Preamble

The workplace is part of the public sphere which includes the right to privacy.

It is generally considered appropriate to balance between the worker’s interest to the protection of his privacy and the competing interests of the employer and the society to disclosure of information and to preventive surveillance of workers. These competing interests are most often dictated by security and productivity concerns.

The technological innovations facilitate the employer’s control over the worker’s activities in the workplace and thus increase the risk of conflict between the interests of the enterprise and the worker’s right to privacy. The border that separates professional life from privacy is therefore very fragile and it reveals that the two spheres (private and public) are not perfectly sealed anymore.

Therefore, the purpose of this study is the protection of privacy that a worker can expect both with regard to his future employer (recruitment phase) or his employer (during his employment period), when information about him circulate on social networks (Facebook, LinkedIn, etc ...) or on blogs depending on:

− whether the worker is circulating this information by himself or it is done by third parties;
− whether there is a direct and free access to the information (« open profile ») or not (« closed profile »);
− whether we are talking about collecting information or using this information;
− the fact that the gathering and use of information is done by the employer or the information is collected by a third party and then made available to the employer who will use it.

* * *
Questions

[1] Does your country have laws or regulations that protect the confidentiality of electronic communications?

Yes.

The main Austrian law dealing with data protection is the **Federal Act concerning the Protection of Personal Data (DSG 2000)**. It is a fundamental **constitutional right**, that everybody shall have the right to secrecy for the personal data concerning him, especially with regard to his private and family life, insofar as he has an interest deserving such protection. Such an interest is precluded when data cannot be subject to the right to secrecy due to their general availability or because they cannot be traced back to the data subject. Insofar personal data is not used in the vital interest of the data subject or with his consent, restrictions to the right to secrecy are only permitted to safeguard overriding legitimate interests of another, namely in case of an intervention by a public authority the restriction shall only be permitted based on laws necessary for the reasons stated in Art. 8, para. 2 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such laws shall provide suitable safeguards for the protection of the data subjects’ interest in secrecy. Even in the case of permitted restrictions the intervention with the fundamental right shall be carried out using only the least intrusive of all effective methods.

The **DSG** regulates the processing of personal data, relating to living individuals, who can be identified from those data or from those data together with other information, which is in the possession of the entity, who decides what the data will be used for. The term “processing” has a wide meaning and is intended to cover any conceivable operation on data, ranging from collecting, recording, holding of them and the carrying out of any operation on those data. The provisions of the DSG 2000 apply not only to information that is processed automatically but also information recorded on paper if there is some structure to the paper records so that you can find specific information about an individual.

Furthermore **works council** and the employer may conclude works agreements. This is a form to exercise participation and also to create provisions, which grant certain rights to employees.


[2] If so, are these provisions applicable when the information is collected on social networks or blogs?

Data shall **only be collected** and only used for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes and kept in a form which permits identification of data subjects as long as this is necessary for the purpose.
General accessibility of information at networks or blogs doesn't mean that the employer can collect and process these information without limit. For any kind of collection and processing of personal information the employer must have legal basis.

Procession of sensitive data (“data deserving special protection”): data relating to natural persons concerning their racial or ethnic origin, political opinion, trade-union membership, religious or philosophical beliefs, and data concerning health or sex life is restricted. The use of sensitive data does not infringe interests in secrecy deserving protection only and exclusively if:

1. the data subject has obviously made public the data himself......
6. the data subject has unambiguously given his consent, which can be revoked at any time, the revocation making any further use of the data illegal, or ....
9. the use is necessary for establishment, exercise or defence of legal claims of the controller before a public authority and the data were collected legitimately or...
11. the use is required according to the rights and duties of the controller in the field of employment law....

For non sensitive data the use of data does not infringe interests in secrecy deserving protection also if over-riding legitimate interests pursued by the controller or by a third party require the use of data (legitimacy of the data application; report to an institution in charge of prosecution of a reported criminal act).

The DSG contains an exemption for personal data that is processed by an individual for the purposes of their purely personal or family affairs, if that data have been disclosed to them by the data subject himself or that they have received in a lawful manner (originate from a legal data application). Data that are processed by a natural person for purely personal or family matters shall be transmitted for another purpose only with the consent of the data subject, unless expressly provided for otherwise by law. The exemption does not cover organisational use of online forums. Organisations that use social media are therefore subject to the DSG in the normal way

[3] If so, are these provisions protecting the information collected or used by an employer:

• during the recruitment phase?

There are no specific rules, what a prospective employer is allowed to look for in the social media profiles of job applicants. But employers have to exercise caution in their use of information which could be deemed to discriminate against potential candidates. Furthermore they have to carried out using data only the least intrusive of all effective methods and to respect an area of strict personal data.
• in the course of the employment for disciplinary reasons or others?

Regarding surveillance of workers and monitoring employees e-mails and cyber communications an employer has to have a policy warning employees that all communications on devices, supplied by the employer or personal, could and would be monitored. It has to be made clear that misuse of internet is prohibited, and such misuse can be used in disciplinary proceedings. Than misuse may be a reason for disciplinary measures for misuse of email or internet. The employees must be aware that monitoring may be undertaken, and monitoring must be proportional.

[4] Are the employees allowed to use social networks during working hours? If so, in which way?

Generally an employer can specify the use of equipment and also prohibit it for privat purposes. Most employers allow a limited amount of personal use. In the absence of a clear policy, employees may be assumed to have a reasonable expectation of using equipment and privacy in the workplace.

Works council can compell the employer to conclude works agreements on this issue.

[5] Can the employer monitor the use of social networks by his employees during working hours?

The employer has to make clear policies and actions in relation to monitoring and surveillance of employees during working hours. Monitoring and surveillance is not only governed by Federal Act concerning the Protection of Personal Data it is also an area of participation of works council. So the works council can limit monitoring during working hours.

Outside working hours social media accounts are private. In cases where social media posts affect the reputation of the employer or constitute bullying and harassment of other employees is forbidden. Furthermore there may be a breach of the duty of secrecy. An employer may investigate and potentially take disciplinary action. For example a bank employee referred in public social media to some missing money in the bank. This led to the employee’s termination of employment. The employee’s unfair dismissal claim was rejected by the Supreme Court (9 ObA 111/14k).The dismissal was regarded as justified due to the breach of trust.

Gerhard Kuras

Austria