Companies in Austria face problems with data protection laws, the DPA and the courts

Dr Rainer Knyrim writes on the difficult situation both for the Data Protection Commission enforcing the law in Austria and the national quirks of privacy law confronting companies

Austrian privacy laws celebrated a double anniversary in 2005. Twenty-five years ago, on January 1 1980, the first Austrian Data Protection Act entered into force. And five years ago, on January 1 2000, the new Data Protection Act of 2000 became effective, implementing EU Directive 95/46/EC.

Yet this double anniversary furnishes no grounds for celebration, because in this year (on July 5 to be exact), the EU Commission initiated proceedings against Austria for violation of the Treaty due to inadequate implementation of the Directive (PL&B International, Sept 2005, p.4). The EU Commission considers that "full independence" of the Austrian Data Protection Commission is not guaranteed. The exact content of the proceedings is secret, but the problem appears to be the organisational, personal and financial dependence of the Data Protection Commission and its close links to Austria's Federal Chancellery where it resides.

Austria's Data Protection Commission is certainly among those with the scarcest financial and human resources in Europe, which substantially impacts on the duration of proceedings handled by it. Complaints, approvals of international data transfers and reports to the Data Processing Register may take months to complete. Even though the small team are very painstaking and obliging and even work on Sundays, occasionally, the shortage of funds cannot be overcome - regardless of the commitment invested. The Commission itself is very outspoken about its situation in its Data Protection Report of 2005, calling it "untenable" and noting its "organisational confusion". The Report lauds the creation, in May 2005, of a job position for covering the Commission's international responsibilities. According to its report, with a staff/population ratio of 1:400,000 the Austrian Commission ranks 24th among 31 European countries.

> "In recent years, privacy law has increasingly become the subject of discussion, both by the general public ... and in the business sector."

In spite of this situation, any impression that data privacy might be an issue that is widely ignored in Austria would be quite wrong. In recent years, privacy law has increasingly become the subject of discussion, both by:

- the general public, triggered especially by "political" projects such as enhanced video surveillance of public spaces, the biometric RFID passports to be introduced in 2006, or the electronic medical card ("e-card") issued to all citizens by the social insurance institutions; and
- in the business sector, especially in view of the closer links and ties between Austrian operations and international corporations.

Below, a closer look is given to some key elements of the Data Protection Act of importance for businesses operating in Austria.

Reporting of data applications, approval of international data transfers

Unlike Germany (to name just one example), the Austrian Data Protection Act makes no provision for any internal data privacy officer within an enterprise, so that each data application must be directly reported to Austria's Data Processing Register. This reporting duty is, however, subject to a number of exemptions for so-called standard applications, which have been identified in a Standard and Model Ordinance as exempt from reporting. Exact regulations are provided that extend to the purpose of an application, the type of data to be processed, and the recipients to which the data may be transmitted without triggering the need for reporting. In practice, this means that the data applications and transmissions by an establishment need to be analysed and compared to the standard applications. If the establishment processes more data or transmits them to other recipients than those listed in the standard applications, it needs to report it. Otherwise, it is exempt from this duty.

To highlight a few cases that are typical for a reporting system used by establishments that are included in the data flow of international corporations: customer and supplier data are processed with a standard application that provides for the transmission of data concerning key customers and suppliers to the controller's headquarters. These data need not be reported, whereas the transmission of all other customer and supplier data is subject to the reporting duty, as is the transmission of data to any affiliated company.

The transmission of employee data to other companies within a group, on the other hand, must always be reported to the Data Processing Register whenever they are independently processed at such other company, because this is not covered by any standard application. This happens quite frequently in Austria because Austrian operations of international corporations tend to be relatively small-scale so that personnel administration, the management of stock option programmes, internal recruiting and other functions are typically performed by the mother company in, say, the UK, or a sister company in Germany where the decision-making takes place (i.e. it is a case of a controller-to-controller transfer). If, however, the service is rendered at the request of the Austrian company (i.e. a controller-to-processor transfer), this need not be reported within the EU.

Both the provision of data to service providers and the transmission of data to processors outside the EU (e.g. the US) must be approved by the Data Protection Commission in advance, regardless of the duty to report them. In complying with this rule, the main difficulty is in actual practice: often it is extremely difficult to determine with the requisite clarity as required by the Data Protection Commission which data are to be transmitted for which purpose. The transmission of personal data is usually viewed with particular suspicion by the Commission because it does not easily accept the need for any independent processing of data by the parent company. Unless a logically coherent explanation is provided, the Commission fails to understand why the parent (located, e.g., in the US) should be able to see who in the Austrian subsidiary is on sick leave for how long or where secretary X has her private flat, which is often the practical outcome of centralising group data management. To get third-country transfers of customer and supplier data accepted by Austria's Data Protection Commission without a consent but based on necessity for "contract performance" is slightly easier than getting a transfer of employee data accepted without a consent of the employee. The Commission is stricter with employee data.

"Even when the EU standard contract clauses for an international data transfer have been agreed, it is necessary to obtain the Data Protection Commission's prior approval."

It should be noted that even when the EU standard contract clauses for an international data transfer have been agreed, it is necessary in Austria to obtain the Data Protection Commission's prior approval for such data transfer. The Commission does not check up on the standard contract clauses, but looks into the legal basis for the transfer and requests a detailed list of which data are transferred for which purpose.

Company code backed by civil law

The Commission has meanwhile gathered experience in codes of conduct and binding corporate rules regarding cases where the parent was domiciled in Austria and exchanged data with its subsidiaries in Eastern Europe. The Commission solved such cases by extracting from the parent a promise under civil law that it would ensure that the code of conduct would be observed within its group. Depending on the liability provisions in such a promise, it may or may not be necessary for the subsidiaries to submit such statements as well. It is, however, not necessary for all group companies to mutually sign contracts, so that this model is easier to handle than a contractual model. It remains to be seen whether this concept will also find adherents at an overall European level.

On the practical side, regular

personal contacts with the responsible Commission officers (by telephone, email or personal calls) are recommended in any proceedings with the Data Protection Commission and the Data Processing Register, especially in the case of urgent approval proceedings, in order to quickly find joint solutions to any problems that may occur.

Problems with statements of consent

In recent years, the Supreme Court has, in a series of rulings on complaints filed by consumers and consumer advocacy groups, developed extremely strict rules regarding the fundamental requirement for a statement of consent on the disclosure of data. In line with these rules, the type of data, recipient and purpose of the processing and transfer must be described in minute detail. Thus, the Supreme Court rejected a clause which failed to make clear which operation within a chain of department stores was to receive the data from a customer affinity programme. The rejected clause ran thus:

"I expressly consent and agree that my personal data as set forth above be computer-processed and disclosed to other companies of the xyz group for the purpose of consumer information and promotional measures."

In the same ruling, the Supreme Court also criticised that the term "promotional measures" was non-transparent. In another decision regarding the consent clause in a customer affinity programme run by a mobile phone operator, the Court made the same criticism. Here the clause ran as follows:

"The data are exchanged between group companies and transmitted to third-party companies for promotional purposes unless the participant withdraws his/her consent upon the start of the scheme or at any later date."

In actual practice, such rigid rules governing the consent clause will lead to considerable problems. Thus, if any companies affiliated with the controller (daughters, sisters, parents) exchange data, the application of the above principle would necessarily lead to all of them being expressly named in the consent clause. A practical solution for this problem is a reference to the list of actual recipients being available on the internet and a note to the effect that this may be subject to change.

Another problem is how to define the purpose of the data transmission, especially when such data are to be used for marketing purposes, because the Supreme Court expressly judged the all-inclusive global formulation "for promotional purposes" to be non-transparent. In practice this regularly leads to a balancing act between formulating the purpose as universally as possible, as is desired by the company so that it will cover as many future eventualities as possible, and the risk that such a wording will again be found to be not sufficiently transparent.

"Data" includes legal persons

For statements of consent that are designed to be effective at an international level as well as for data transfers it should be noted that the Austrian definition of "data" varies from that used by most other EU Member States. The Austrian Data Protection Act in its definitions includes not just the data of natural persons, but also those of legal persons and groups of legal persons, such as companies, and is thus much more comprehensive in its scope of application.

> "The Austrian definition of 'data' varies from that used by most other EU Member States...[It] includes not just the data of natural persons, but also those of legal persons and groups of legal persons, such as companies."

Laws governing data protection and competition

Another Austrian idiosyncrasy can be found in the relationship between data protection and competition. In 1992, the Supreme Court found that if customer bank accounts are analysed for payments to other banks on contracts made with a building society (savings & loan association) in order to furnish such customers with promotional literature on building society contracts, this constitutes a breach of banking secrecy and a violation of the Data Protection Act. Such a breach and violation gave the defendant an unacceptable and unfair advantage.

In a 2004 case involving proceedings to obtain a temporary injunction under the Unfair Competition Act, a similarity of clerical errors in the customers' names made it clear that lists of customers had been passed on to a competitor. Since this competitor could not furnish any credible evidence of how these data had ended up with it, the Supreme Court assumed that the competitor had obtained these data by dishonest means and ruled in favour of the other party who had argued that it had suffered a competitive disadvantage because the opponent had written to its own customers.

Shortly before, the Supreme Court had issued a ruling that was severely criticised due to a misinterpretation of the principles of data protection. In this decision, the Supreme Court amazingly found it acceptable that an ex-employee used the customer and supplier data of his former employer for his own business. The Supreme Court refused to grant the former employer any rights as a data subject, arguing (inappropriately) that these were simply the company's own data which did not fall within the scope of the Data Protection Act. It is possible that this decision was a singular lapse only and will soon be superseded by a new decision.

AUTHOR:

Rainer Knyrim, attorney-at-law,
Preslmayr, Austria
E-mail: knyrim@preslmayr.at