International Data Privacy Law Advance Access published November 8, 2010

Whistleblowing Hotlines in Austria

Rainer Knyrim*, and Gerald Trieb†

Abstract

- The Sarbanes-Oxley Act requires publicly-held US companies and their EU-based affiliates, as well as non-US companies listed on a US stock exchange, to establish a procedure for the receipt, retention, and treatment of complaints regarding accounting, internal accounting controls, and similar matters (so-called 'whistleblowing systems').
- The Austrian data protection authority has already issued four decisions on the compatibility of such whistleblowing systems with data protection law, which impose a number of detailed requirements that go beyond those contained in the Article 29 Working Party opinion.
- Besides data protection issues, the implementation of whistleblowing systems also has important implications under Austrian labour and employment law.

I. Introduction to the Legal Environment of Whistleblowing Systems

In reaction to a number of major corporate and accounting scandals in the United States (including Enron, Tyco International, and WorldCom) which cost investors billions of dollars when the share prices of the affected companies collapsed and shook public confidence in the securities markets, in 2002 the US Congress enacted a federal law commonly known as the 'Sarbanes-Oxley Act' (Pub.L. 107–204, 116 Stat. 745, enacted 30 July 2002, amended by the Dodd-Frank Act, Pub.L. 111–203, H.R. 4173, enacted 21 July 2010, referred to hereinafter as 'SOX'). The bill sets new or enhanced standards for all US public company boards, management, and public accounting firms.

In particular, SOX requires publicly-held US companies and their EU-based affiliates, as well as non-US companies, listed on one of the US stock markets to establish within their own audit committee a 'procedure for the receipt, retention and treatment of complaints received by the issuer (the publicly held corporation) regarding accounting, internal accounting controls and auditing matters; and the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters' (Sarbanes-Oxley Act of 2002, Pub. L. No. 107–204, 116 Stat. 745, Sec 301 (4)). As a consequence of this broad coverage, companies based around the globe have to comply with the provisions of SOX and (since massive sanctions are imposed for noncompliance) to provide their employees with opportunities to report any misconduct and infringements by their colleagues and managers of corporate ethical standards and legal requirements regarding SOX-related matters to the corporate headquarters. Systems established for such purposes are commonly known as 'whistleblowing systems'.

Whistleblowing systems have important implications under data protection and privacy law, since their operation is closely connected to the processing and transfer of personal data of the employees. Thus, if implemented within the EU, they often conflict with the mandatory rules of European data protection law, and those of the EU member states. Therefore, the systems often have to be modified and adapted in order to be compliant with such regulations. This is certainly the case for Austria, where the national Data Protection Authority (hereinafter 'DPA') has already been confronted with applications for permission to implement whistleblowing systems of various affiliates of US corporations.

II. Authorization of data processing under Austrian law

The EU Data Protection Directive 95/46/EC has been implemented in Austrian Law in 2000 by adoption of a new 'Federal Act concerning the Protection of Personal Data' (Federal Law Gazette 165/1999, 'Datenschutzgesetz 2000', hereinafter 'ADPA'). The ADPA has recently been amended by the Federal Law Gazette 133/2009,

* Partner, Preslmayr Attorneys-at-Law, Vienna, knyrim@preslmayr.at.

† Associate, Preslmayr Attorneys-at-Law, Vienna, trieb@preslmayr.at.

implementing new rules for topics such as video surveillance, and establishing a duty for the controller of a data application to file a 'data breach notification' in cases of the unlawful processing of personal data processed within the application.

Subject to a number of limited exceptions, the ADPA requires any processing of personal data to be either notified to or authorized by the DPA prior to its implementation by the data controller. Such permission is necessary, for example, if the processing of personal data either involves sensitive data (meaning data on health, racial or ethnic origin, sexual orientation, political or philosophical opinions, etc) or other special categories of data such as those relating to criminal offences. If this is not the case, the data processing can be initiated by the controller immediately after the notification has been filed with the DPA. After the DPA has determined that the processing is legitimate under the ADPA, the data application is registered with the Austrian Data Processing Register.

Exceptions from this general rule of notification are listed in so-called 'standard applications' published by the DPA, which specifically determine particular types of data which can be lawfully processed and transmitted to a limited list of recipients. If the data application exclusively contains data listed in the standard application which, in addition, are solely transmitted to the listed recipients, the application does not need to be notified to the DPA.

However, with respect to whistleblowing systems, no standard application has been adopted by the DPA, and one is unlikely to be adopted in the near future (standard application number 2, comprising the processing and the transfer of employment data ('personnel management'), is not applicable). As a result, whistleblowing systems must be individually notified to the DPA. Furthermore, since the operation of such systems typically involves the processing of sensitive data as well as of special categories of data, their implementation generally requires the permission of the DPA before they can be operated. This 'procedure of prior approval' may take several months before the DPA issues its permission, usually after having asked one or more rounds of questions on the functionality and the structure of the system. Often, several amendments or modifications of the system are necessary to obtain the permission.

This procedure of evaluation of the legitimacy of the data processing by the DPA has to be distinguished from an examination of the legitimacy of the transfer of the data. Typically, problems arise if the processed data are sent to a country located outside the EU or European Economic Area (EEA), such as the US, which is not regarded as offering an adequate level of data protection under European standards. Therefore, in addition to the notification of the application, prior approval of the international data transfer by the DPA is necessary. Thus, if any transfer of personal data to the parent company located in the United States is intended within the scope of operation of the whistleblowing system, the transfer of the data has to be authorized by the DPA prior to the system's implementation. The application for authorization of the data transfer can be omitted only if the parent company is a member of the US Safe Harbor system.

III. Austrian case law on the implementation of whistleblowing systems

In Austria, the DPA has been dealing with whistleblowing systems since 2007, and issued its first decision in 2008 (DPA, 5.12.2008, K178.274/0010-DSK/2008; decisions of the DPA are available in German only). So far, the DPA has rendered four decisions on whistleblowing systems, the last of which was issued in January 2010 (DPA, 20.1.2010, K600.074/0002-DVR/2010). In these decisions, the DPA eventually granted permission to implement the systems, but only after the applicants repeatedly had to amend and modify their functionality, structure, and description. The required changes affected, among other things, the qualification of the Austrian subsidiary as controller of the data application; the description of the system; the types of data collected on the data subjects, as well as those transmitted to the US-based parent company; and certain guarantees regarding confidentiality and non-retaliation for the users of the systems.

These decisions in effect establish guidelines that whistleblowing systems should comply with in order to be approved by the DPA, which are described in detail below. The guidelines are based upon the Article 29 Working Party opinion dealing with the subject (Article 29 Working Party, 'Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting controls, auditing matters, fight against bribery, banking and financial crime' (WP 117), 1 February 2006), but with some important differences in emphasis. The implementation of whistleblowing systems is one of the most difficult issues under Austrian data protection law, since the DPA generally examines and evaluates the functionalities, structures, purposes, and safeguards

of those systems in a very detailed manner. The DPA is very stringent with respect to the types and categories of data handled and processed as well as with regard to the transfer of the data, especially to companies having their headquarters in foreign countries such as the US. A number of further cases concerning whistleblowing systems are currently pending before the DPA.

IV. Guidelines for whistleblowing systems resulting from DPA decisions

As stated above, the decisions of the DPA can be used as guidelines for the implementation of whistleblowing systems in Austria. The issues discussed in the following sections are of particular importance.

Identification of the data controller

Although, strictly speaking, the employees of the local subsidiary provide information for the US-based parent company implementing the whistleblowing system in its entire group according to duties imposed on them by a specific 'Code of Conduct', according to the DPA the controller of a whistleblowing system is actually the local subsidiary. This is because the employees providing the reports are attributed to the Austrian subsidiary, which regulates such reports either by a general, internal direction to the employees or by a specific provision in the employment contract obliging them to comply with such Code. Thus, the local subsidiary must file the notification for authorization of the whistleblowing system. The identification by the DPA of the local subsidiary as the data controller has been criticized in the Austrian legal literature, since it does not reflect the actual legal situation, and requires a certain directive or incorporation of clauses in employment contracts of the local subsidiary that the whistleblowing system might not have been designed for.

Aim of the whistleblowing system

Attached to the notification, the applicant has to provide a full and complete description of the whistleblowing system, which has to show that the system has been explicitly designed as a procedure for the internal report of observed misconduct of employees (eg 'Whistleblowing Hotline', 'Compliance System', etc).

In addition, the documentation has to make clear that the system as a whole is exclusively aimed at implementing the provisions of SOX, which basically cover complaints about misconduct in accounting and internal accounting controls or auditing matters. In this context, the DPA only allows data of those reports actually concerning matters relating to SOX and covering allegations of severe misconduct or infringements of the Code of Conduct to be transmitted for investigation to the appropriate departments of the parent company in the US. Other reports which merely affect local matters or minor misconduct may not be transmitted. At the time this article was finalized, a case was pending with the DPA that sought approval not only for SOX matters, but also for anti-money-laundering and anti-terrorism provisions, so further guidance on this point is likely.

Affected persons

Reports may only be transferred if the alleged misconduct affects managers of the controller or its employees of an equal status. However, in one of its decisions, the DPA has adopted a small exception to this general rule, applicable in cases where the direct manager of an employee violating or infringing the 'Code of Conduct' has not reacted to the misconduct reported and, thereby, himself violated the Code.

Independent whistleblowing entity

Limitation of reporting to severe misconduct of managers in matters relating to SOX is supposed to be guaranteed by the existence of an independent department of specially-trained persons, who are bound to treat the reports received confidentially and determine if the misconduct reported qualifies for transmission to the corporate headquarters or should instead be referred back to the local subsidiary. The department in charge of this selection could either be an independent entity within the corporation (eg the compliance department), or a separate legal entity for this task, a solution which the DPA prefers (this could be a third party processor, such as Ethics Point, Inc.).

In this respect, according to the DPA, this internal department or separate legal entity is acting as a processor for the local subsidiary. Therefore, a special contract entered into by the local subsidiary on the one hand and by the processor on the other hand has to be concluded, obliging the processor to process the reports received from the system solely according to the guidelines mentioned above.

These requirements may cause significant problems in practice, especially if a company decides to contract with a third party processor to evaluate the reports submitted via the whistleblowing hotline. Even if this processor specializes in the evaluation of such reports and is therefore able to identify matters relating to

SOX, it may have difficulty determining which matters can be handled internally within the local subsidiary, and which ones are of sufficient severity to implicate the overwhelming interests of the parent company and thus justify transmission of the report to the parent. The processor may not have the required insight and knowledge of the internal processes, structures and mechanisms within the local subsidiary, not to mention within the entire group in which the whistleblowing system is implemented, to make such judgements.

These difficulties may be ameliorated by having the local subsidiary issue specific and detailed instructions to the processor to help it evaluate the reports and decide whether they should be transmitted to the parent. But even if such instructions are issued, there will remain the problem of monitoring the processor's compliance with them. Therefore, the requirement of the pre-evaluation of the reports by a separate entity or a third party processor is a problematic issue for local Austrian subsidiaries of parent companies that implement whistleblowing systems on a global scale.

Non-SOX matters

The reason for the restrictions discussed above can be found in the relevant legal basis for the legitimacy of the operation of whistleblowing systems, as well as for the transfer of the data collected, which are regarded as being based in the overriding interests or the compelling needs of the data controller (the Austrian subsidiary) in the establishment of an internal compliance system (see Art 8 para 1 (4) and Art 8 para 4 (3) ADPA). However, such interests and needs can only outweigh the legitimate interests of the data subjects with respect to a transfer of the data collected regarding reports of severe misconduct of managers in SOX-related matters, and probably for a few other issues of significant importance such as compliance with anti-money-laundering or anti-terrorism regulations.

No legal basis exists with regard to reports of misconduct of matters other than these. The argument that the US-based parent company requires the data in order to comply with the provisions of SOX is not sufficient to provide a legal basis under Austrian law. In addition, such matters can usually be dealt with sufficiently by the local subsidiary. Reports affecting matters other than SOX compliance regularly contain sensitive data, and the compelling interests of the controller are not sufficient to provide a legal basis. On the contrary, the explicit consent of the data subjects to the transfer of their sensitive data would be necessary to justify the transfer. However, obtaining the explicit consent of every employee is not only implausible, but also inappropriate for the company itself.

Types of data

Regarding the types of personal data which are processed and transmitted within the operation of a whistleblowing system, the DPA has established a list limiting the data to those absolutely essential for determining and evaluating the reported and alleged misconduct; in this regard, the DPA distinguishes among three possible types of data subjects. With respect to a manager who is accused of violating the code, the following data types may be processed:

- data for the identification of the accused person (name, title, or description of the position within the company);
- postal address and contact data;
- position of the reporter;
- facts of the case;
- data regarding possible investigations and actions as a consequence of the report.

With respect to an employee of the controller who reports the misconduct, the following data types may be processed:

- data for the identification of the accused person (name, title, or description of the position within the company);
- postal address and contact data;
- position of the reporter;
- the facts of the case.

With respect to employees of the controller or its affiliates who are reported to be witnesses or who are allegedly able to provide any information or documentation valuable for the investigation of the report (third party data subjects), the following data may be processed:

- data for the identification of the accused person (name, title, or description of the position within the company);
- postal address and contact data;
- position of the reporter;
- the facts of the case;
- possible means of evidence as well as information on the relation of the person to the alleged misconduct.

Rights of data subjects

The DPA has established a few other conditions for the compliance of whistleblowing systems with the ADPA,

one of which is that the data controller generally may permit anonymous reports, but is not supposed to encourage them.

The DPA furthermore places great emphasis on ensuring the rights of data subjects. In this respect, persons accused of misconduct have to be informed of the report of the alleged misconduct; must be provided with access to the allegations; must be interviewed concerning the accusations; and have to be informed about the results of any investigation of the case. Furthermore, personal data of the person alleging the misconduct have to be treated confidentially by the investigator, and his or her identity may be disclosed, if at all, only if it is proven that the accusation has been unjustified. Finally, according to the DPA, the data collected in the course of operation of whistleblowing systems have to be deleted no later than two months after finalization of the investigation. This provision reflects the principle of the ADPA that personal data must only be kept for the period of time absolutely necessary for the purpose of their processing.

Formal procedure

With regard to the transfer of the data collected in the scope of operation of the system, prior authorization of the DPA is required as stated above. Authorization can be omitted if the recipient is located in a country with an adequate level of protection under EU law, such as with regard to US-based data recipients that have certified to the 'Safe Harbor' principles.

For purposes of authorization of the transfer, the recipient of the data (parent company as the data importer) has (apart from membership in the Safe Harbor) two further options, namely, on the one hand, signature of the EU-approved Standard Contractual Clauses, or, on the other hand, the adoption of so called 'Binding Corporate Rules' (hereinafter 'BCRs'), in which the importer assures that it has adopted sufficient internal binding rules regarding the protection of personal data and obliges itself to process the data received according to those standards. Therefore, the purpose of processing the data for the purpose of the whistleblowing system has to be specifically addressed in the BCRs in order to make them a viable means of obtaining the authorization. In addition, each Austrian subsidiary in which the whistleblowing system is implemented has to file the application for authorization of the BCRs as a data controller.

It has to be said that in practice, the amount of time necessary to make a global whistleblowing system satisfy the above requirements is substantial. In addition, a chronic shortage of staff at the Austrian DPA means that approval may take longer than in many other countries. If considerable revision to the company's whistleblowing guidelines is necessary, this may lead to repeated requests by the DPA to amend the documentation, and it may take six months or even longer before the system is approved.

V. Implications under Austrian labour and employment law

Since the DPA also examines whether requirements imposed by labour or employment law have been fulfilled, compliance with such requirements is important to obtain authorization by the DPA to operate the system and to transfer the data internationally to the parent company.

Whistleblowing systems are considered to constitute means and actions of the employer likely to control its employees and are, therefore, subject to mandatory provisions of Austrian constitutional labour law and employment contract law. In case the Austrian subsidiary has established a works council, which may be installed by the employees once a business has at least five employees, the conclusion of a company agreement (an agreement entered into between the subsidiary and its works council) regarding the hotline is necessary. This agreement must cover the purposes, functionalities, and the structure of the system, contain a list of the personal data processed as well as of their recipients, and specify the rights of information and co-management of the works council. As a consequence, any future alteration of the system may require a modification of the company agreement as well, such as regarding information given to the works council.

If a works council is not established, a special provision in Austrian employment law requires the explicit consent of every employee to the implementation of the system. Either the executed company agreement or a model form for the explicit consent of the employees has to be attached to the notification submitted to the DPA. Since the conclusion of such company agreements or obtaining the explicit consents of all employees may take many months, labour and employment law issues should be taken into account from the very beginning when implementing a whistleblowing system in Austria.

VI. Conclusions

'The Austrian DPA generally examines and evaluates the functionalities, structures, purposes, and safe-

guards of whistleblowing systems in a very detailed manner, which may lead to significant modifications of the system. While this may be understandable from the point of view of Austrian law, it is problematic in light of the fact that whistleblowing systems are used on a global scale. As the Austrian experience shows, it would be highly desirable for the EU member state DPAs to avoid imposing detailed national interpretations of the conditions for the use of whistleblowing systems.

doi:10.1093/idpl/ipq005