disclosure of confidential information). Each employee should be individually informed about the rules relating to the controlling and/or monitoring and its purposes, in particular, any prohibition of the use of business emails for private purposes.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

There is no special regulation of employers' access or reliance on information taken from social media sites. In practice employers may access and rely upon any information about applicants that is publicly available unless it relates to a protected characteristic, such as race or disability; or a protected activity, such as union organising.

As indicated above, the control and/or monitoring of employees' activities cannot be of a permanent character. Any potential sanctions for breach or suspected breach of any employer's computer usage policy should be assessed on a case-by-case basis bearing in mind how effective the policy is, i.e. whether it is clear that employees have restricted rights to privacy in their usage of company systems and that such usage may be monitored by the

employer. Moreover, in the case of breach, the employer may consider the following disciplinary actions: (1) admonition; (2) serious reprimand. Dismissal should be considered on a case-by-case basis.

4. Private and public information

4.1 Treatment of private and public information

Information posted by employees on social media sites unrelated to work will be considered to be publicly available and not subject to privacy protection.

There is no distinction in law between business and private webpages. Polish law does not provide any special protection for information posted on an employer-sponsored webpage.

There is no distinction between information found on search engines and that available only to 'friends' in Polish law.

The consent of the employee will be necessary for the processing of information gained from third parties.

For consent to comply with the law, it must be evident that it was freely given and it must be clear and specific.

5. Consent and works council rights

5.1 Consent

The employer may use information posted by employees, not necessarily because the posting constitutes consent, but because, by voluntarily posting the private information or photos and making them publicly available, the information is no longer considered private and no longer enjoys protection under privacy law. Because no expectation of privacy exists, no consent is needed.

5.2 Works council rights

Works councils have no information or participation rights where an employer wants to use information posted on social media before inviting a job applicant.

6. Sanctions

6.1 Regulatory authority and sanctions

The most common enforcement tool against an employer that violates privacy protection for an employee's social media activity would be a private lawsuit filed by the employee against the employer seeking to recover damages and possibly injunctive relief. The Inspector General for Data Protection may also impose a fine.

The courts would enforce any court-issued judgment against an employer resulting from litigation.

6.2 How often sanctions are imposed

We have no official statistics to say how often sanctions are imposed, but we assume that they are imposed infrequently.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are obliged to appoint an administrator of information security to ensure the security principles are upheld.

Portugal

1. General use of social media sites

1.1 Popularity of social media sites

Social media are very popular in Portugal, specially Facebook and LinkedIn. Figures collected from the website www.socialbakers.com, show that 4,081,460 people in Portugal have a profile on Facebook. A survey conducted at the end of 2010 also showed that more than 400,000 people in Portugal use LinkdIn and this number is likely to have increased in the course of 2011.

2. Use by employers

2.1 Use of information from social media by employers

To our knowledge, there are no specific statistics available about the extent to which employers use social media as a source of information about future or current employees, but the figure is without doubt rising.

2.2 Case law about use of information from social media by employers

Despite the popularity of social media in Portugal, to our knowledge there is no case law on social media, and therefore none on the use of information from social media sites by employers. The same is true of the legal literature, although this theme is commonly discussed in seminars.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

In general, employers (i.e. data controllers) may process personal data on an applicant or employee (data subject) that originate from social media. In addition, employers, just as any other user, may access information made available on social media sites.

Data controllers must, however, at all times comply with the Portuguese Data Protection Act (the 'Act'). This means that data must be processed fairly and lawfully in accordance with the rules on data processing. The processing operations allowed under the Act depend on the nature of the data and sensitive personal data require a higher level of protection.

If the employer wishes to monitor employees' Internet use at work, including social media webpages, the employer must inform employees that their online conduct will be monitored before the monitoring begins.

In terms of dismissals based on social media usage, it is our view that although this matter is not directly addressed in law, employers will generally be able to use data from social media sites if they are relevant and necessary to the dismissal and are job-related.

4. Private and public information

4.1 Treatment of private and public information

In general terms, private information posted on social networking sites will be considered to be publicly available. However, there is no clear threshold for determining whether the information is or is not public.

It can nevertheless be inferred that if an employee posts private information and/or photos on a social networking site, it may be viewed by an undetermined number of people (depending on its level of accessibility). This amounts to an implied authorisation, the effect of which is that the data subject may not reasonably argue that the employer is breaching his or her privacy. This would mean that the employer could use the information provided it does so in a proportionate and legitimate way.

The Act applies to the processing of personal data by automatic means and does not distinguish whether the webpage is private, business-related or employer-sponsored. As a result, the level of protection is the same for all webpages.

Nor does Portuguese law distinguish whether data can be found by a search engine or whether it is only available to 'friends' or close contacts. In practical terms, however, it should be noted that in terms of sensitive data, the Act allows data controllers to process data of this kind if they have been made public by the data subject.

Employers must give fair processing information to applicants and employees, i.e. inform them of the types of data being processed and the purpose of the processing, and explain how their data will be used. This also applies if the data being processed have been posted by third parties. However, please note that employers should be cautious of third party data, as they may be unreliable.

5. Consent and works council rights

5.1 Consent

Under the Act, data may be processed with the data subject's consent. If the data subject has not been asked to consent, but the data are publicly available, the employer will normally be justified in processing the data, but this will depend on the specific circumstances of each case. In addition, however, it must be 'necessary' for the employer to process the data.

5.2 Works council rights

There are no works council information or participation rights for employee representatives where an employer wants to use information posted on social media before inviting a job applicant.

6. Sanctions

6.1 Regulatory authority and sanctions

Under the Act, data controllers must compensate any harm caused by data processing in breach of the Act unless it is established that it could not have been avoided through adequate diligence and care.

The Portuguese Data Protection Agency is authorised to:

- enter and inspect (without a court order);
- issue (public) opinions;
- bring an action against a data controller for failure to comply with the Act or the Agency's opinions;
- apply fines for non-compliance.

Failure to register data processing with the Agency may result in a fine ranging from EUR 1,496 to EUR 14,963.

Negligence is punishable by one year's imprisonment or a 120 day fine (calculated in accordance with the law, i.e. depending on the nature of the infringement and the economic capacity of the infringer). These sanctions may also be applied to a data controller that intentionally:

- omits to notify the Agency of a request to process data (in cases where this is necessary);
- supplies false information when making a request;
- fails to meet a deadline set by the Agency for compliance with its obligations.

6.2 How often sanctions are imposed

The Agency often issues opinions and criticises data controllers, but only very few and minor fines have been imposed for non-compliance with the Act.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are not required to have a data protection officer.

Russia

1. General use of social media sites

1.1 Popularity of social media sites

According to research conducted in the spring of 2010 by Rose Creative Strategies (together with Head Hunter, one of Russia's leading Internet recruitment companies) 89% of Internet users in Russia have accounts on social media websites. Moreover, 49% of them spend about five to ten hours a month on social media sites and 23% spend more than 20 hours a month. There are about 75 million accounts on Vkontakte and 45 million on Odnoklassniki (the two most popular social media sites in Russia) and there are around one million Facebook accounts. Further, 31% of Internet users already have an account on Facebook.

2. Use by employers

2.1 Use of information from social media by employers

There is not much official statistical information available with respect to the use of social media as a source of information about employees.

However, social media sites are becoming an increasingly popular tool for obtaining extra information on job applicants, but employers rarely use such data as a reason for refusing to hire a candidate because to do so would be unlawful.

According to available information 57% of Russian companies claim to use social media to advertise jobs (research conducted by Head Hunter in September 2010). The disadvantages that are identified by employers are the need to spend more time in order to find candidates using social media and the fact that candidates do not necessarily have the required level of qualification. The most popular media for hiring purposes is Moikrug.ru and 25% of HR specialists say they use Odnoklassniki, LinkedIn and Vkontakte for recruitment purposes.

2.2 Case law about use of information from social media by employers

No rules for using social media sites in the workplace have yet been established in law.

Employers should be cautious when using information taken from social media sites, i.e. when making decisions basing on information from social media, both for recruitment and disciplinary purposes. For example, dismissal is

lawful only upon grounds stipulated by law and in compliance with established procedures.

There is only one relevant case, in which an employee was dismissed for repeated failure to perform her duties. The employee was dismissed because she spent most of her working time on social media sites for private purposes and therefore failed to do her job.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

The law permits employers to access and rely on all information about an employee that is publicly available.

When making recruitment decisions, the employer can access and rely on information at its own risk, but may not refuse to hire on the basis of negative information published about the employee (by himself or third parties) on social media sites.

The employer may access and rely on information as a form of monitoring during employment for information purposes only. It is unlikely that such information could be used for making employment decisions. For example, an employee could not be dismissed purely because misconduct was made known to the employer on a publicly available web site, as there would need to be additional evidence against him or her. An employee may only be dismissed on certain grounds and in compliance with established procedures.

An employer may not use coercion or fraudulent means to gain access to an employee's social media posts or content if the employee has taken steps to secure the information or otherwise keep it private. Even if the employer has a clear and very detailed policy on the use of company equipment (e.g. stating that employees should use company email and equipment only for business-related purposes; that private emails and other use of company property is prohibited; and that the employer may monitor employees' emails and activity in order to ensure compliance with the policy), this does not eliminate the risk that an employee may claim breach of his or her constitutional right to secrecy of private correspondence.

4. Private and public information

4.1 Treatment of private and public information

Information posted on social media sites will be considered to be publicly available, but all general legal requirements (e.g. relating to consent) will still apply. Generally, for employment purposes, photos and/or information posted on social media sites will not provide grounds for termination of employment.

The law does not make a distinction between information published on public, private or employer-sponsored webpages.

Nor does the law distinguish between information that can be found by search engines and information that is only available to 'friends' or close contacts.

In terms of information posted by third parties and used by the employer, this may be inaccurate and incomplete and it may be hard to define the source of information. In those circumstances, it could be risky for the employer to use it.

The Labour Code of the Russian Federation stipulates that the employer should receive all personal data from the employee. If personal data are received from a third party, the employee should be notified of this fact and his or her prior consent obtained.

5. Consent and works council rights

5.1 Consent

The act of uploading photos or information cannot be regarded as consent for use of the photos and information. In some circumstances, publicly available photos and information, duly certified by a notary following a specific procedure, can be used by the courts as indirect evidence. However, making photos publicly available does not automatically mean consent to their use. For example, the use of an individual's picture almost always requires his or her consent, except as provided by law.

5.2 Works council rights

There are no specific provisions in Russian law with regard to information or participation rights for the works council.

6. Sanctions

6.1 Regulatory authority and sanctions

Individuals are subject to administrative, disciplinary, civil, criminal and other types of liability as stipulated by the law of the Russian Federation for breach of data protection requirements. Companies (as legal entities) are subject to administrative sanctions. Administrative liability is usually imposed in the form of administrative fines both on the company and its officials.

Disciplinary liability may be imposed on employees and may be in the form of a warning, reprimand or dismissal (although dismissal is only possible in certain circumstances envisaged by law).

Criminal liability may be imposed only on individuals and may be in the form of a fine, complusory service, arrest or imprisonment. The individual may also be deprived of the right to hold certain positions.

The sanctions may be enforced by different state authorities depending on the type of breach, for example, in terms of data protection, the Federal Service for Supervision in the sphere of communications, information technology and mass communications; in terms of privacy and secrecy of correspondence, the court and law enforcement agencies, such as the police.

6.2 How often sanctions are imposed

At the time of writing, there have been only a very limited number of cases in which employees or administrative agencies have obtained sanctions against an employer based on the employer's access to, or use of, information on social media sites for employment purposes.

7. Data protection officers

7.1 Requirement for data protection officer

Employers are obliged to protect the confidentiality of personal data of their employees, and must determine who is given access to the personal data (e.g. HR, payroll and security).

Moreover, employers must undertake measures which are necessary and sufficient to ensure the fulfillment of the obligations of personal data operators. By law such measures may include appointing a person responsible for arranging personal data processing.

If there are breaches of the data processing rules, the responsibility will be borne by the appointed responsible person and/or by the company, as the legal entity. In the absence of an appointed responsible person, the responsibility will probably be imposed on the head of the Company.

Spain

1. General use of social media sites

1.1 Popularity of social media sites

According to the latest data provided by Facebook, there are nine million users in Spain (out of a total of 46.7 million inhabitants). The largest group of users are between 25 and 34 years old, followed by those 18 to 24 years old.

Facebook is the most widely-used network. Other popular sites include YouTube, Tuenti and Twitter. LinkedIn is the fifth most used social network.

2. Use by employers

2.1 Use of information from social media by employers

There are few reliable statistics. Some studies by consulting firms have estimated that 49% of companies use social networks to select and recruit candidates.

In particular, companies are using professional social networks like LinkedIn or Xing.

According to certain surveys, social networks such as Facebook are used to verify information obtained in job interviews, or even when the employee already has the job.

2.2 Case law about use of information from social media by employers

There are no court cases that explore how companies use social networking sites.

By contrast, there are a large number of court cases about the use and monitoring of, for example, employees' email and computers.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

There are no specific provisions in law on the use of social networks for the selection, control and dismissal of employees.

However, there are general laws about Internet services (Law 34/2002 on the Information Society and electronic commerce) and personal data protection (Law 15/1999 on Data Protection).

Theoretically, employers could access any publicly available information and use it if it is professionally relevant to selection, recruitment or the implementation of disciplinary measures. Social networks such as LinkedIn are specially designed for some of these professional purposes.

4. Private and public information

4.1 Treatment of private and public information

There are no cases on whether posted information is considered to be publicly available but if the information is accessible to all, based on the consent of the user of the social network, the data will be less well-protected than private data would be. There are no legal references to the use of information posted on social networks by employees.

However, there are several court cases concerning the private use of the Internet at work which suggest that limited use is allowed and does not constitute breach of the employee's duties.

The law does not distinguish between information from search engines and that available only to friends, and there are no court cases on this issue. However, in our opinion, information that is only available to 'friends' or close contacts would be better protected or considered to be private.

There is no statute or case law on the use of information posted by third parties by employers, but our assumption is that the information could be used if it is publicly available and relates to professional matters.

5. Consent and works council rights

5.1 Consent

The employer can use information posted by employees, not necessarily because the posting constitutes consent, but because, by voluntarily posting the private information or photos and making it publicly available, the information is no longer considered to be private.

However, the use of sensitive personal data, such as those related to ideology, religion, health and sex life is unlikely to be permitted.

5.2 Works council rights

There are no information or participation rights for works councils where an employer wants to use information posted on social media before inviting a job applicant.

6. Sanctions

6.1 Regulatory authority and sanctions

The Law on Data Protection, and the Spanish Agency for Data Protection (the 'AEPD'), regulate the processing of personal data, because of their link to civil liberties and the fundamental rights of individuals.

The AEPD monitors breaches of data protection, with a group of inspectors. They can impose monetary fines ranging from EUR 900 to EUR 600,000, depending, for example, on the severity of the offence, whether it was continuous, any benefit obtained as a result of it and, harm to the data subjects or third parties.

AEPD decisions can be appealed to the courts. If the company does not pay the fine and does not appeal to the courts, the AEPD can start an enforcement procedure involving, for example, seizing the money from the company's bank accounts.

6.2 How often sanctions are imposed

The AEPD is very active and penalties are commonplace. However, there is no precedent for a sanction relating to the use of social networks by companies.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are not required to have a data protection officer. However, they must comply with the Law on Data Protection.

Today, there are many consulting firms in the field of data protection and in practice companies sometimes use consultants to do the job of a data protection officer.

Switzerland

1. General use of social media sites

1.1 Popularity of social media sites

According to the latest statistics available in specialised literature, currently almost three million people (approximately 43% of the Swiss population) use Facebook in Switzerland. The number of users is constantly increasing. Other social media sites such as Twitter and LinkedIn are far less popular. According to the same statistics, Twitter has currently approximately 250,000 users in Switzerland and LinkedIn only approximately 150,000.

2. Use by employers

2.1 Use of information from social media by employers

Reliable statistics are difficult to find. A wellknown Swiss market research institute has recently published a survey conducted among the largest publicly listed Swiss companies. The results showed that approximately 62% of employers use social media, but it was unclear what the term 'use' covered. It may be that employers use social media for marketing and other purposes, rather than only as a source of information on future or current employees. According to the survey, 45% of employers that use social media are primarily active on Facebook. Only 22% of employers that use social media indicated that they had a sophisticated social media strategy (e.g. marketing, branding and recruitment). According to the Swiss Federal Data Protection and Transparency Commissioner's ('FDPTC') website, two thirds of HR managers would use social media and Google to obtain information on job candidates. It does not, however, specify whether this percentage only refers to employers based in Switzerland.

2.2 Case law about use of information from social media by employers

There is still very little legal literature and no supreme court decisions dealing specifically with the use of information from social media sites by employers. However, there are various decisions relating to Article 328 of the Swiss Code of Obligations ('CO'), which requires the employer to protect the employee's personality and privacy, and Article 328b of the CO, which, as a matter of mandatory law, sets out the principles based on which employers may process personal data relating to employees.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

Generally speaking, any processing of personal data must comply with the general principles set out in the Swiss Federal Data Protection Act ('DPA'), such as the principles of good faith, proportionality and transparency. Generally, there is no infringement of the personality if the data subject has made the data available to any third party and has not objected to their processing (Article 12 paragraph 3 of the DPA). Article 328b of the CO further provides that employees' personal data may be processed by the employer only to the extent that they are necessary for the performance of the employment contract or if the data relate to the employee's ability/suitability to perform his or her job (e.g. diplomas, certificates, references and appraisals).

During the recruitment process, case law prohibits employers from asking questions to candidates that do not relate to the job (e.g. questions on origin or religion), but whether a particular question is acceptable will always depend on the circumstances of the case. As a general rule, these principles should apply to the use of information from social media as well. Therefore, some legal authors are of the view that the case law noted above should apply to the use of information from social media, i.e. if an employer may not ask certain questions (unrelated to the job) during an interview, it may not lawfully obtain this information by using social media. In any event, an employer must not use coercion or fraudulent means to gain access to a candidate's social media posts or content, especially if the latter has taken steps to secure the information or otherwise keep it private. The employer should, however, be entitled to access and rely on information posted on social media if the applicant has referred to, say, his Facebook profile in the application documents on his own initiative.

During employment, whether the employer can access or rely on information from social media as a form of monitoring will however depend on several factors, for example, whether the private use of social media at work is permitted; whether the employer has issued a policy on the subject; whether the employees have been advised in advance of possible monitoring; and how the monitoring is conducted. The purpose of the monitoring is also important in this respect: measures taken by the employer should not be exclusively aimed at monitoring the employees' behaviour at work, but should rely on another business-related ground (e.g. security).

Dismissal could be permitted under certain circumstances, in particular if the employer discovers, amongst information that is publicly available, that an employee has made negative statements harming the employer's reputation or if the employee has disclosed know-how or trade secrets.

4. Private and public information

4.1 Treatment of private and public information

The question of whether information posted on social networking sites is considered to be publicly available has not yet been settled by case law and is debated among legal authors. The general rule is that there is no infringement of the personality if the data subject has made the data available to any third party and has not objected to their processing (Article 12 paragraph 3 of the DPA). The fact that private information or photos have been posted on social media sites does not automatically mean that these data should be considered as publicly available and hence are not protected at all. The issue should be assessed on a case-by-case basis and will depend on the circumstances, such as whether the employee has taken steps to restrict access to the information or otherwise keep it private (e.g. by using a password-protected social media site or privacy settings to restrict access to 'friends only'). If this is the case, the information should remain private. The content and context of the posting will also play a role, for example the nature of the website (i.e. professional networks as opposed to social media) or the intention of the person posting the information, provided this is apparent to third parties. In the employment context, some authors are of the view that the use of information by the employer will be lawful only if it remains within the initial purpose and framework contemplated by the employee when he posted the information, which may not be the case if it was posted on websites aimed at sharing private information or photos with a limited number of people.

Swiss law does not expressly make a distinction between business webpages and private ones, but legal literature does. If an employee posts information on publicly available business web pages, the employee's consent to the use of such information in a business context (i.e. by a future or current employer), can be presumed.

Because blogs contain information that the blogger has made publicly available, they are likely to be less well protected than information that is posted on other webpages that can only be accessed by a restricted number of people. That being said, the use of private information by the employer will be restricted by the general principles of the DPA (e.g. good faith), by Article 328b of the CO and by the context of the posting.

The legal literature does make a distinction between information found on search engines and information for 'friends only'. Information that is only available to 'friends' or close contacts should generally be considered as private and the employer should not be entitled to use it. However, this does not mean that information that can be found by search engines will not be protected at all.

In terms of whether employers can use information posted by third parties, this question has not yet been settled. In any event, the risk of breaching the (future) employee's privacy is much higher with third party information. It would also be very risky for an employer to rely on such information since it could very well be entirely inaccurate.

5. Consent and works council rights

5.1 Consent

The general rule is that there is no infringement of the personality if the data subject has made data available to any third party and has not objected to their processing (Article 12 paragraph 3 of the DPA). Although the question of whether posting is considered to be consent has not yet been settled by case law, some legal authors consider that the posting could only be regarded as consent by the data subject to the use of this information by a future or current employer if it was posted for such use. This could be presumed for information posted on professional networks and/or recruitments websites such as LinkedIn. If the employee posts such information on websites that focus on sharing private information with friends or a limited circle of people, the posting may not be considered to be consent per se.

Any use of personal data must also comply with the general principles of the DPA, and, in particular, with the requirements set forth in Article 328b of the CO.

5.2 Works council rights

There are no specific information or participation rights owed to the works council.

6. Sanctions

6.1 Regulatory authority and sanctions

Generally speaking under the DPA, the FDPTC only has limited monitoring powers vis-à-vis private persons:

- He may advise private persons in relation to data protection.
- He may open an inquiry (fact-finding) either upon his own initiative or upon request when: (i) a method of processing is likely to harm the personality rights of a substantial number of persons; (ii) data files must be registered; or (iii) there is an information duty in the case of a cross-border transfer of data. Within the framework of such an inquiry, the FDPTC may ask for information and require to be provided with documents or other evidence.
- After an inquiry, the FDPTC may also issue non-binding recommendations (aimed at modifying or ceasing specific data processing).
- If a recommendation is not followed, he may bring the case to the Federal Administrative Tribunal, which will reach a decision. If the data subject is likely to suffer harm that will be hard to remedy, the FDPTC may also seek injunctive relief before the Tribunal.

The DPA further provides for the following criminal sanctions:

Upon a complaint, individuals may incur a fine if they intentionally:

- do not comply with the obligations laid down in Articles 8 to 10 of the DPA (e.g. the obligation to grant access to the file) and in Article 14 (i.e. information duty when collecting sensitive data or personality profiles) by providing inaccurate or incomplete information;
- omit to inform the data subject as required by Article 14 paragraph 1 of the DPA or to provide the data subject the information required pursuant to Article 14 paragraph 2 of the DPA.

Individuals may also incur a fine if they intentionally:

- omit to inform the FDPTC as required by Article 6 paragraph 3 of the DPA (i.e. information duty in the case of cross-border transfer of data) or omit to register their data files with the FDPTC as required by Article 11a of the DPA or provide inaccurate information when registering such files;
- provide the FDPTC with inaccurate statements or refuse to collaborate in the context of an inquiry.

Data subjects are also entitled to bring a civil claim (including asking for injunctive relief) against the data controller to protect their rights under the DPA.

The FDPTC has no authority to impose a sanction, let alone a criminal sanction. The FDPTC may only bring certain administrative claims against a data controller to the Federal Administrative Tribunal.

Fines, if any, are imposed by the competent local criminal authorities. The maximum fine that can be imposed is CHF 10,000 (EUR 8,083) in the case of a severe violation.

Civil claims may be initiated by the data subject (e.g. for infringement of privacy rights, correction or deletion of data, prohibition from disclosing data to third parties and damages). Such claims must be brought before the competent local civil courts against the data controller. The Federal Act on Civil Procedure applies.

6.2 How often sanctions are imposed

According to information available on the FDPTC's website, the FDPTC issued in 2009 at least three non-binding recommendations (including one to Google). He further commenced at least three sets of judicial proceedings before the Federal Administrative Tribunal (one of which was directed against Google). According to legal scholars, one criminal investigation was opened at one stage, but thereafter closed.

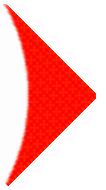
Taking into account the importance of data processing in the employment context, it is safe to say that severe sanctions in individual cases are rarely imposed.

7. Data protection officers

7.1 Requirement for data protection officer

Swiss data protection legislation does not provide a mandatory requirement for companies to appoint a data protection officer. Nevertheless, larger companies often do appoint a data protection officer, as this has certain advantages. In particular, companies with a data protection officer are exempt from registering their data files with the FDPTC (Article 11a paragraph 5 of the DPA).

United Kingdom



1. General use of social media sites

1.1 Popularity of social media sites

Social media sites are extremely popular in the UK:

- over 30 million UK adults use Facebook regularly;
- 32.1 million UK adults use YouTube regularly;
- 15.5 million UK adults are on Twitter; 7.9 million UK adults are on LinkedIn; and 6.7 million UK adults use Flickr.

(Source: http://www.umpf.co.uk/blog/social-media/social-media-usage-in-the-uk-the-findings).

2. Use by employers

2.1 Use of information from social media by employers

Careerbuilder.co.uk report that in 2008 22% of employers reviewed the social media sites of applicants as part of the recruitment process. This rose to 45% in 2009, with Facebook and LinkedIn being the most popular sites. Just 7% reviewed Twitter feeds. In terms of the industry sectors that screen potential applicants the most, these would appear to be IT (63% of those surveyed) and professional services (53%). By the start of 2010 the number of employers reporting using social media to screen applicants had risen to 53%.

Of those employers that used social media to screen applicants 43% reported finding content that caused them not to hire candidates, with the most common reasons being that they lied about their qualifications or showed poor communications skills. Conversely, 50% reported that viewing social media sites caused them to recruit because they provided evidence of their qualifications or demonstrated good communication skills.

2.2 Case law about use of information from social media by employers

Case law on dismissal arising from online misconduct is beginning to develop. If what is alleged constitutes a clear case of misconduct, such as harassment of a fellow employee using the employer's equipment, then the fact that the conduct occurs online will not have an impact on the fairness of the dismissal and the employer can use the information found online to justify the dismissal.

The most difficult areas are where the conduct takes place on the employee's own equipment in his or her own time or where the employer asserts that the employee's online conduct damages or has the potential to damage the employer's reputation.

In relation to the first concern, an employer can be liable for the acts of its employees even if they take place outside the workplace. For example, where comments are made by the employee about another employee that constitute harassment, the employer will need to take disciplinary action because the tribunals apply a very wide test as to what constitutes acting 'in the course of employment'.

In the second case (damage to reputation) dismissal can be difficult. The factors that would support a dismissal include (1) whether actual damage occurs or the threat of damage is material and tangible. There is one case where the Tribunal took into account the number of hits on the website and, because the number was very low, did not accept the employer's evidence concerning the threat to its reputation posed by the footage posted; (2) the severity of the conduct; (3) the steps taken by the employer to put in place clear rules about the use of social media and to communicate acceptable behaviours to staff; (4) the employee's role and responsibilities; and (5) the impact that the online information has on the employee's ability to do his or her job effectively.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

Data protection laws and guidance are relevant. In the UK the relevant legislation is the Data Protection Act ('DPA') and the Employment Practices Data Protection Code (the 'Code').

When an employer consults online information to glean more about a job applicant it is 'processing' that information. If the employer discovers conduct that may influence its decision then the employer should consider the general principles set out in guidance published by the Information Commissioner's Office ('ICO') for employers in the form of the Code. This does not specifically address the issue of the use of online information (and significantly, the ICO has not yet published specific guidance) but Part 1 of the Code does address vetting and verification exercises. The Code requires the employer to tell job applicants/employees what checks it undertakes, indicating that checks should only be undertaken at a late stage in the recruitment process, and the candidate should be given the opportunity to comment on the accuracy of the data obtained.

The Code also deals with monitoring. At a general level any monitoring should be proportionate to the risks faced by the employer. Continuous monitoring e.g. to monitor productivity is rarely justified. Most employers would struggle to defend monitoring of this nature if it was done on a routine basis rather than when grounds for concern had been raised and as part of an investigation into those issues. Employees should also be given information about the employer's monitoring activities telling them about what will be monitored, when and how, where the information obtained as a result of the employer's monitoring will be stored and so on.

If an employer relies on such information to dismiss for online misconduct the factors that would support a fair dismissal would include (1) whether actual damage occurs or the threat of damage is material and tangible (there is one case where the Tribunal took into account the number of hits on the website and, because the number was very low, did not accept the employer's evidence concerning the threat to its reputation posed by the footage posted); (2) the severity of the conduct; (3) the steps taken by the employer to put in place clear rules about the use of social media and to communicate acceptable behaviours to staff; (4) the employee's role and responsibilities; and (5) the impact that the online information has on the employee's ability to do his or her job effectively.

Finally it would be relevant to consider what the employer had told employees about the online monitoring that it undertook and as such, whether the employer was in compliance with its obligations under the 'DPA'.

4. Private and public information

4.1 Treatment of private and public information

Early cases under the ECHR did suggest that if the employee put personal information in the public domain then he or she had lost the right to privacy pursuant to Article 8. Later European Court of Human Rights cases have suggested, however, that the issues are not so straightforward. The most relevant case is *Pay v United Kingdom* [2009] which involved sado-masochistic photographs being posted online. Mr Pay was the subject of the photographs, although his face was hidden. He had not authorised the posting of the images. The argument was that he had engaged in those activities in public (in a private members' club). The Court found that he had not lost his right to privacy (although they said his dismissal was a proportionate response by the employer because of the connection between his job as a probation officer dealing with sex offenders and his own conduct and its impact on his ability to do his job effectively).

In a case involving the covert filming of an employee the employee had not lost his Article 8 right to privacy simply by walking down a public street. By analogy the Internet should be no different and the context in which the information is made available will be very relevant.

One of the most recent cases on the subject however is a first instance decision concerning a chain email that the employee instructed should be 'forwarded on'. In those circumstances the Tribunal decided that the employee had not intended the communication to be private because he had instructed that it could be sent to an unknown audience.

An even more recent case finds that an employee could have no expectation of privacy for posts made on Facebook because of their potential to be forwarded on to friends of his friends.

The DPA does not deal with privacy per se but the protection of personal data. This means that to comply with the DPA certain steps must be taken for fair and lawful processing to occur. The requirement for fair and lawful processing requires employees to be told when and how online information will be viewed, although when it comes to sensitive personal information the additional protection that is generally applicable to the processing of such data does not apply if the data subject deliberately makes the information public. These additional requirements apply to the justification of the employer's actions in processing the data and do not affect the employee's rights to be given information about the employer's processing activities. Furthermore, what is public for these purposes is not clear and has not been determined by the courts.

There is no case law on whether there is a distinction between business and private webpages. However, it is likely that there would be a distinction where the information is contained on employer-sponsored webpages because the employee does not have the same expectation of privacy and because the employer can give specific information to the employee about its processing of that information to comply with the first data protection principle. Similarly, distinctions may be drawn between LinkedIn and other media where the expectation is that the user's profile will be reviewed by potential employers.

There is no case law as to whether there is a distinction between search engine information and information available only to 'friends'. However, we are beginning to see the Employment Tribunal making a distinction between posts which the employee has made on Facebook where the employee should have no expectation that they will remain available only to his friends and information found on search engines, where it is arguable that the employee could have an expectation of privacy. If the information was retrieved by trawling search engines across a number of sites, the employee may argue that he has an expectation of privacy because he was not aware that information could be found or used in this way.

As explained, above, Mr Pay did not lose his right to privacy because information had been posted online without his consent. The employer was however still able to rely on it because of the impact of what the information revealed on his job. However, as a general rule information posted by others may be unreliable and an employer should always test its accuracy.

5. Consent and works council rights

5.1 Consent

The question of consent has not been conclusively settled by the English courts but it is likely that an employee would not be considered to have given his or her consent simply by posting information on the Internet. Of relevance here is the employee's right to privacy under Article 8 of the European Convention on Human Rights (the 'ECHR') and the employee's rights under the DPA.

Overall, if the employer informed the employee that it would be reviewing online information and expressly sought and obtained the employee's fully informed consent, this would be sufficient. The employer should also consider whether it is able to satisfy the requirement for the processing to be proportionate (i.e. in pursuance of a legitimate aim and reasonably necessary to achieve that aim).

5.2 Works council rights

There are no information or participation rights for works councils where an employer wants to use information posted on social media before inviting a job applicant.

6. Sanctions

6.1 Regulatory authority and sanctions

The courts and the ICO are the bodies with sanctioning powers. Most significant are the ICO's powers under the DPA. The following sanctions may be made:

- Undertaking – the ICO may require data controllers to sign a formal undertaking, pledging to take certain steps to prevent further data protection breaches.
- Information notices – the ICO may require data controllers to disclose information relating to their processing procedures.
- Assessment notices – the ICO makes an assessment regarding whether a data controller has complied with the DPA.
- Enforcement notices – in the most serious cases, the ICO requires data controllers to take steps to comply with the data protection principles.
- Power of entry, inspection and seizure of documents (subject to a court order).
- Imposition of a fine (up to a maximum of GBP 500,000) where data controllers knowingly or recklessly commit serious breaches of the DPA.

Data controllers that breach the DPA, may be liable to:

- a fine of up to GBP 5,000 upon summary conviction in the magistrates' court and an unlimited fine if convicted on indictment in the crown court (this course of action is unusual);
- direct imposition of a fine by the ICO (of up to GBP 500,000), without a court order (pursuant to new powers granted under s144 Criminal Justice and Immigration Act 2008 in the new Section 55A of the DPA, which recently came into force).

6.2 How often sanctions are imposed

Sanctions are imposed more frequently now than in the past. The ICO has recently served two organisations with the first monetary fines for serious breaches of the DPA. The ICO is able to impose such fines without a court order and it is therefore likely that the ICO will be utilising these with increasing frequency.

7. Data protection officers

7.1 Requirement for data protection officer

There is no requirement for a data protection officer, although it is advisable for larger organisations to appoint a senior employee to oversee its organisation's compliance with the DPA and it is increasingly common for them to do so.

1. General use of social media sites

1.1 Popularity of social media sites

According to Goldman Sachs, an investment bank seeking capital contributions for a possible initial public offering for Facebook, 149 million people in the United States have a Facebook account, which is the equivalent of roughly 42% of the US population. Other sites such as LinkedIn, Twitter and MySpace do not disclose statistics delineating the number of US subscribers. Yet, according to the most recent survey, US residents spent 23% of their Internet time on social media sites – more than three times as much time as they spend on email. This figure is a 43% increase in usage over the previous year.

2. Use by employers

2.1 Use of information from social media by employers

Reliable statistics are difficult to find and are mainly being tracked by HR support organisations rather than employers. The results vary widely and claim that anywhere from 24% to 36% of employers regularly utilise social media for hiring or recruiting purposes. To our knowledge, no organisation tracks the frequency of usage of social media by employers to monitor current employees. However, in 2009, one in nine employers had terminated an employee for social media-related misconduct, up from 1 in 16 the year before.

2.2 Case law about use of information from social media by employers

Employers must exercise caution when imposing discipline based on social media-related conduct. One case recently upheld a jury verdict on a claim for privacy violations where an employer terminated two employees after accessing their restricted MySpace page. The National Labor Relations Board (the 'NLRB') is actively pursuing complaints against employers which allege that discipline based on an employee's social media activity has violated the federal National Labor Relations Act. The Act protects employees, whether in a unionised workplace or not, who communicate with co-workers about the terms and conditions of employment. In at least one case, an administrative law judge reversed the terminations of several employees, finding that the discipline violated the Act.

3. Employer access

3.1 What the law says about accessing and relying on information from social media

The law permits employers to access and rely upon all information about applicants and employees that is publicly available unless the information relates to a protected characteristic, such as race or disability, or a protected activity, such as union organising. An employer may not use coercion or fraudulent means to gain access to an applicant's or employee's social media posts or content, where the employee has taken steps to secure the information or otherwise keep it private. However, an employer may monitor its employees' social media use even with respect to private content if the employee is utilising employer-owned or controlled equipment or networks and the employer has a clear, well-written computer usage policy informing employees that they have no right to privacy in their usage of company systems and that such usage may be monitored at any time by the employer.

Employers can rely on such information to discipline employees as long as the information is not protected, for example, by the National Labor Relations Act or laws prohibiting discrimination based on genetic information.

4. Private and public information

4.1 Treatment of private and public information

Information posted on social media unrelated to work will be considered publicly available and not subject to privacy protection under US law unless the employee takes steps to restrict access to the information (for example, by using a password-protected social media site or privacy settings to restrict access to 'friends only'). As noted above, US laws, such as anti-discrimination and labour laws, may impose restrictions on the use of publicly available information for employment purposes.

US law does not distinguish between business webpages and private webpages. US privacy laws provide no protection for information posted on an employer-sponsored webpage. Other laws, such as anti-discrimination and labour laws, would still apply to information posted on an employer-sponsored webpage.

There is no legal distinction between information from search engines and information available only to 'friends'. The former is usable by the employer, the latter is generally not.

No authority has spoken on whether employers may use information posted by third parties, but based on prior rulings by the courts and administrative agencies, the general rule that publicly available information can be used, while secured information cannot, would be likely to apply. However, it would be risky for an employer to utilise information about an employee which is posted by a third party because the information may be inaccurate or unreliable.

5. Consent and works council rights

5.1 Consent

The employer can use information posted by an employee, not necessarily because the posting constitutes consent, but because, by voluntarily posting private information or photos and making them publicly available, the information is no longer considered private and no longer enjoys protection under privacy laws. Because any expectation of privacy no longer exists, no consent is needed.

An employee's consent for the employer to access information on a password-protected or otherwise restricted social media site would eliminate any basis for the employee to claim protection under US privacy law. However, other US laws, such as anti-discrimination and labour laws, may limit the employer's ability to use the information.

5.2 Works council rights

The employer is not required to consult with the union (if any) before using social media posts or content in the hiring process.

6. Sanctions

6.1 Regulatory authority and sanctions

The most common enforcement tool against an employer that violates privacy protections in relation to an employee's social media activities would be a private lawsuit filed by the employee against the employer seeking to recover damages and, possibly, injunctive relief. The National Labor Relations Board (the 'NLRB') is increasingly filing complaints against employers – whether unionised or not – who have disciplined employees based on social media activity. These complaints typically allege that the discipline violated the employee's right under the National Labor Relations Act to communicate with co-workers about the terms and conditions of employment.

The courts would enforce any court-issued judgment against an employer resulting from litigation. The courts would also enforce any sanctions imposed by an administrative agency, such as the NLRB, against an employer.

6.2 How often sanctions are imposed

To date, there have been only a small number of instances in which employees or administrative agencies have obtained sanctions against an employer based on the employer's access to, or use of, information on social media sites for employment purposes.

7. Data protection officers

7.1 Requirement for data protection officer

Companies are not required to have a data protection officer except in limited circumstances unrelated to social media activity.

Ius Laboris
280 Boulevard du Souverain
B-1160 Brussels, Belgium
Tel. +32 2 761 46 10
Fax. +32 2 761 46 15
Email: info@iuslaboris.com