INTERNATIONAL NEWSLETTER

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Data breach notification duty added to Austria's DP Act

Dr Rainer Knyrim explains what this new provision means to organisations. Will Germany and Austria set a trend for Europe?

As Austria follows Germany in amending its data protection law to include a specific data breach requirement, the EU is also following this path (p.6) and France may do so. Other countries' DPAs, such as Denmark, are already interpreting their data protection laws' security provisions to require breach notification.

Austria's Data Protection Act 2000 (ADPA) has seen its biggest amendments since its introduction in 2000. These include the introduction of an explicit Data Breach Notification Duty which came into force on 1 January 2010 as well as provisions on video surveillance, and more and stronger powers for the Data Protection Commission (also in force since 1 January). Furthermore, a fully computerised and completely automated notification system will be introduced for the Austrian Data Processing Register by 1 January 2012.

Breach notification duty

Austria is the second country in the European Union after Germany to

Continued on p.3

France to discuss mandatory appointment of DP officers

Nathalie Métallinos looks at the role of the *Correspondant* under the current law and the advantages and disadvantages associated with this proposed change in the law.

On 6 November 2009, Senators Yves Détraigne and Anne-Marie Escoffier introduced a private member's bill[1] into France's Senate that would impose the obligation to appoint a Data Protection Officer (DPO) in each government body and most[2] large private sector companies.

This measure is accompanied by other substantial proposed amendments to France's Data Protection Act of 1978[3]: a general obligation to notify security breaches, increased transparency of data processing, prior information on retention periods, increased civil penalties by the CNIL and systematic publicity given to the CNIL's sanctions.

The bill also addresses the question of IP addresses and cookies. IP addresses, defined as "any address or identifier of the terminal equipment connected to a communication network" would be expressly qualified as personal data and an express consent (opt-in) regime would be required for cookies unless they are needed for communication purposes or to permit access to an online

Continued on p.4

Issue 103 **February 2010**

Austria, continued from p.1

introduce an explicit Data Breach Notification Duty (for the status of other countries see the *Privacy Laws & Business* report on Data Breach Notification Laws in Europe, at www.privacylaws.com/Documents/data_breach_conference.pdf).

The duty was added as sec 24 (2a) ADPA. It is a very short provision consisting of only two sentences. The unofficial translation is as follows:

"If a data controller finds out that data from one of its data applications [the sum of logically linked stages of data use which are organised in order to reach a defined result] has been used in a systematic, grave and unlawful manner, and the data subjects may suffer damage, he is obliged to inform the data subjects of this without delay and in an appropriate form. This duty does not apply if the notification would require a disproportionate effort in terms of the data subjects facing only minor damages, or the cost of notifying all data subjects in question."

This new provision has not been drafted clearly. For example, it is not clear what a "systematic" or "grave" use of data is. "Grave" would indicate that minor incidents are not included. "Systematic" might mean that there is a time constraint in the abuse of the data. As "data" by its definition in the ADPA is only "information relating to data subjects who are identified or identifiable", this indicates that an incident involving encrypted data which cannot be decrypted by normal technical means would not trigger a notification duty. Furthermore it is unclear what is a "minor damage" which would exclude a notification duty. Even a small sum such as €50 could be a substantial amount for an unemployed person. Also, it is not clear what an "appropriate form" would be. Would it be written communication to the data subject's address, email or a telephone call? The accompanying materials from the legislative body also refer to getting the mass media involved.

An interesting fact is that the Austrian Data Protection Commission neither needs to be informed about a data breach nor is it involved in any other way in such an incident. This, at first, looks like an advantage for companies, but companies might discover that they will have to make decisions without any guidance as to how to inform data subjects about a breach.

Therefore it is advisable for companies to prepare for an emergency case which would require not only a legal assessment of typical emergency scenarios by the legal department, but also cooperation with the marketing department, the call centre, the CRM department, IT, management, etc to established a contingency plan.

Video surveillance

The new regulation on CCTV, in force since 1 January 2010, does not change the principal duty to apply for the Data Protection Commission's prior approval for implementing a CCTV system. It is strictly forbidden to use CCTV for the surveillance of employees. But it will still be possible to conduct video surveillance for security purposes, and that can include filming employees. Standard storage time of CCTV data is 72 hours, and a longer storage time needs to be applied for.

There are two rather strange provisions for CCTV data. Firstly, CCTV data may not be matched with data from other applications. This would mean a step back in technology with regard to those access control systems that automatically store a video sequence or a picture from the video surveillance system in case of any abuse is detected at a control point where access may be gained to the system. The second provision is even stranger if seen from a technical point of view: analogue video data is excluded by the provisions of the ADPA, which means a hard disk, used as storage media for the video data, could be replaced by an old VHS home video recorder.

Fully automated notification

The amended ADPA includes a provision that, from 1 January 2012, a new, fully automated notification system will be introduced in Austria. A web interface will enable a data controller to fulfill its notification duty by entering the information electronically. Software will then check if the notification is complete and its description of the data processing plausible (!). If this is the case, it will immediately and automatically accept the notification. Although it is possible, in case of errors to the system, to apply in paper form as before, this seems to be the first time in Austria that an administrative procedure is fully automated and that civil servants are completely replaced by a computer. This new procedure will not be applicable for data applications that need prior authorisation by the Austrian Data Processing Register, such as those containing sensitive data or data on criminal records.

More and stronger powers

The powers of the Data Protection Commission are a little stronger now and will enable the Commission to deal with complaints faster, and to control notification duties better. Fines have risen from 1 January from €19,000 to a maximum of €25,000, which is still comparatively very low. The power to stop data processing and the use of software associated with that processing remains unchanged, as well as the punishment – a prison sentence of one year – for the use of data with the intention to make a profit or to cause harm.

Penalties and damages

How many fines are imposed on average per year? There are no statistics available as the fines are imposed by the local district authorities and are not made public. If a person informs the authorities about an abuse, the complainant is not party to the fining procedure and the authorities will not inform the complainant if they have imposed a fine.

What is the typical range of fines? There is no data available on the typical range of fines.

Can the Data Protection Commission impose a fine? It does not have a fining competence, only the competence to inform a district authority about a breach of the law and to suggest that a fining procedure is started. New since 1 January is the Commission's

Continued on p.8

AUTHOR

Dr. Rainer Knyrim, Partner at Preslmayr Attorneys at Law, Vienna, Austria, is speaking on Austria's data breach law at PL&B's 23rd Annual International Conference, 5-7 July 2010, Cambridge.
email: knyrim@preslmayr.at
Web: www.preslmayr.at/en/kanzlei.php

being careful with that information, not losing it, getting rid of it when it is out of date and so on and so on, all of the eight principles that are set out in the Data Protection Directive, one would have greater confidence that we could do business where it was needed. We think it is putting the cart before the horse for the Stockholm Programme [to define the framework for EU police and customs cooperation] to just talk about ensuring the best possible flow of data within European-wide networks when you have not actually done the fundamental thing of making sure that the data that is retained is being processed lawfully under the Directive. That is why we say you have to step back and get that right first and then build whatever structure you feel it is appropriate to build. We are in danger of tinkering with a lot of specifics instead of getting to a fundamental problem, which is that the data protection principles do not adequately apply across the European Union [uncorrected oral evidence]."

The ICO's response to the consultation states that an amended version of the existing Directive is needed. "This will contain many features of the current directive, such as the principles relating to data quality contained in Article 6. However, the new framework will be ordered better and be clearer about the principles, obligations and rights. It will also contain new features, intended to ensure that the law works effectively in practice. It will need to provide clarity in areas where there is currently confusion and it will need to update provisions where these are clearly out of step with the world today. In doing all this it should provide better real data protection for individuals and be a help rather than a hindrance to those within its scope."

The ICO also promotes BCRs by saying: "A useful measure, both in the short term and long term, would be to amend Article 25 to exempt transfers where another Member State has authorised an organisation's BCR or other long-term alternative."

INFORMATION

The consultation responses (167) can be seen at http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm

Reding's speech from 28 January can be seen at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/16&format=HTML&aged=0&language=EN&guiLanguage=en

Israel to join adequacy club

The EU Art. 29 Data Protection Working Party has made a positive assessment of the level of data protection in Israel. **Laura Linkomies** reports.

In an opinion issued on 1 December 2009, the Working Group says that it "believes that Israel guarantees an adequate level of protection according to … Article 25 of [the Data Protection] Directive".

Pending approval by the Article 31 Group, representing the governments of the EU Member States, Israel will join the small group of non-EU countries that have been assessed as adequate: Switzerland, Canada, Argentina, Jersey and Guernsey (UK Channel Islands) and the Faroe Islands.

The right to privacy is enshrined in Israel's Basic Law: Human Dignity and Liberty, which establishes the right to privacy, and the Privacy Protection Act (PPA) 1981. The PPA is enforced by the Israeli Law, Information and Technology Authority (ILITA) within the Ministry of Justice. ILITA, headed by Yoram Hacohen, a lawyer with a business background, has implemented a proactive audit and enforcement policy (p.9).

"We are are honoured by the Working Party opinion and happy to join this exclusive club," said Hacohen. "We have always felt that our regime is adequate, yet we intend to continue reforming our laws to increase accountability and enforcement of data protection regulation. We will work with companies and government agencies to devise reasonable compliance plans, while at the same time vigorously pursue privacy offenders."

Future work

The Working Party encourages Israeli authorities to, in future legislative developments, adopt provisions that envisage:

1. The application of Israeli legislation to manual databases.
2. The express application of the proportionality principle in relation to the totality of personal data processing carried out by the private sector.
3. An interpretation of the exemptions in international data transfers online envisaged in Article 26.1 of the Directive.

Andorra was awarded a similar opinion on 1 December 2009.

INFORMATION

The Opinion 6/2009 on the level of protection of personal data in Israel – WP 165, adopted on 1 December 2009, can be seen at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp165_en.pdf.
The Opinion on Andorra, adopted on 1 December 2009, can be seen at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp166_en.pdf.
ILITA recently sought public comments on its position paper proposing data security duties for data processors.
See www.justice.gov.il/MOJEng/RashutTech/News.

Austria, continued from p.3

power to forbid a data processing, in particular in cases of imminent danger.

Is there provision for compensation for financial and immaterial damages?
The Data Protection Act refers the claimant for compensation for damages to the civil courts ("Laender" level, one level above district courts). The rights to deletion and correction of data also need to be claimed in the civil courts.