NYMITY

Privacy Interviews with Experts
August 2011

Toronto / Washington DC / Brussels
www.nymity.com

Rainer Knyrim
Attorney and Partner
Preslmayr Attorneys at Law
Vienna, Austria

Overview of Employment and Employee Privacy Laws and Key Trends in Austria

While employee privacy regulation in Austria is nothing new, it is becoming more complex as the world becomes more and more digital, the workforce more mobile, economies more fragile and various types of laws within and across economies converging. The Austrian economy and the Austrian worker is no exception to being affected by this phenomenon. It is important for companies resident in Austria, companies operating web-sites assisting Austrian workers and multi-nationals to understand Austrian labour, privacy and even export laws as they relate to the overall employment life cycle.

Dr. Rainer Knyrim, attorney at law and partner with Preslmayr Attorneys at Law in Vienna, Austria, provides us with an overview about current employment law, related employee privacy laws, pending laws and regulations and the key trends in Austria. Rainer highlights the unique aspects of employee privacy and data protection today and in the coming years in Austria as well as some of the major risks and more importantly mitigating controls that are necessary for those of us that do business in Austria to understand.

Rainer has advised local mid-sized, large and big international corporations on the implementation of various kinds and types of employee data applications (SAP, PeopleSoft, Siebel, etc) as regards both, their data protection and privacy implications (notifications with the DPA, authorization of international data transfer, drafting of standard clauses for processing agreements or employee privacy notices and policies, etc) as well as connected requirements of labour law (drafting and negotiating company agreements or employees consent forms, notifications of the works council, etc). In addition, Rainer regularly speaks on employees privacy conferences and seminars directed to HR-representatives of local and international businesses.

Nymity: What are the employment related laws and regulations in Austria that have a direct impact on employee privacy?

Knyrim: Asking for specifically employment related laws and regulations in Austria, those that first come to my mind are the Austrian Constitutional Act ("Arbeitsverfassungsgesetz" – ArbVG) as well as the Act on the Adaption of Employment Contracts ("Arbeitsvertragsrechts-Anpassungsgesetz" – AVRAG). Those acts specifically include protective regulations in case the employer implements measures, which include the collection and processing of personal data of the employees or qualify as means to inadmissibly control the behaviour of the employee at their workplace. Supplementary, the most important statute for data protection, the Austrian Act on the Processing of Personal Data, is applicable as it generally regulates the processing of personal data, notwithstanding the particular field or area, in or for which the data are processed. Certainly, fundamental rights found in Austrian Constitution Law do also protect the privacy of the citizens, eg the right for privacy as stated in the European Covention on Human Rights. Such fundamental rights must particularly paid attention to when the interests of the employee for privacy and the immanent and overwhelming right of the employer to effectively run his or her business have to be balanced.

Nymity: What is the scope of these employment related laws and regulations? What data is covered? What entities does the law apply to?

Knyrim: The scope of those laws extends from the regulation of the basics of the processing of personal data for the purpose of personnel administration and customers/suppliers-databases over more complex systems of employee performance control and evaluation up to intensive surveillance methods such as video surveillance or access control for the business premises using biometrical data.

The regulations, basically, cover any processing of personal data with regard to the employees. It is not the question, which kinds of data are processed, but to what extent and intensity data of the employees are processed. Most of the provisions, however, do only apply to entities (in the meaning of corporations, partnerships as well as sole proprietorships, in which a works council is established), such as the relevant provisions of the ArbVG. The rest is applicable to all businesses implementing employee data applications, respectively measures likely to control the employees.

Nymity: Does the law apply outside of its jurisdiction, be it a state, province or country?

Knyrim: The employment related laws having direct impact on employee privacy do not apply outside Austria's jurisdiction. The same is true with respect to the regulations mentioned above under question 1 (Constitutional as well as the Austria Act on the Processing of Personal Data).

Nymity: What are the employee privacy and security related laws and regulations in Austria?

Knyrim: See question 1 above.

Nymity: What is the scope of the law? What data is covered? What entities does the law apply to?

Knyrim: See question 2 above.

Nymity: Does the law apply outside of its jurisdiction, be it a state, province or country?

Knyrim: See question 3 above.

Nymity: What are the employee consent requirements?

Knyrim: The most important regulations requiring the explicit consent of the employee are Sect 96 para 1 no 3 ArbVG, respectively. Those provisions require such consent in case the employer implements or makes use of so called measures likely to control the behaviour of the employees. Whereas, Sect 96 para 1 no 3 ArbVG refers to businesses having established a works council and substitutes the consent of every single employee by the conclusion of the company agreement, the requirement of Sect. 10 para 1 AVRAG applies supplementary, if no works council exists. In this case, the consent of every single employee must be obtained.

Nymity: In general what does the employee privacy law/regulation require, by privacy principle?

Knyrim: Generally, the employee privacy laws and regulations require – as is a general principle of Austrian privacy and data protection law - that personal data of the employees are only processed to the extent absolutely necessary for the respective purpose. Furthermore, those regulations require the employer as the data controller to effectively inform the employees on the data processed as well as on any alterations or amendments of/to the processing of personal data. The laws follow the system that in case a works council is established – the employee's interests regarding privacy are represented by this body.

Nymity: What are the works council and union laws/regulations that relate to employee privacy and data protection?

Knyrim: The works council and union laws/regulations that relate to the employee's privacy are found in the Labour Constitutional Act. The relevant provisions can be found between Section 89 and 97. For a company's respectively businesses, which did not establish a works council, Sect 10 para 1 of the AVRAG is relevant as well.

Nymity: How have most companies addressed the risks these laws raise in an effective manner?

Knyrim: The awareness of companies regarding the risks raised by these laws is increasing, but the measures addressing them should already be more developed. Some companies voluntarily establish a so called data protection officer who is responsible for the compliance with data protection regulations. Otherwise observance of privacy and data protection related issues usually is delegated to the general compliance department of the companies; as those departments usually have to cover many areas of regulatory laws, data protection, unfortunately, does often play a minor role, only. Some of my new clients often do not have implemented any risk addressing measures regarding proper and admissible processing of employee data, yet. In general, it can be concluded that Austrian companies do not have effective measurements incorporated in order to address the risks timely. Usually, once a project is started, data protection issues have not been taken into account, properly. Once the project is already in the

course of actual implementation, data protection measures are imposed to the extent compatible with the already set up systems and implementation plans.

Nymity: Do you have a Data Protection Authority or regulator and if so who is the Data Protection Authority or regulator?

Knyrim: Yes, in Austria, there is established a Data Protection Authority ("Datenschutzkommission" - DPA) located in Vienna.

Nymity: Is there a Registration/Notification requirement of a company with the Data Protection Authority or regulator for collecting and/or processing Employee Personal and Sensitive Personal Data?

Knyrim: Austrian data protection law imposes extensive registration, respectively notification requirements for companies processing personal data. At first, companies processing personal data have to officially register themselves as controllers with the DPA-. Secondly, those controllers have to evaluate, whether their data applications, in which personal data are processed were subject to the duty of notification. There is only a limited number of standard applications enacted, which exempt a data application completely falling under such standard from this notification-duty.

The notification duty covers both, the processing of "normal" as well as sensitive personal data. However, in case a data application processes sensitive personal data, the "risk" that the applications is subject to notification rises significantly, as well as that the application may not "go live" until the DPA has rendered its prior approval. Usually, data applications processing sensitive data as well as criminal data, indeed, are subject to the prior approval procedure of the DPA.

Nymity: If your Data Protection Authority is active, what has been their primary focus relating to employee privacy? What types of fines have they issued during the last calendar year if any?

Knyrim: The Austrian DPA sees its primary role in the notification procedure, which is very strict, not in fining. Moreover, I cannot even provide for a rough statement, since data on fines for such administrative violations are not publicly available and not subject to any statistics.

Nymity: Are there laws/regulations regarding international transfers of Employee Personal or Sensitive Personal Data?

Knyrim: Austrian data protection law does not know any laws or regulations specifically regulating the international transfer of personal or sensitive data of employees. This issue is generally addressed in the Austrian Data Protection Act. However, any time an international transfer of the personal data of an employee is intended even within a group of companies, special attention must be paid to the purposes of such transmission. Specialized legal assistance is recommended regarding those questions.

Nymity: Is there new or pending draft employee related data protection law(s) or regulations? What will they require companies to do? Is there an English version and if so where would it be located?

Knyrim: To my knowledge, there is currently no pending draft for any employee related data protection law, or although there have been political discussions. However, as Germany is in the process of enacting such regulation, I expect Austria to wait until the final result of this legislation process, probably, even until the first experiences with the new German Act have been evaluated, before work will be spent by the legislative bodies to draft and adopt any laws particularly addressing the collection and transfer of personal data of employees.

Nymity: What are the expected next steps for the new draft employee data protection law or regulations? Will it be passed as is? Will the law require additional regulations to be written? What do you see as the timeline for its passage and the activities needed to make it effective, if indeed it is to pass?

Knyrim: Please see my answer to the previous question.

Nymity: Currently what are the employee privacy and data protection practices that are common in your country?

a. **Do most companies have internal employee privacy policies and external privacy notices for their applicants and employees?**

Knyrim: Internal employee privacy policies are emerging and becoming more common within Austrian companies; however, for the time being, such policies are still the exception and are mostly found in the Austrian subsidiaries of multinational

groups of companies. The same is true with respect to external privacy notices for applicants and employees. From my experience I can say that it is a matter of the ideology or ethical approach of a company, whether it does provide employees or applicants for such policies. Hence, most companies have not paid as high attention as necessary to such policies, yet.

b. Are there specific privacy related laws that apply to applicants?

Knyrim: No, there aren't any specific privacy related laws existing, which apply to applicants. Privacy issues of applicants have to be qualified and evaluated under the general rules of the Austrian data protection act. Nevertheless, just recently the standard application for personnel administration was amended with basic data of applicants, exempting the collection of their basic data from the duty of notification.

Besides this privacy related regulation, a special act obliges employers to treat applicants equally. This act does also prohibit employers to ask applicants certain questions regarding topics such as family planning, their marital status, religious beliefs and/or ethnic origin, etc. Violation of this Act may lead to administrative sanctions and damage claims of unequally treated applicants.

c. How do most companies address applicant and employee background checks for criminal and credit problem related activities? Are there certain restrictions that apply to the process?

Knyrim: In Austria, companies do not have any legal right to check the employee's background with respect to criminal sentences or credit problems. Such data are specially protected under the Austrian data protection act. If a company would process such data, prior consent of the data protection authority was necessary and presumably not obtained.

The collection and processing of information on criminal sentences of the employee may only the eligible once a certificate of good character is required under any laws or codes particularly regulating the terms and conditions a particular profession or job may be exercised and which the applicant is applying for.

d. How do most companies address various forms of employee testing, be it psychological, skills, drug or alcohol related testing? What employee rights are protected by law related to employee testing?

Knyrim: If a company or another employer wants to perform a test of their employees, the general rule is that the interests of the employees have to be balanced with any immanent needs of the employer regarding the knowledge of the result of the test of each employee. Generally, skill tests are admissible only as long as they are required for a valid purpose pursued by the employer. However, privacy protective measures have to be taken into account. In this regard, it has to be assured that no sanctions may be imposed on the employees due to the results of such tests.

e. How do most companies address employee data security and eMail and internet monitoring? Have organizations implemented additional employee monitoring measures? If so, what do these monitoring measures included? What employee rights are protected by law from employee monitoring?

Knyrim: Many companies have already implemented employee data security policies as well as acceptable use policies for the purpose to regulate the use of the business email-account and internet access. Those policies usually do also include some provisions for internet monitoring, respectively the admissible use of it. Usually, such policies prohibit entering websites with pornographic, criminal or gambling related content. In this respect, however, internet monitoring does not include control of the internet behaviour of the employees and, hence, does not allow the employers to trace and store the history of the internet-use of the employees to an extent which exceeds its necessity for technical reasons. It may be conducted by blocking the access to webpage with said content.

So far, in Austria, companies have implemented employee monitoring measures including telephone conversations in order to prohibit employees to extensively use the business phone at work for private calls. In this regard, the Austrian Supreme Court has decided that a telephone monitoring system requires consent of the works council, which records all numbers dialled, the length of such calls, date and time and its costs. The fact that the employees could press a button to indicate that a call was private, for which calls the four last digits of the number dialled were collected, did not make any difference. The system was too intrusive in the eyes of the court and provided the employer possibilities to control the workforce he would not have had by conducting admissible controls every now and then. Nevertheless, private calls to a certain extent (as long as absolutely necessary and urgent for the employee) must always be admissible for employees. The same is true for any use of the internet or the business email address.

f. **How are most companies addressing international transfers and contracting with controllers, service providers (vendors/suppliers and their sub-vendors/suppliers, when it relates to employee personal and sensitive personal data?**

Knyrim: Companies in Austria usually try to address transfers of personal data within the subsidiaries of the group by the conclusion of data transfer or data processing agreements pursuant to the Model rules provided for by the European Union (Standard Contractual Clauses); another possibility is the adoption of Binding Corporate Rules ('BCRs') with the company and have them authorized with a DPA of the European Union. Once BCR's have been authorized by such DPA, the Austrian DPA does not examine and evaluate the content of the BCR's (and hence recognizes the decision of the foreign DPA located within the EU) but only determines whether the topic or purposes of the data transfer is covered by the respective BCRs.

In case the international data transfer does require authorization of the DPA, it is very favorable if the recipient can be qualified as a processor (eg by limiting his/her ability to handle the data solely on instruction of the data exporter), as such processing of data is more likely to be authorized than a data transfer to another controller located in a third country.

g. **What about whistle-blowing hotline requirements? Are special measures necessary for implementing such hotlines?**

Knyrim: The ADPA does not contain specific regulations concerning whistle-blowing hotlines, neither does any other Austrian law. The legitimacy of such hotlines, thus, has to be evaluated according to general rules and principles. The DPA has, indeed, not published any guidelines for the structure of such hotlines, but has - at least - rendered four decisions on the notifications of whistle-blowing systems, especially on the legitimacy of the data transfer to an US-based mother company of the Austrian subsidiary. Those decisions provide for some guidance on the legitimate basis for the processing of specific types of personal data within such systems nationally and internationally, the structure of the systems and the use of processors.

As whistle-blowing systems usually qualify as a measure likely to control the employees, the obligatory conclusion of a company agreement (in case a works council exists) could be named as a specific requirement for their legitimacy. Furthermore, the implementation of the system is subject to prior approval of the DPA, as data relating to criminal offenses might be processed via the hotline.

h. **What are companies doing about employee privacy issues that arise during e-Discovery and forensic research into security breaches, Foreign Corrupt Practices Act/Briber Act violations, fraud and cyber-attacks?**

Knyrim: In such cases, companies do have to observe the general obligation of a data breach notification addressed to the data subjects. Such notification is required once personal data get lost or transmitted to a receiver or processor not eligible to access or somehow process those data. As also Austrian companies have been subject to various cyber attacks in the past few months, I expect the companies to spend more funds for IT-security, finally.

As I have not heard of the foreign corrupt practices act/prior act, I cannot make any comments to those regulations.

i. **Are there special employee regulations or industry codes for the cyber world, such as for behavioural marketing, on-line tracking, placement of cookies, geo-location services, mobile devices, social networks, payment processing, and so on?**

Knyrim: No, there are currently no specific regulations in place on those issues. They have to be evaluated under general principles and according to the provisions of the ADPA respectively the Telecommunications Act. However, as the EU e-privacy directive 2002/58/EC has been amended by directive 2009/136/EG, new special regulations for the declaration of consent for the use of cookies on websites have to be implemented to the Telecommunications Act now. Drafts for the amendment are already existing, an entry into force of the amendment is expected not before late 2011.

Are there other special employee regulations or industry codes that have not been discussed?

Knyrim: No, there are no other relevant codes existing.

Nymity: What are the hot topics in employee data protection and privacy in your country? What are the risks and what are you recommending to clients to address those risks?

Knyrim: Hot topics in employee data protection law currently are the implementation of whistleblowing hotlines, general data applications for personnel administration, employee evaluation and performance management systems, employee questionnaires and video surveillance.

Risks do always consist in problems with traditionally strong Unions in Austria, as they have selected specialists in employee data protection law in their legal departments. Those specialist usually actively advice works councils of companies in negotiations about the conclusion of company agreements regulation the implementation of applications processing personal data. If companies do not timely address the issues connected to data processing employee-management-systems, the risks consist in a delayed "go-life" of such system, which can negatively affect the whole process of the entire group. Therefore, I always recommend my clients to timely (at least an entire year before implementation) address and communicate the privacy related issues within their company, and, especially, to the affiliated companies. Usually, the project leadership team is located in the mother company or in another foreign affiliated company of the Austrian subsidiary and is not aware of the intensive and strict Austrian data protection rules and requirements. Therefore, the Austrian subsidiary often has to ask for detailed and specific information and documentation, which the mother company has to compile, create and provide for.

Besides a delay in the implementation of data applications processing personal data of employees, risks are represented by fired employees who try or intend to take revenge for their termination and harm their former companies by means of revealing its often non-complying policies with the strict rules and requirement of Austrian data protection law to the DPA or any other official Austrian authority. This may lead to administrative sanctions up to the amount of EUR 25.000,-- imposed by the DPA, if a subsequent investigation comes to the conclusion that data of the employees have been processed, illegally.

Nymity: In closing, do you anticipate additional significant changes from the authorities relating to employee privacy? If so, what might these changes include and from where will they come?

Knyrim: For the upcoming years, notwithstanding any possible enactments of special provisions for employee privacy issues, I do not expect the DPA to significantly change its behaviour and approach to employee privacy. This is also due to the fact that the personnel situation of the DPA is disastrous.