INTERNATIONAL newsletter

ISSUE NO 74 August/Sept 2004

EDITORIAL DIRECTOR & PUBLISHER
Stewart H Dresner
stewart@privacylaws.com

EDITOR
Alan Pedersen
alan@privacylaws.com

NEWSLETTER SUBSCRIPTIONS
Glenn Daif-Burns
glenn@privacylaws.com

ISSUE 74 CONTRIBUTORS

Pascale Gelly
Avocat à la Cour, Paris

Bridget Treacy
Barlow Lyde & Gilbert

Laura Linkomies
Privacy Laws & Business

Joe Figuerdo
FIT Services

Dr Jan-Peter Ohrtmann
Bird & Bird

Robert Waixel
Anglia Polytechnic University

Lilly Taranto
Marketing Improvement

Valerie Taylor
Privacy Laws & Business

PUBLISHED BY
Privacy Laws & Business,
5th Floor, Raebarn House,
100 Northolt Road, Harrow, Middlesex,
HA2 0BX, United Kingdom
Tel: +44 (0)20 8423 1300,
Fax: +44 (0)20 8423 4536
Website: www.privacylaws.com

The *Privacy Laws & Business* International Newsletter is produced five times a year and is available on an annual subscription basis only. Subscription details are at the back of the newsletter. Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given. No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior permission of the publishers.

Design by ProCreative +44 (0)20 8429 2400
Printed by Hendi +44 (0)20 7336 7300

ISSN 0953-6795

Editorial

National differences key to understanding new Europe

It was very clear at this month's 26th International Conference on Privacy and Personal Data Protection which I attended in Wroclaw, Poland (www.giodo.gov.pl), that there are still many differences between national data protection commissioners, even those in the European Union. For some, a change in their national law has led to a fundamental rethink.

France's CNIL, with its new law adopted this summer, now has stronger enforcement powers, formerly handled by a separate judicial body, as well as direct powers to impose fines on data controllers. Will the CNIL follow the precedent of Spain and impose substantial penalties? With a change of president, the CNIL is now more favourable to Binding Corporate Rules schemes. How will the CNIL use its discretion and choose its priorities in future?

Austria has changed how it will interpret its rules on international transfers. Its data protection commissioner has recently approved the binding corporate rules scheme of an Austrian bank with operations in Balkan countries that do not have adequate privacy laws. Austria's Commissioner has accepted a "unilateral declaration" from the bank that it will keep to its commitments regarding the transfer of personal data to these countries.

In other EU countries, detailed rules for opt-outs from direct marketing may be derived from the law and published by an industry body. However, in Italy, the Garante has adopted a detailed binding decision on how an opt-out from mail and telephone marketing must be shown in graphic form in a paper or electronic telephone directory.

In central and Eastern Europe, there are major differences of policy and enforcement methods between the Commissioners of neighbouring countries, such as Poland, Czech Republic and Hungary. The European Privacy Officers Network will explore these changes and differences in our meeting on November 2nd and 3rd in Prague.

Stewart Dresner, Editorial Director
PRIVACY LAWS & BUSINESS INTERNATIONAL

Contribute to PL&B publications

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Alan Pedersen on Tel: +44 208 423 1300, or E-mail: alan@privacylaws.com.

French data protection law, continued from p.1

protection authorities (including the CNIL) see consent differently and are increasingly considering that in cases of mass processing (which, in the end, is what software programs are meant to do), consent is not the best way to legitimise data processing.

Unlike Spain, France has transposed Article 7f of the directive (the so-called balance of interest clause), adopting a slightly different wording. In spite of the above, overall the French article 7 is very close to the directive (see box below).

Sensitive categories of data

As far as sensitive categories of data are concerned, France confirms the EU directive's prohibition of processing, subject to very limited exceptions, including individuals' consent. Surprisingly, the law does not authorise the processing of sensitive data, such as health-related data, in cases where the processing is necessary for the performance of legal obligations by the data controller under employment law (Article 8(2b) of the directive). Employers will therefore be in a difficult position to comply with their legal obligations such as ensuring the security of their staff, handling work-related accidents and sickness leave. We should hope that in these cases, the CNIL will use the power given by article 8(4) of the law to authorise the processing of sensitive data justified by the public interest.

An interesting addition had been introduced into the draft law allowing companies which are victims of criminal offences to process such types of data for the purposes of prevention and fight against fraud and damage compensation. Such processing was prohibited by the previous law.

This provision was, however, cancelled by the Constitutional Court in July as it did not include the necessary safeguards to protect privacy, in particular in terms of data sharing and retention obligations. Although it can be essential to their activities, companies will have to wait for the adoption of another law before they know under which rules they can operate this type of processing. Only copyright agencies may be authorised by the CNIL to operate such kinds of processing, in particular to fight against copyright breaches over the Internet.

Notification

Although the intent was to lighten existing formalities, the law maintains the principle that automated data processing must be notified to the CNIL ("déclaration").

The major exception to the notification obligation is for controllers who appoint a data protection correspondent ("correspondant à la protection des données"). However, this exception may be of little interest to companies operating globally, as the notification duty remains for data processing involving data transfers out of the European Community, although it is unclear whether it is only the data transfer which has to be notified or the entire processing. Having an in-house correspondent would still be useful in this respect for local or EU-based data processing activities and, of course, to create a privacy culture and controls within the companies. The pros and cons of such an appointment have to be carefully weighed (see box above).

In addition, the law gives the CNIL the possibility to reduce the notification burden in cases where the data processing does not present risks for privacy or civil liberties. The CNIL can publish simplified standards as it did under the previous law. Data processing which meets a standard's criteria would benefit from a simplified notification procedure. The CNIL could also issue notification exemptions in such cases. Anticipating the adoption of the law, the CNIL has already issued an exemption for payroll processing which complies with the corresponding standard.

Simplification of formalities can also be found in the possibility to notify the CNIL electronically, but most of all in the right for a body to make a single notification (this applies to the authorisation procedure) for several applications which have identical or connected purposes.

Note that article 23(2) of the law uses the term body ("organisme") rather than "controller". Hopefully, this will be interpreted as enabling a group of companies to make a single notification for the same data processing.

The notification would then need to have a common basis and specific sections for each application differing from the common basis. This provision may not make the exercise of notifying easier, but it will at least reduce the number of dockets filed by a company.

Continued on p.20

Appointing a data protection correspondent

The data protection "correspondent" must be a qualified person who shall keep a list of all data processing operated by the company and make it available to anyone upon request. The correspondent's appointment must be notified to the CNIL and he/she "may" bring issues to the attention of the CNIL. His/her independence must be ensured, therefore the correspondent cannot be sanctioned by the employer because of the performance of his/her functions.

In case of non compliance with the law, the correspondent will be asked by the CNIL to actually make the notifications. In addition, if he/she is found in breach of his/her duties, the correspondent may be discharged at the request of, or after consultation with, the CNIL.

For more detailed information see PL&B International, May/June 2004, p.17.

Article 7 (processing requirements)

Data processing must either have received the consent of the data subject or meet one of the following conditions:

- compliance with a legal obligation bearing upon the controller
- safeguard of the life of the data subject
- performance of a mission of public interest ("mission de service public") by the Controller or the data recipient
- performance of a contract with the data subject or pre-contractual measures made upon his/her request
- performance of a legitimate interest of the controller or of a recipient, provided that the interest or the fundamental rights and liberties of the interests of the data subject are not ignored.

- Unofficial translation