The prospects of data breach laws in 18 European countries

Stewart Dresner, Chief Executive, Privacy Laws & Business

11:30 a.m. Privacy in Transition: The International Perspective

THE PRIVACY SYMPOSIUM - SUMMER 2008, HARVARD:
PRIVACY IN TRANSITION

August 18th – 21st 2008

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Contents

- Introduction
- The research
- Results: DPAs' views and preferred policies
- Advantages & disadvantages of a data breach law for DPAs, companies and individuals
- Common themes
- Recommendations by DPAs and companies
- Conclusions
- What next?

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Introduction

- US data breach laws
- Have these US laws set a trend for Europe or are the current data protection laws sufficient?
- Have US laws played a role in helping raise awareness?
- DP and privacy laws in the EU and US cover data security – is there a need for specific provisions on action to be taken when personal data is lost or stolen?

Research Scope

27 EU member states

All other countries within the European Economic Area:

- Norway, Iceland, Liechtenstein
- Switzerland
- Jersey, Guernsey, Isle of Man

Research Timeline

- **January**: Questionnaire by email to DPAs
- Follow-up telephone calls and emails
- Responses from: Czech Republic, Denmark, Finland, Guernsey, Hungary, Iceland, Ireland, Jersey, Slovak Republic, Sweden & United Kingdom
- EPON members' survey and results
- **February:** Report in PL&B's International newsletter
- **March:** Detailed report for DPAs and feedback
- **April**: Decision to pursue larger or more experienced countries and DPAs
- **May**: Responses from Italy, Spain, Portugal, Poland, Luxembourg, France and Belgium

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Research Method

- Email responses from most countries.
- Face-to-face interviews (Italy, Portugal, Luxembourg)
- Telephone interviews (Jersey, Guernsey)

Other Methods

- Survey distributed in Germany (Datenschutz Berater)
- National expert's comments in Switzerland (David Rosenthal, *Special Counsel, Member of IT & Telecommunications at Homburger, Zurich)*

Current data breach laws

- Data protection legislation in all countries but no *specific* stand-alone piece of legislation governing a data breach
- Data breaches covered by data protection laws, criminal & civil codes and additional e-communication legislation
- General application of this legislation to the unauthorised access, loss or theft of personal information
- Catalogue of legislation covering general data security but no specific mention of action to be taken in the event of a data breach.

Demand for data breach laws

- Rising number of reported data breach incidents
- Hot topic for the media and growing political interest
- Differing pressures in different countries
- Trend for data controllers to contact the authorities where data has been inappropriately released
- Some DPAs aware of only a small number of organisations suffering data breaches
- No Europe-wide demand for a specific data breach law as current legislation is sufficient in some countries

Demand for data breach laws

Current law is sufficient to deal with this problem

Denmark, Czech Republic, Hungary, France, Iceland, Spain, Switzerland

No definitive answer as to whether or not their existing legislation is sufficient

Slovak Republic, Belgium & Ireland

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

DPAs' views on purpose and scope of new data breach rules

1. Harmonisation within the EU and national implementation to reflect national needs
2. Any new data breach provisions to include both data controllers and data processors
3. Problems with breach notification in the US discourage Europe from following e.g. over-notification and inconsistency of reporting rules
4. Data breach provisions to cover both the public and private sectors
5. A 'multi-prong strategy' and strong intergovernmental links
6. Risks always attached to data processing

DPAs views on possible data breach laws 1

Agreement that some form of a data breach law would be a good idea. Three options or a combination:

1. Continue to insert data provisions into existing related legislation
2. Amend EU e-communications or general DP Directive
3. Practical Guidelines by the EU Art. 29 DP WP

Arguments for and against separate piece of legislation

One DPA suggested reasons for a separate data breach law:

- a vulnerable society is dependant on data security
- the need for building trust amongst data controllers

DPAs views on possible data breach laws 2

Some consistency is needed across Europe in this area *(All)*

EU should regulate first *(Guernsey)*

DPAs favouring amending their current data protection or other law to cover data breaches *(UK, Jersey, Finland, Poland, Portugal, Luxembourg, Italy)*

DPAs' Preferred Policies 1

1. More human and financial resources
2. Notification of data breaches.
3. Orders from DPAs to data controllers and processors to act in a specific way in response to a data breach.
4. Discretion to impose sanctions and appropriate fines
5. Compensation to individuals (in conjunction with civil law provisions)
6. Power to conduct audits when necessary

DPAs' Preferred Policies 2

7. DPAs favouring new provisions covering both the public and private sectors *(All)*
8. DPAs favouring new provisions to cover both data processors and controllers *(All DPAs apart from Ireland & Guernsey)*
9. DPAs favouring companies notifying them of data breaches *(UK,Jersey, Czech Republic, Guernsey, Ireland, Finland, France, Portugal, Luxembourg, Italy)*
10. DPAs favouring companies paying compensation to individuals *(Poland, UK, Finland, France & Italy)*
11. DPA offering data breach guidance *(UK)*

PL&B's Conclusions

The 'ideal' is a synthesis of DPAs' and companies' views which are also practical for data subjects. A data breach plan should be:

- proportionate
- an alert to a DPA when there is substantive rather than a procedural problem
- have more emphasis on a remedy to a problem, and
- less emphasis on sanctions

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

What next?

EU Level

1. Extension of EU e-communications directive to include data breach legislation for ISPs, other sectors
2. Amend general EU DP Directive
3. Practical guidelines by the Article 29 Working Party

National Level

1. Modest amendments to national laws
   e.g. Luxembourg amending DP code to include responsibilities of processors as well as controllers

Company Level

1. Broader breach management programmes
2. Continuing improvement of internal systems
   e.g. reporting mechanisms

…and full report from *Privacy Laws & Business*

Questions?

dresner@privacylaws.com

Stewart Dresner, Chief Executive

Privacy Laws & Business

Monument House, 215, Marsh Road, Pinner, Middlesex, United Kingdom

Telephone: + 44 (0) 868 9200 E-mail: stewart.dresner@privacylaws.com

www.privacylaws.com

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE