Have US laws set a trend for Europe? Are the current data protection laws sufficient?

Is there a need for specific legal provisions in Europe at EU and national level on action to be taken when personal data is lost or stolen?

Advantages & disadvantages of data breach notification provisions for DPAs, companies and individuals.

What would be an appropriate and proportionate response for data subjects?

Next steps for data breach notification at EU and national levels in Europe

Report
by Stewart Dresner and Amy Norcup

Results of PL&B’s European survey on attitudes of 21 European National Data Protection Authorities towards a European Union mandatory breach notification requirement and the introduction of national laws on action organisations must take when personal data is lost or stolen.

PL&B Client companies include:
25 of the Global Top 50, 24 of Europe’s Top 50,
25 of the UK Top 50 in the Financial Times lists;
10 of the Global Top 20 in the Fortune lists;
17 of the UK’s Top 20 law firms in the UK Legal 500.

Register for our events and get more information at www.privacylaws.com
The prospects for data breach laws in 21 European countries
Privacy Laws & Business Copyright © May 2009
13. Bibliography .................................................................................................................. 54

14. Appendices .................................................................................................................. 62

Appendix A: Country Reports

Austria ............................................................................................................................. 62
Belgium ............................................................................................................................ 65
Czech Republic ............................................................................................................... 67
Denmark .......................................................................................................................... 69
Finland ............................................................................................................................. 71
France ............................................................................................................................... 74
Germany .......................................................................................................................... 76
Guernsey ......................................................................................................................... 79
Hungary ........................................................................................................................... 82
Iceland .............................................................................................................................. 84
Ireland ............................................................................................................................. 86
Italy .................................................................................................................................. 88
Jersey ............................................................................................................................... 91
Luxembourg .................................................................................................................... 94
Netherlands ..................................................................................................................... 97
Poland ............................................................................................................................. 101
Portugal ........................................................................................................................... 104
Slovak Republic ............................................................................................................. 107
Spain ............................................................................................................................... 109
Sweden ............................................................................................................................ 112
Switzerland (David Rosenthal) .................................................................................... 115
UK ................................................................................................................................. 119

Appendix B: Datenschutz-Berater Survey ........................................................................ 123

Appendix C: Conference Report and European Parliament’s E-Privacy text ............... 126
1. Abstract

The Data Breach Notification laws which started in California in 2003, and have now spread over most of the USA, have provided a stimulus to companies doing business there to take the protection and use of the personal data in their care with much greater seriousness and commitment realising that their companies’ reputations are at stake.

In Europe, with national data protection laws already in place, as early as 1973 in Sweden, data security remains just one element of their comprehensive coverage. Notifying a national Data Protection Authority (DPA) when personal data has been lost or stolen is now under discussion and in some countries, on the political agenda. Notification of data breaches provides an instrument to assist Data Protection authorities and financial regulators to enforce the national data protection laws.

In the last two years, the question of whether the European Union should legislate on notifying data breaches has become an issue of conflict during the revision of the E-Privacy Directive. What constitutes a security breach, to whom should notification apply, and what should companies do?

Several questions arise which form the core of this Data Breach Survey conducted over 15 months by Privacy Laws & Business, and which focuses on the prospects of national data breach laws in 21 European countries. As such, this report offers a valuable insight into the current views of national Data Protection Authorities on the subject of breach notification. It suggests that amendments to data protection legislation at both the EU and national levels are likely, starting in the coming months, to tackle lost and stolen personal data, often known as data breaches. Privacy Laws & Business (PL&B) has addressed the following areas in all 21 countries:

- Current data breach laws
- Demand for data breach laws
- Impact of US breach notification laws in Europe
- Purpose and scope of new data breach provisions
- Regulatory options for implementing breach notification
- Advantages and disadvantages for national authorities, data subjects and companies.

From all the comments, PL&B has identified three potential regulatory options which could be combined or pursued separately in the future:

1. Insert new provisions into existing legislation
2. Amend the European Union’s (EU’s) E-communications draft directive or the general Data Protection (DP) directive as being recommended by the European Union’s Data Protection Supervisor
3. Publish practical Guidelines by the EU’s Article 29 DP Working Party.
2. Acknowledgements

Privacy Laws & Business (PL&B) would like to thank all the participants in the 21 national Data Protection Authorities in the survey whose names, job titles and organisations are listed in the section on DPA Participants (pp.7-8). We greatly respect their abilities to respond in English recognising that it is often their second or third language.

The research was greatly helped by visits by PL&B’s researcher, Amy Norcup, to: Antonio Caselli at the Garante (Italy’s Data Protection Authority) in Rome; and to Luxembourg where all three Data Protection Commissioners, Gérard Lommel, Thierry Lallemand, and Pierre Weimerskirch, participated in our interview. We appreciate Portugal’s Data Protection Commissioner, Dr. Luís Novais Lingnau da Silveira taking time during a visit to London to be interviewed by Amy Norcup and me. In the absence of an official view from Switzerland’s Data Protection Commission, David Rosenthal, Counsel at law firm, Homburger, in Zurich offered a ‘personal’ insight into data breaches in Switzerland. Hans Gliss, Editor of Datenschutz-Berater, Germany, translated and published the survey in his newsletter and helped us, together with Claus Ulmer, Executive Vice-President, Deutsche Telekom AG, to reach the appropriate people at Germany’s Federal DPA. Fabrizio Lelli, Vice-President, ABB Asea Brown Boveri Ltd in Zurich assisted us in making contact with the Swiss DPA.

Several organisations invited PL&B to address the results of this data breach survey on data breach notification in European countries in conference presentations by Stewart Dresner alone or with Amy Norcup. These events were: the Privacy Symposium at Harvard University (August 2008) in the USA; the United Kingdom’s Data Protection Forum (December 2008) in London; Israel’s Law, Information and Technology Authority (April 2009) in Tel Aviv; and Nymity.com (April 2009) in the form of an interview for its e-news. We also gave presentations at PL&B’s own 21st Annual International Conference in Cambridge (July 2008) and at our data breach conference in Edinburgh (April 2009). This week, Professor Artemi Rallo Lombarte, Director of Spain’s Data Protection Agency, invited me to address the 31st Annual Data Protection and Privacy Conference in Madrid in November this year on the prospects for data breach regulation in Europe.

This is, of course, an ongoing subject. European Commissioner for the Information Society, Viviane Reding, announced on May 6th that the new E-Privacy rules “introduce mandatory notifications for personal data breaches” by providers of communications networks and services. She was responding to the European Parliament which voted on the same day for data breach notification “regardless of sector or type of the data concerned.” Privacy Laws & Business is pleased to make this contribution to the policy making process. While many issues remain, such as the need to ensure consistent definitions for collection of statistics and action on data breaches, we have made a start to assess the regulatory landscape at national level.

We have made great efforts to not only accurately collect each Data Protection Authority’s views but also to give them an opportunity to review the draft report for their jurisdiction. If there are any changes of view due to policy changes or the passage of time, please inform us at e-mail addresses: amy.norcup@privacylaws.com and stewart.dresner@privacylaws.com

I gratefully acknowledge discussing the issues and research design with our editors, Laura Linkomies and James Michael. Laura prepared this report for publication with Glenn Daif-Burns who organised our Edinburgh conference which Adèle Kendler managed efficiently.

Last, but not least, I am delighted to express my appreciation to Amy Norcup, researcher and primary author of this report, who has been dedicated, determined and cheerful at all times. In retrospect, I was optimistic in January last year to expect this project to take only a few months. The effort in obtaining responses from 21 national Data Protection Authorities over more than a year has been worthwhile. We welcome your comments.

Stewart Dresner, Chief Executive, Privacy Laws & Business, May 8th 2009
3. Illustrations

Tables

Table 1 New Zealand’s Overview of the Privacy Breach Process (p.47)

Table 2 Data Security Breaches notified to the ICO since November 2007 – broken down by breach type and sector (p.49)
### 4. Data Protection Authority (DPA) Survey Participants

<table>
<thead>
<tr>
<th>Country</th>
<th>Contact</th>
<th>Role</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Georg Lechner</td>
<td>Datenschutzkommission</td>
<td>Email</td>
</tr>
<tr>
<td>Belgium</td>
<td>Willem Debeukelaure</td>
<td>Chairman</td>
<td>Email</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Jiri Mastalka, Vanda Vaculikova</td>
<td>Office for Personal DP</td>
<td>Email</td>
</tr>
<tr>
<td>Denmark</td>
<td>Jesper Husmer Pedersen</td>
<td>Head of Datailsynet – Danish DP Agency</td>
<td>Email</td>
</tr>
<tr>
<td>Finland</td>
<td>Reijo Aarnio</td>
<td>DP Ombudsman</td>
<td>Email</td>
</tr>
<tr>
<td>France</td>
<td></td>
<td>Head of European &amp; International Affairs, CNIL</td>
<td>Email</td>
</tr>
<tr>
<td>Germany</td>
<td>Helmut Heil</td>
<td>Senior Legal Advisor, Federal DP Commission</td>
<td>Email</td>
</tr>
<tr>
<td>Guernsey</td>
<td>Dr. Peter Harris</td>
<td>Commissioner</td>
<td>Telephone interview</td>
</tr>
<tr>
<td>Hungary</td>
<td>Friedler Gabor</td>
<td>Member of staff Hungary’s DPA</td>
<td>Email</td>
</tr>
<tr>
<td>Iceland</td>
<td>Bragi Axellson</td>
<td>Legal Counsel</td>
<td>Email</td>
</tr>
<tr>
<td>Ireland</td>
<td>Diarmuid Hallinan</td>
<td>Assistant Commissioner</td>
<td>Email</td>
</tr>
<tr>
<td>Italy</td>
<td>Antonio Caselli</td>
<td>International &amp; Communications Officer, Garante</td>
<td>Face-to-face interview</td>
</tr>
<tr>
<td>Country</td>
<td>Name</td>
<td>Position/Title</td>
<td>Contact Information</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Jersey</td>
<td>Emma Martins</td>
<td>Commissioner</td>
<td>Telephone interview</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>Gérard Lommel</td>
<td>Commissioners</td>
<td>Face-to-face interview</td>
</tr>
<tr>
<td></td>
<td>Thierry Lallemang</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pierre Weimerskirch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netherlands</td>
<td>Sjoera Nas</td>
<td>Senior Policy Officer</td>
<td>Email Registratiekamer</td>
</tr>
<tr>
<td>Poland</td>
<td>Piotr Drobek</td>
<td>Deputy Director, Social Education and International Cooperation Department</td>
<td>Email</td>
</tr>
<tr>
<td>Portugal</td>
<td>Dr. Luis Novais Lingnau da Silveira</td>
<td>Commissioner</td>
<td>Face-to-face interview</td>
</tr>
<tr>
<td></td>
<td>Dr Clara Guerra Vieira</td>
<td>International Relations Consultant</td>
<td>Email</td>
</tr>
<tr>
<td>Slovak Republic</td>
<td>Daniel Valentovic</td>
<td>Office for Personal Data Protection</td>
<td>Email</td>
</tr>
<tr>
<td>Spain</td>
<td>Head, International Dept.</td>
<td>AEPD (DP Agency)</td>
<td>Email</td>
</tr>
<tr>
<td>Sweden</td>
<td>Elisabeth Wallin</td>
<td>Member of Datainspektionen Swedish Data Inspection Board</td>
<td>Email</td>
</tr>
<tr>
<td>Switzerland</td>
<td>David Rosenthal</td>
<td>Legal Counsel Homburger, Zurich</td>
<td>Email</td>
</tr>
<tr>
<td>UK</td>
<td>David Evans</td>
<td>Senior DP Practice Manager, Information Commissioner’s Office</td>
<td>Email &amp; telephone interview</td>
</tr>
</tbody>
</table>
5. Introduction

An increase in data breaches has led to legislation in 44 states in the USA, Privacy Commissioners’ recommendations in Canada, Australia, New Zealand and Ireland, and legal provisions in several Asian countries.

To evaluate the need for data breach laws in Europe, PL&B asked 34 European Data Protection Authorities (DPAs) in January 2008 for their views on the prospect of a national data breach law. Responses were received from 21 national Data Protection Authorities:

- Austria
- France
- Ireland
- Poland
- Belgium
- Germany
- Italy
- Portugal
- Czech Republic
- Guernsey
- Jersey
- Slovak Republic
- Denmark
- Hungary
- Luxembourg
- Spain
- Finland
- Iceland
- Netherlands
- Sweden
- Switzerland (David Rosenthal)
- UK

This research is mainly based on email responses, but face-to-face interviews were conducted with the DPAs in Luxembourg and Italy and Portugal’s DP Commissioner in London. Telephone interviews were conducted with the Jersey and Guernsey DPAs. For Germany, we also refer to a survey distributed in Germany (Datenschutz-Berater www.datenschutz-berater/).

This research looks at the following areas:

- Current laws or regulations covering data breaches
- The demand for data breach laws
- The purpose and scope of data breach legislation
- Legal provisions to be included in any data breach law.

PL&B produced a report based on interviews with the first 11 DPAs to respond in the February 2008 edition of PL&B’s International Newsletter. We then addressed the topic at PL&B 21st Annual International Conference ‘Value Privacy, Secure your reputation, Reduce Risk’ at St John’s College Cambridge in July 2008. The findings of DPAs from 18 countries were then put to the Privacy Symposium at Harvard University in the US in August and in December 2008 to the UK Data Protection Forum at Clifford Chance, Canary Wharf. More recently, on 16th April, we gave a presentation to an audience of both public and private sectors and lawyers at the office of Israel’s DPA, the Law, Information and Technology Authority in Tel Aviv. Finally, on 22nd April 2009, PL&B organised a conference as the pre-event to the European Data Protection Commissioners’ Conference in Edinburgh to discuss the issue with both DPAs and companies.
6. PL&B Survey Questions

A. Current Data Breach Laws in your Country, if any

1. What law, if any, is currently in place in your country?

B. Demand for Data Breach Laws, if any

2. Do you as a DPA consider there to be a demand in your country for more explicit data breach laws?

3. Do you think a specific national law dealing with data breaches is necessary or is there enough ‘related law’ to achieve maximum protection against data breaches? Is the current problem of the loss or theft of personal data in your country at such a level to justify a national law?

4. In light of the adoption of data breach law in US, to what extent do you think your country should be following this example?

5. Do you consider existing data security provisions of your national Data Protection law sufficient?

C. Purpose and Scope of Data Breach Legislation

6. Should data breach law be consistent across the EU but have scope for national implementation to reflect national needs?

7. Do you think the scope of data breach law should include not only controllers but also processors? For example during the course of credit card transactions.

8. What do you consider to be the positive and negative impact of a national data breach law on data subjects?

9. Do you think that a national data breach law would help protect personal data more than current provisions?

10. What would be the expected impact of a data breach law? For example, to what extent do you think that national legislation dealing with data breaches will:

    (a) Help restore confidence and
    (b) Force businesses to take data breaches more seriously?

11. To what extent do you agree that the implementation of a national law will strengthen data security but restrict the free flow of data between both member states and third countries not in the European Economic Area?
D. Legal Provisions to be included in a Data Breach Law

12. Would it be enough to incorporate data breach law into other related areas of law such as theft or will it be necessary to move further than this and create a distinct piece of legislation?

13. What powers would your Data Protection Authority be seeking in a national law?

14. Would you expect your new legal provisions to cover both public and private sectors?

15. What would your DPA want from a national law?

16. What would your DPA want a data breach law to do in practice?

- Compensation to individuals
- Notifying the authorities of any breaches (if not the DPA, which authority?)
- Notifying customers
- Notifying staff
- Media plan
- Other, please specify
European Parliament’s legislative resolution of 6 May 2009 on data breach amendments to the European Union’s E-Privacy Directive


(Codecision procedure: second reading)

(45) The provider of a publicly available electronic communications service should take appropriate technical and organisational measures to ensure the security of its services. Without prejudice to Directive 95/46/EC, such measures should ensure that personal data can be accessed only by authorised personnel for legally authorised purposes, and that the personal data stored or transmitted, as well as the network and services, are protected. Moreover, a security policy with respect to the processing of personal data should be established in order to identify vulnerabilities in the system, and monitoring and preventive, corrective and mitigating action should be regularly carried out.

45a) The competent national authorities should promote the interests of the citizens of the European Union by, inter alia, contributing to ensuring a high level of protection of personal data and privacy. To this end, they should have the necessary means to perform their duties, including comprehensive and reliable data about actual security incidents that have led to the personal data of individuals being compromised. They should monitor measures taken and disseminate best practices among providers of publicly available electronic communications services. Providers should therefore maintain an inventory of personal data breaches to enable further analysis and evaluation by the competent national authorities.

(45b) Community law imposes duties on data controllers regarding the processing of personal data, including an obligation to implement appropriate technical and organisational protection measures against e.g. loss of data. The data breach notification requirements contained in Directive 2002/58/EC (Directive on privacy and electronic communications) provide a structure for notifying the competent authorities and individuals concerned when personal data has nevertheless been compromised. Those notification requirements are limited to security breaches which occur in the electronic communications sector. However, the notification of security breaches reflects a general interest of citizens to be informed about security failures which may result in their
personal data being lost or otherwise compromised and about available or advisable precautions that they may take in order to minimise possible economic loss or social harm that could result from such failures. This general interest for users to be notified is clearly not limited to the electronic communications sector and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at the Community level as a matter of priority. Pending a review to be carried out by the Commission of all relevant Community legislation in that regard, the Commission, in consultation with the European Data Protection Supervisor, should take appropriate steps without delay to encourage the application of the principles embodied in the data breach notification rules in Directive 2002/58/EC (Directive on privacy and electronic communications) throughout the Community, regardless of sector or type of the data concerned.

(46) Competent national authorities should monitor measures taken and disseminate best practices among providers of publicly available electronic communications services.

(47) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the subscriber or individual concerned. Therefore, as soon as the provider of publicly available electronic communications services becomes aware that such a breach has occurred, it should notify the breach to the competent national authority. The subscribers

(49) When implementing measures transposing Directive 2002/58/EC (Directive on privacy and electronic communications), the authorities and courts of the Member States should not only interpret their national law in a manner consistent with that Directive, but should also ensure that they do not rely on an interpretation of it which would conflict with fundamental rights or general principles of Community law, such as the principle of proportionality.

(50) Provision should be made for the adoption of technical implementing measures concerning the circumstances, format and procedures applicable to information and notification requirements to achieve an adequate level of privacy protection and security of personal data transmitted or processed in connection with the use of electronic communications networks in the internal market.

(51) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.

(52) Software that surreptitiously monitors the actions of the user or subverts the operation of the user's terminal equipment to the benefit of a third party ("spyware") poses a serious threat to the privacy of users, as do viruses. A high and equal level of
protection of the private sphere of users needs to be ensured, regardless of whether unwanted spying programmes or viruses are inadvertently downloaded via electronic communications networks or are delivered and installed in software distributed on other external data storage media, such as CDs, CD-ROMs or USB keys. Member States should encourage the provision of information to end-users about available precautions, and should encourage them to take the necessary steps to protect their terminal equipment against viruses and spyware.

(52a) Third parties may desire to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (e.g. certain types of cookies) to those involving unwarranted intrusion into the private sphere (e.g. spyware or viruses). It is therefore of paramount importance that users are provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access. The methods of giving information and offering the right to refuse should be made as user-friendly as possible. An exception to the obligation to provide information and offering the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user. Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's will to accept processing may be expressed by way of using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of the enhanced powers granted to the relevant national authorities under Article 15a of this Directive.

(52b) Safeguards provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes by means of electronic mail are also applicable to SMS, MMS and other kinds of similar applications.

(53) Electronic communications service providers make substantial investments in order to combat unsolicited commercial communications ("spam"). They are also in a better position than end-users in that they possess the knowledge and resources necessary to detect and identify spammers. Email service providers and other service providers should therefore be able to initiate legal action against spammers, and thus defend the interests of their customers, as part of their own legitimate business interests.

(54) The need to ensure an adequate level of protection of privacy and personal data transmitted and processed in connection with the use of electronic communications networks in the Community calls for effective implementation and enforcement powers in order to provide adequate incentives for compliance. Competent national authorities and, where appropriate, other relevant national bodies should have sufficient powers and resources to investigate cases of non-compliance effectively, including powers to obtain any relevant information they might need, to decide on complaints and to impose sanctions in cases of non-compliance.
(55) The implementation and enforcement of the provisions of this Directive often require cooperation between the national regulatory authorities of two or more Member States, for example in combating cross-border spam and spyware. In order to ensure smooth and rapid cooperation in such cases, procedures relating for example to the quantity and format of information exchanged between authorities, or deadlines to be complied with, should be defined by the relevant national authorities, subject to examination by the Commission. Such procedures will also allow the resulting obligations of market actors to be harmonised, contributing to the creation of a level playing field in the Community.

For individuals whose data and privacy could be adversely affected by such breaches should be notified without delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the subscriber's or individual's data and privacy where it entails e.g. identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the provision of publicly available communications services in the Community. The notification should include information about measures taken by the provider to address the breach, as well as recommendations for the subscriber or individual concerned.

HAVE ADOPTED THIS DIRECTIVE:

4) Article 4 shall be amended as follows:

a) the title shall be replaced by the following:

"Security of processing"

b) the following paragraph shall be inserted:

"1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:

–ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;

–protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and

–ensure the implementation of a security policy with respect to the processing of personal data.

Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve."
ba) the following paragraphs shall be added: "

3. In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.

When the personal data breach is likely to adversely affect the personal data and privacy of a subscriber or an individual, the provider shall also notify the subscriber or individual of the breach without undue delay.

Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorized to access the data.

Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so.

The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

4. Subject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which notification by providers of personal data breaches is required, the format of such notification and the manner in which the notification is to be made. They shall also be able to audit whether providers have complied with their notification obligations under this paragraph and impose appropriate sanctions in the event of a failure to do so.

Providers shall maintain an inventory of personal data breaches, comprising the facts surrounding such breaches, their effects and the remedial action taken, sufficient for the purpose of enabling the competent national authorities to verify compliance with the provisions of paragraph 3. The inventory shall only include the information necessary for this purpose.
DATA BREACH REPORT ORDER FORM

Personal Details
Name: ______________________
Position: ____________________
Organisation: ______________________
Address: ______________________
Postcode: ______________________
Tel: ______________________ Fax: ______________________
E-Mail: ______________________

Data Breach Report Fees
(Please tick your choices and delete as appropriate)

Data Breach Report for DPAs
☐ Report in pdf format based on the survey
  Survey participants: Free, other DPAs: £100 +15% VAT

Data Breach Report for Companies
☐ Report in pdf format based on the survey: £200 +15% VAT

Payment Options
VAT No.: 505 3809 59.
Address of Accounts (if different):
Postcode:

☐ Purchase Order
☐ Cheque payable to: Privacy Laws & Business
☐ Bank transfer direct to our account:
Privacy Laws & Business, Barclays Bank PLC,
355 Station Road, Harrow, Middlesex, HA1 2AN, UK.
Bank sort code: 20-37-16 Account No.: 20240664
IBAN: GB92 BARC 2037 1620 206 64 SWIFTBIC: BARCBGB2
Please send a copy of the transfer order with this form.
☐ American Express ☐ MasterCard ☐ Visa
Card Name: ______________________

Newsletter Subscriptions
☐ PL&B UK Annual Subscription £285
☐ PL&B International Annual Subscription £375
☐ International/UK Combined Annual Subscription £595
☐ Send me a FREE sample of the International/UK Newsletter
  Preferred Format: ☐ Print ☐ PDF (+15% VAT PDF version)

Expiration Date: ______________________

Total: £ ________________

Signature: ________________ Date: ________________

By signing this form, you agree that PL&B may process this data

Data Protection Notice Privacy Laws & Business will not pass on your details to third parties. We would like to send you information occasionally on privacy law services. Please indicate if you do not wish to be contacted by: ☐ Post ☐ E-mail ☐ Telephone.

Please return this form to: Privacy Laws & Business, 2nd Floor, Monument House, 215 Marsh Road, Pinner, Middlesex HA5 5NE, United Kingdom.

INTERNATIONAL & UK

newletters
The Essential Information Source for Privacy Law Compliance

Privacy Laws & Business has been providing data protection publications, conferences, advice and consultancy since 1987. It has become the comprehensive information source for privacy and data protection managers and lawyers.

Through a mixture of corporate case studies, legal analysis and advice, the Privacy Laws & Business newsletters:

► Show you where organisations have gone wrong, and how to go about correcting any problems
► Help your organisation benchmark its compliance practices and discover new ways of improving your procedures
► Provide you with expert comment from leading privacy consultants, managers, lawyers, and regulators.

Subscription Package:
► Six Newsletters a year
► E-Mail Updates
► Helpline Enquiry Service
► Newsletter Index

Electronic Format/Enterprise Licence
The newsletters are available in print and PDF formats. For an additional enterprise licence fee, you may upload the newsletters onto your Intranet or network. This option enables you to see the newsletters on any computer on your network and to print out pages at any location.

Subscription Prices
International Newsletter £375
UK Newsletter £285
Combined Subscription £595
Free sample issue available