New data breach notification duty introduced in the 2010 Amendment to the Data Protection Act

Austria is the second EU member state to oblige businesses and government authorities to notify victims of data breaches

Largely ignored by the public, a new notification duty for data breaches was introduced in addition to the new rules on video surveillance through the Amendment to the Data Protection Act effective as of 1 January 2010. Together with Germany, Austria once again acts as a pioneer in developing privacy law.

Under a provision which takes up just two sentences in a new Paragraph 2a of Section 24 of the 2000 Data Protection Act "DSG", private enterprises and public agencies alike have a duty of notification imposed on them in the event of "systematic and seriously wrongful use of data where the data subject may be harmed". This means that an IT security leak such as a "hacker attack" can no longer be "swept under the carpet" unobserved by the public.

Blackmail by USB stick

Rather, if in future a USB stick should go missing, its rightful owners must investigate whether this involves an abuse (as defined by this provision) of the data stored on it (because, to give just one example, the thief or chance finder attempts to blackmail the enterprise by threatening to publish the data). The management must consider whether to notify the data subjects, i.e. those individuals (e.g. customers) affected by the breach of data privacy, if they are threatened with suffering a more than petty loss in the event that the thief should misuse such information.

In the United States, this duty of information has been known for some years under the title of "data breach notification duty", and most of the states have since passed explicit laws to deal with such cases. In Europe, the discussion of whether to add appropriate provisions to the Data Protection Directive is of more recent date. With its 2010 Amendment to the Data Protection Act, Austria is only the second member of the European Union to introduce such a notification duty, effective as of 1 January 2010.

The Austrian regulation, however, is not particularly satisfactory as it is awash with vague, blurry and ill-defined terms. Thus there is no clarity as to what constitutes a "systematic" or "serious" data abuse. Neither is it clear what is meant by a "suitable" form of notifying the data subject.

In the US, same as in the regulation applicable in Germany since 1 September 2009, the form of first resort is a direct and personal communication (by letter or, conceivably, by e-mail, telephone, etc.). If this should not be feasible or involves an unreasonable effort, it is necessary to take out adverts in newspapers (in Germany: two adverts of a half-page each in two daily papers published throughout the territory as a minimum) or, in the US, in some cases even pay for TV broadcasts.

What exactly is "petty"?

The second sentence of Para 2a of Section 24 in the 2000 Data Protection Act provides an exception from the notification duty in the event that it "requires an unreasonable effort compared to the pettiness of the threatened loss to the data subject on the one hand

or the cost of notifying all data subjects concerned on the other hand". This leaves open a margin of interpretation of what exactly is meant by a "petty loss" (geringfügiger Schaden, to quote the original). It is similarly left obscure at what amount the cost of notification becomes unreasonable. The turn of phrase "on the one hand or ... on the other hand" probably needs to be read as a plain and simple "or" set between the two grounds for an exception.

Interestingly – and in contrast to the trend in the United States and the discussion in other EU member states – there is no need to notify the Austrian Data Protection Commission nor to involve it in any other way in the handling of a case of data breach. At first sight, this appears to offer an advantage to the enterprise affected, because it seems to give it leave to "sweep abuses under the carpet". But a closer look makes it obvious that, in the final analysis, enterprises are left entirely to their own devices in having to decide whether (and if so how) to inform data subjects of an abuse. They also have a substantial level of accountability imposed on them in terms of liability under civil law: it might involve an infringement of the duty to mitigate the damage, or allow a risk insurer to contract out of its liability if the notification duty is neglected (breach of a protective law!).

Prepare for the worst

It is thus advisable for enterprises as much as government authorities not to adopt a wait-and-see attitude but to proactively take measures to prepare for what may come. These include not just running risk scenarios through their law departments but also getting affected departments (such as p.r., IT, crisis management, executive management and any specialist department concerned) together to draft emergency plans.

For further information on the subject please contact:

Dr. Rainer Knyrim
Lawyer and Partner

knyrim@preslmayr.at

Pollirer · Weiss · Knyrim

DSG – Datenschutzgesetz
(Austrian Data Protection Act)

The authors of the commentary on the Data Protection Act have written a **convenient manual** on data privacy law:

- DSG updated – to key you in on the 2010 Amendment
- informative – including precise comments and materials
- handy – a quick reference book to take with you

The authors:
Hans-Jürgen Pollirer, court expert and managing director of SECUR-DATA GmbH.
Ernst M. Weiss, retired judge
Rainer Knyrim, lawyer and partner of Preslmayr Rechtsanwälte, specialising in data privacy law

Available only in German

New Partner

In early February 2010, we welcomed Ms (Dr) Esther Hold, attorney-at-law, as a partner to our law offices. She had been part of our team as a trainee lawyer since March 2007, working predominantly in Austrian and European cartel law, medical law, labour law and the law of contracts.

Her joining us as a partner was duly celebrated in the customary manner by a welcome bash thrown by our staff members together with her friends in early March 2010.