The Privacy, Data Protection and Cybersecurity Law Review

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 1
(published in November 2014 – editor Alan Charles Raul).

For further information please email
Nick.Barette@lbresearch.com

The Privacy, Data Protection and Cybersecurity Law Review

Editor

Alan Charles Raul

Law Business Research Ltd

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INTERNATIONAL INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

www.TheLawReviews.co.uk

PUBLISHER
Gideon Roberton

BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, James Spearing

ACCOUNT MANAGER
Felicity Bown

PUBLISHING COORDINATOR
Lucy Brewer

MARKETING ASSISTANT
Dominique Destrée

EDITORIAL ASSISTANT
Shani Bans

HEAD OF PRODUCTION AND DISTRIBUTION
Adam Myers

PRODUCTION EDITOR
Timothy Beaver

SUBEDITOR
Janina Godowska

MANAGING DIRECTOR
Richard Davey

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-909830-28-8

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following law firms for their learned assistance throughout the preparation of this book:

ASTREA

BALLAS, PELECANOS & ASSOCIATES LPC

BOGSCH & PARTNERS LAW FIRM

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JONES DAY

KIM & CHANG

NNOVATION LLP

NOERR

PINHEIRO NETO ADVOGADOS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SYNCH ADVOKAT AB

URÍA MENÉNDEZ ABOGADOS, SLP

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Editor's Preface v
Alan Charles Raul

Chapter 1 EUROPEAN UNION OVERVIEW.....1
William Long, Géraldine Scali and Alan Charles Raul

Chapter 2 APEC OVERVIEW.....19
Catherine Valerio Barrad and Alan Charles Raul

Chapter 3 BELGIUM 31
Steven De Schrijver and Thomas Daenens

Chapter 4 BRAZIL.....43
André Zonaro Giacchetta and Ciro Torres Freitas

Chapter 5 CANADA.....54
Shaun Brown

Chapter 6 FRANCE.....70
Merav Griguer

Chapter 7 GERMANY.....83
Jens-Marwin Koch

Chapter 8 GREECE.....98
George Ballas and Theodore Konstantakopoulos

Chapter 9 HONG KONG.....113
Yuet Ming Tham and Joanne Mok

Chapter 10 HUNGARY.....127
Tamás Gödölle and Péter Koczor

Chapter 11 ITALY....142
Stefano Macchi di Cellere

Chapter 12 JAPAN....156
Takahiro Nonaka

Chapter 13 KOREA....170
Jin Hwan Kim, Brian Tae-Hyun Chung, Jennifer S Keh and In Hwan Lee

Chapter 14 MEXICO....180
César G Cruz-Ayala and Diego Acosta-Chin

Chapter 15 RUSSIA....194
Vyacheslav Khayryuzov

Chapter 16 SINGAPORE....204
Yuet Ming Tham, Ijin Tan and Teena Zhang

Chapter 17 SPAIN....219
Cecilia Álvarez Rigaudias and Reyes Bermejo Bosch

Chapter 18 SWEDEN....230
Jim Runsten and Charlotta Emtefall

Chapter 19 TURKEY....241
Gönenç Gürkaynak and İlay Yılmaz

Chapter 20 UNITED KINGDOM....253
William Long and Géraldine Scali

Chapter 21 UNITED STATES....268
Alan Charles Raul, Tasha D Manoranjan and Vivek Mohan

Appendix 1 ABOUT THE AUTHORS....295

Appendix 2 CONTRIBUTING LAW FIRMS' CONTACT DETAILS....309

EDITOR'S PREFACE

The first edition of *The Privacy, Data Protection and Cybersecurity Law Review* appears at a time of extraordinary policy change and practical challenge for this field of law and regulation. In the United States, massive data breaches have vied with Edward Snowden and foreign state-sponsored hacking to make the biggest impression on both policymakers and the public. In Europe, the 'right to be forgotten', the draconian new penalties proposed in the draft Data Protection Regulation and the Snowden leaks, have significantly altered the policy landscape.

Moreover, the frenetic conversion of the global economy to an increasingly digital, internet-driven model is also stimulating a rapid change in privacy, data protection and cybersecurity laws and regulations. Governments are playing catch-up with technological innovation. It is reported that half the world's population will be online by 2016 and the economies of emerging nations (except, perhaps, in Africa) are being developed directly through electronic commerce rather than taking the intermediate step of industrial growth as Western economies did. Growth and change in this area is accelerating, and rapid changes in law and policy are to be expected.

In France, whistle-blowing hotlines are meticulously regulated, but now, in certain key areas like financial fraud or corruption, advance authorisation for the hotlines is automatic under a 2014 legal amendment. In Singapore, 2014 saw the first enforcement matter under that country's Personal Data Protection Act – imposing a financial penalty on a company that sent unsolicited telemarketing messages. In Russia, a new 2014 'forced localisation' law requires data about Russians to be stored on servers in-country rather than wherever the data can be most efficiently managed and processed, and jurisdictions around the world have debated enacting such proposals. Interestingly, while notice of the location of the relevant servers must be provided to the Russian data protection authority, it is not clear whether the law prohibits personal data to be simultaneously stored both in-country and in foreign servers.

The European Union continues to seek to extend its model for data protection regulation around the world by deeming only countries that adopt the 'omnibus' legislative approach of the EU to be 'adequate' for data protection purposes. The EU model is not being universally endorsed, even outside the US and the Asia and Pacific

Economic Cooperation (APEC) economies. But nonetheless, the EU's constraints on international data transfers have substantially inhibited the ability of multinational companies to move personal data around the world efficiently for business purposes. In particular, conflicts with the US abound, exacerbated by the Snowden leaks regarding US government surveillance. One of the primary methods by which such EU–US data flows are facilitated, the US–EU Safe Harbor regime, has come under attack from EU parliamentarians who believe that such information will not be as carefully protected in the US and could become more susceptible to surveillance, despite the comparable surveillance authorities of EU intelligence agencies.

While policy conflicts over data protection conflicts appeared to be moderating before the Snowden leaks, afterwards, officials around the world professed to be so shocked that governments were conducting surveillance against possible terrorists that they appear to have decided that US consumer companies should pay the price. Some observers believe that digital trade protection, and the desire to promote regional or national 'clouds', play some role in the antagonism leveled against US internet and technology companies.

The fact that the US does not have an omnibus data protection law, and thus does not have a top-level privacy regulator or coordinator, means that it has been difficult for the US to explain and advocate for its approach to protecting personal information. This has allowed the EU to fill a perceived policy void by denying mutual recognition to US practices, and to impose significant extraterritorial regulatory constraints on American and other non-European businesses.

Nevertheless, it cannot be denied that privacy enforcement in the US is distinctly more aggressive and punitive than anywhere else in the world, including the EU. Substantial investigations and financial recoveries have been conducted and achieved by the Federal Trade Commission (which has comprehensive jurisdiction over consumer data and business practices), 50 state attorneys general (who have even broader jurisdiction over consumer protection and business acts and practices), private class action lawyers who can bring broad legal suits in federal and state courts, and a plethora of other federal and state agencies, such as the Consumer Financial Protection Bureau, the Federal Communications Commission, the Department of Health and Human Services (for medical and health-care data), the Department of Education, the Securities and Exchange Commission and various banking and insurance agencies.

In sum, there are no shortage of privacy regulators and enforcers in the US, Europe, and Asia. Enforcement in South America, as well as Africa and the Middle East appears to be developing more slowly.

Trumping many other privacy concerns, however, is the spate of data breaches and hacking that have been epidemic and part of public discourse in the years following California's enactment of the first data breach notification law in 2003. While the US appears (as a consequence of mandatory reporting) to be suffering the bulk of major cyberattacks – on retailers, financial institutions and companies with intellectual property worth stealing by foreign competitors or governments – it is also true that the US is leading the rest of the world on data breach notification laws and laws requiring that companies adopt affirmative data security safeguards for personal information.

For corporate and critical infrastructure networks and databases, the US has also led the way with a presidential executive order and the Cybersecurity Framework

developed by the National Institute of Standards and Technology in the US Department of Commerce. The United Kingdom has also been a leader in this area, developing the UK CyberEssentials programme, which will soon include an option for companies to be certified as compliant with the programme's cybersecurity standards. The EU Parliament has also enacted cybersecurity directives, and the EU's European Network and Information Security Agency has provided extensive and expert analysis, guidance and recommendations for promoting cybersecurity for EU-based organisations.

Despite attempts to implement baselines for cyber safeguards, it appears that no one is immune and no organisation is sufficiently protected to have any confidence that it can avoid being the victim of successful cyberattacks, particularly by the sophisticated hackers employed by state sponsors, organised crime, social hacktivists or determined, renegade insiders (like Snowden). Government agencies and highly resourced private companies have been unable to prevent their networks from being penetrated, and sometimes are likely to identify 'advanced persistent threats' months after the malware has begun executing its malicious purposes. This phenomenally destructive situation cannot obtain, and presumably some more effective solutions will have to be identified, developed and implemented. What those remedies will be, however, is not at all clear as 2014 yields to 2015.

In the coming year, it would seem plausible that there could be efforts at international cooperation on cybersecurity as well as cross-border enforcement against privacy violators. Enforcers in the EU, US and among the APEC economies, may increasingly agree to work together to promote the shared values embodied in the 'fair information practices principles' that are common to most national privacy regimes. In early 2014, a step in this direction was taken when APEC and the European Union's Article 29 Working Party (on Data Protection) jointly released a framework by which international data transfers could be effectuated pursuant to the guidelines of both organisations.

Challenges and conflicts will continue to be factors with respect to: assurances of privacy protection 'in the cloud'; common understandings of limits on and transparency of government access to personal data stored either in the cloud, or by internet companies and service providers; differences about how and when information can be collected in Europe (and perhaps some other countries) and transmitted to the US for civil discovery and law enforcement or regulatory purposes; freedom of expression for internet posts and publications; the ability of companies to market on the internet and to track – and profile – users online through cookies and other persistent identifiers; and the deployment of drones for commercial and governmental data acquisition purposes.

The biggest looming issue of them all, however, will likely be 'big data'. This is a highly promising practice – based on data science and analytics – that collects and uses enormous quantities of disparate (and often unstructured) data, and applies creative new algorithms enabled by vastly cheaper and more powerful computer power and storage. Big data can discover helpful new patterns and make useful new predictions about health problems, civic needs, commercial efficiencies, and yes, consumer interests and preferences.

The potential social utility of big data has been unequivocally acknowledged by the US administration as well as by the key policymakers in the EU. But, big data challenges the existing privacy paradigm of notice and disclosure to individuals who are then free to

make choices about how and when their data can be used and collected. Many existing and proposed applications of big data only work if the vast stores of data collected by today's companies can be maintained and analysed irrespective of purpose limitations. Such limitations may have been relevant (and disclosed) at the point of collection, but no longer address the value of the data to companies and consumers who can benefit from big data applications. Numerous highly thoughtful reports by policymakers in the US and EU have noted concerns about the possibility that unfettered big data applications could result in hidden discrimination against certain demographic groups that might be difficult to identify and correct; or could result in undue profiling of individuals that might inhibit their autonomy, limit their financial, employment, insurance or even serendipitous choices, or possibly somehow encroach on their personal privacy (to the extent that otherwise aggregate or anonymous data can be re-identified).

This publication arrives at a time of enormous ferment for privacy, data protection and cybersecurity. Readers are invited to provide any suggestions for the next edition of this compendium, and we look forward to seeing how the many fascinating and consequential issues addressed here will evolve or develop in the next year.

Alan Charles Raul
Sidley Austin LLP
Washington, DC
November 2014

Chapter 18

SWEDEN

Jim Runsten and Charlotta Emtefall[1]

I OVERVIEW

The fundamental rights of freedom of expression and the right to privacy are laid down in the Swedish Constitution. Everyone shall be protected from secret interception, surveillance and severe intrusion into one's personal integrity. No legislation contrary to the European Convention on Human Rights may be issued.[2]

Although protection of privacy is a fundamental right, the legislation is not codified but scattered over several areas of law. Hence, the protection of privacy may be found within various areas, such as criminal, public and civil law. With regards to the protection of individuals against the violation of their personal integrity by the processing of personal data, the implementation of the Data Protection Directive 95/46/EC by the Personal Data Act (PDA) is fundamental. There are, however, about 100 acts regulating the processing of personal data. In addition, the Personal Data Ordinance authorises the Data Inspection Board (DIB) as the data protection regulatory authority to issue further regulations. The freedom of the press and right of freedom of expression set forth in the Constitution prevail over the provisions set forth in the PDA. In addition, certain provisions of the PDA shall not apply in relation to the processing of personal data made exclusively for the purpose of artistic or literary creation, or for journalistic purposes.

The Electronic Communication Act (ECA), applies to electronic communication services and networks, including internet and telecommunication services and networks. Under the ECA, privacy in the use of electronic communication services is regulated, including the use of cookies. Furthermore, the ECA, handles privacy intrusion issues such as legal interception and secret surveillance, which are strictly regulated and may only be undertaken within criminal investigations by the authorities.

1 Jim Runsten is a founder and Charlotta Emtefall is a lawyer at Synch Advokat AB.

2 The Instrument of Government, Chapter 2, Section 19.

Safeguarding cybersecurity within companies in general, beyond, for example, ISPs, telecommunications operators and data controllers, is based to a significant degree on non-binding advice provided by the authorities, and on voluntary security undertakings. Sweden is a member of the Council of Europe's Convention on Cybercrime. Existing criminal and procedural laws already fulfil to a great extent such Convention, and only few adjustments are likely to be made.

II THE YEAR IN REVIEW

The DIB has pursued investigations within several areas during the past year, in particular regarding the use of cloud computer services within municipal schools, where the use of cloud computing services has been increasing continuously. The DIB has reviewed data processing agreements between the cloud service providers and the respective municipalities, and concluded that some agreements do not fulfil the requirements set forth in Swedish legislation.

The invalidity of the Data Retention Directive as ruled by the European Court of Justice has been of great interest in Sweden. The government pursued a rapid analysis of the Swedish legislation implementing the Directive, concluding that despite the invalidity of the directive, Swedish legislation is proportionate and not in conflict with EU laws.

It has been revealed that the Swedish police authorities could categorise information in their general surveillance register in such a way that subjects' ethnicity could be revealed. One ethnic group in particular was exposed, and the procedure of registration was heavily debated and criticised. After conducting an investigation, the DIB ordered the police authorities to make adjustments to such registers, for example, by way of only registering only specifically important data and perhaps most importantly by erasing data that is no longer relevant, such as that of acquitted persons or where charges have been dropped.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The PDA applies to controllers established in Sweden, and to controllers established in third countries but where equipment in Sweden is used, provided such equipment is not used only to transfer data to third countries. For controllers based in third countries and where the PDA applies it is mandatory to appoint a representative established in Sweden.

The PDA applies to all wholly or partially automatic processing of personal data, including registers, databases and personal data contained in continuous text. The definition of personal data is broad,[3] hence almost any information that can be connected to a living natural person is considered being personal data. Both pictures, sound recordings and location data as well as more obvious data such as name, address,

3 The PDA defines personal data as any information that can be directly or indirectly connected to a natural living person.

phone number and national identification numbers constitute personal data, provided such data can be connected to a living person.

The PDA distinguishes between structured and unstructured processing of personal data. The first includes processing in regular data registers, databases and matter handling systems. The latter includes processing of unstructured material such as running text, pictures and sound. In order to facilitate 'everyday processing', the PDA includes exemptions from several regulations, as regards processing of unstructured material. Hence, unstructured processing may be undertaken more or less without restrictions provided, however, that the processing is not defamatory in relation to the data subject.

There is a distinction between personal data and sensitive personal data, where the latter include data revealing race or ethnic origin, political views, religion or philosophical conviction and union memberships, as well as data concerning a person's health or sexual life[4].

The PDA defines several terms, including the following:[5]

a 'processing' of personal data is every activity pursued with respect to personal data, regardless of whether such activity is made automatically or not, including for example, the collection, registration, organisation, storing, use, blocking, destruction or distribution of personal data;

b 'data subject' is the natural person whom the personal data concerns;

c 'controller' is the person who independently or jointly with others decides the purpose of and the means of the processing;

d 'processor' is the person who processes personal data on behalf of the controller; and

e 'data officer' is a natural person who has been appointed by the controller to independently safeguard the correct and legal processing of personal data.

The controller is responsible for processing the personal data, and may allow a data processor, and sub-processor(s), to process the personal data in accordance with the controller's instructions, which shall be set out in a written processor agreement. This agreement shall specifically state that that the processor must only process personal data in accordance with instructions by the controller, and that the processor is obliged to undertake the security measures that are set forth in the PDA.[6] The agreement may be made electronically.[7]

ii General obligations for data handlers

Under the main rule, the controller shall notify the DIB in writing before commencing any processing under the PDA. There are, however, a number of exemptions, of which the most important is whether the controller has appointed a data officer and notified the DIB of such appointment, then notification of the processing itself is not required.

4 The PDA Section 13.

5 The PDA Section 3.

6 The PDA Section 30.

7 The preparatory works to the PDA, Prop. 1997/98:44, p.136.

Hence, many corporations appoint a data officer, whereby notification of every processing can be avoided. Instead the data officer's tasks include keeping a list of the processing undertaken that should otherwise have been notified to the DIB if the data officer had not been appointed.

The controller shall ensure that personal data is processed only if the processing is legal, correct and in accordance with good practice. Furthermore, personal data must only be collected for specific, explicitly specified and legitimate purposes. The personal data must not be processed for any other purpose that is incompatible with the purpose for which the data was collected. In addition, the personal data shall be accurate and relevant in relation to the purpose of the processing, and more data than necessary with respect to the purpose of the processing must not be processed. The personal data shall be correct and if necessary, up to date. The data must not be stored any longer than necessary with respect to the purpose for which the data was collected.

Processing of personal data is subject to the grounds set forth in the PDA, for example, based on consent, the controller's fulfilment of legal obligations or subject to an assessment of interest between the controller and the data subject.[8] Consent is often used as the legal ground for personal data processing. A consent may, however, at any time be revoked by the data subject. Upon receipt of the data subject's withdrawal of consent, the controller may continue to process previously collected data based on the original consent. Such data may, however, not be updated, and since all data must be accurate and up to date, withdrawal of consent may cause the controller to delete data if such data would become inaccurate or incomplete.[9]

Processing of sensitive personal data is prohibited under the PDA, unless the data subject has explicitly consented to such processing, or if the data subject has clearly made the data publicly available.[10]

Any consent must be specific, unambiguous, freely given and informed,[11], namely, the data subject must be provided information on, *inter alia,* the purpose of the processing[12] before a valid consent may be given. The consent may be given orally, in writing or by way of pursuing a certain action, such as by ticking a box on a website. It is the controller's responsibility to prove the consent, hence it is advisable to always receive a well-documented consent. Consent must be obtained before the commencement of processing.

The controller shall provide the data subject with the following information:

a information of the controller's identity, including name and contact information to the controller,

b information on the purposes of the processing; and

8 The PDA Section 10.

9 Öman, Sören & Lindblom, Hans-Olof, *Personuppgiftslagen En kommentar*, 4 uppl. 2011, p.280.

10 The PDA Section 15.

11 The PDA Section 3.

12 The PDA Sections 23–25.

c all other information that the data subject may need to safeguard his or her rights in connection with the processing, including information of the receivers of the data, the obligation to provide information and the right to request information and correction of data.[13]

The controller is required upon the data subject's request, to free of charge, once annually, provide an excerpt of such person's processed data. The excerpt shall contain information of which data is processed, from where the data has been collected, the purposes of the processing and to which receivers or categories of receivers the data is provided. Such requests shall be in writing and must be signed by the data subject.[14]

The controller shall upon request by the data subject, urgently redress, block or destroy the personal data that has not been processed in accordance with the PDA. The request for correction may be submitted both orally and in writing.[15] It is the controller's choice whether to redress, block or destroy the data.[16]

iii Technological innovation and privacy law

New technology provides possibilities to track individuals and their behaviour both online and offline. In order to safeguard personal integrity and the right to privacy, it is important to understand the application of privacy laws to new technology. The PDA also applies to the processing of personal data when using new technology.

When using cloud services for the processing of personal data, the controller is always responsible. The cloud service provider and when applicable its subcontractors are data processors. The relationship between the parties shall therefore be regulated by written agreement as outlined above. The cloud service provider may often provide a standard agreement to be used. It is important to verify such agreement to make sure that the legal requirements are fulfilled. Furthermore, it is essential to know where the data will be processed, and if the processing involves transfer of data to third countries.

The use of cookies is subject to the ECA which applies to electronic communication networks and services offered to the Swedish market. A website user shall consent to the use of cookies. Since cookies are considered equipment[17] under the PDA, the requirements of consent set forth in such act apply. The user shall be informed of the use of cookies, the type of cookies used and the purpose of such use. Consent to the use of cookies shall be provided before any cookies may be placed on the user's computer. Many websites use a banner on the entrance page to provide cookie information, and to obtain consent. Such banner will stick on the site until the user actively consents to or rejects the use of cookies. Implied consent such as 'by the use of our services, you consent to the use of cookies' is not in accordance with Swedish legislation.

13 The PDA, Sections 23–25.

14 The PDA, Section 26.

15 The PDA Section 27, and Öman, Sören & Lindblom, Hans-Olof, *Personuppgiftslagen En kommentar*, 4 uppl. 2011, p.416.

16 The preparatory works to the PDA Prop 1997/98:44 p.134.

17 Article 29 Working Party Opinion 8/2010 on applicable law.

Sending direct marketing by e-mail and text messages (SMS) is allowed subject to consent by the receiver (opt in), unless the company has received the electronic contact information from the natural person in connection with selling its products or services to such person.[18] The consent must be unambiguous, specific, informed and provided freely. It is generally accepted that a user can opt in by clicking 'yes' in a tick-box on a website after having received sufficient information. However, the tick-box may not be pre-ticked.

GPS location systems in, for example, cars used by employees may have several advantages and may provide companies with several benefits. GPS location systems may contain data that can be indirectly connected to a living person, such as by connecting a certain taxi to the name of a certain driver, which will cause the PDA to apply. If data on a vehicle's speed is collected, it shall be noted that such collection may lead to the processing of criminal activities (i.e., speeding). Only public authorities may process such data, unless the DIB subject to request has expressly permitted the processing.

iv Specific regulatory areas

The PDA applies to all data subjects. In addition, legislation within specific regulatory areas (e.g., internet and telecommunication services) may provide additional protection. Under the ECA, operators have a fundamental confidentiality obligation, *inter alia*, with respect to information on the contents of an electronic message. Such information may only be revealed under certain circumstances, such as to law enforcement agencies as specified by the legislation. The confidentiality obligation has been intensely discussed in connection with the implementation of the Data Retention Directive, which does interfere with this obligation and therefore also with the right to privacy. In the light of the invalidity of the Data Retention Directive, Swedish legislation has been analysed. It has been concluded that the Swedish implementation is proportionate and fulfils the fundamental rights to privacy. Nevertheless, minor adjustments to the ECA may be proposed in the near future.

Furthermore, acts within the financial sector provide the right for certain organisations to process personal data as required by such legislation. Under the Anti-Money Laundering Act, specific obligations regarding the documentation of know-your-customer require processing of personal data. The Act also requires a certain duration of the storage of the personal data.

IV INTERNATIONAL DATA TRANSFER

Transfer of personal data to a third country without an adequate level of security is prohibited under the PDA. All countries outside the EEA are third countries. The prohibition applies to personal data being processed, as well to personal data that will be transferred for processing in the third country. The assessment of an adequate level of security shall be made with regards to all circumstances connected to the transfer, specifically the type of data, the purpose and duration of the processing, the country

18 The Marketing Act (2008:486), Section 19.

of origin, the country of final destination and the regulatory framework in the third country.[19] Nevertheless, transfer to third countries may be pursued based on consent by the data subject, or if transfer is necessary for the: (1) fulfilment of an agreement between the data subject and the controller, or for the fulfilment of requests by the data subject prior to entering into an agreement; (2) the fulfilment of an agreement between the controller and the third party that is in the interest of the data subject; (3) the identification, enforcement or defence of legal claims; or (4) the protection of the vital interests of the data subject.[20]

Exemptions from such prohibition, either to specific countries, or where the transfer is based on an agreement providing sufficient guarantees for protection of the rights of the data subjects may be granted by the DIB. The decisions of the EU Commission regarding which countries have an adequate level of security apply in Sweden.[21] The standard contractual clauses adopted by the EU Commission are considered to provide sufficient guarantees to the protection of rights of the data subject, and may therefore by used in the transfer of data from Sweden to third countries.[22] Provided that the EU standard contractual clauses are used for such transfer, the controller is neither required to submit the agreement regulating the transfer to the DIB, nor to receive an approval of the transfer from the DIB. Nevertheless, the actual processing of data may have to be notified to the DIB, unless any of the many exemptions apply. Furthermore, the Safe Harbor principles adopted in the USA have been considered by the EU Commission to provide an adequate level of security.[23] Hence, transfer of personal data from countries within the EU to organisations that have adopted the Safe Harbor Principles is permitted.

Transfer of personal data to third countries based on binding corporate rules, require submission of such rules to and approval by the DIB, before any transfer may take place.

V COMPANY POLICIES AND PRACTICES

Private organisations that process personal data are generally not obliged to implement specific privacy policies. Nevertheless, the controller is responsible for all processing of personal data and is obliged to inform the data subject of the processing. Such requirements may be fulfilled by the implementation of a policy. Various types of policies in relation to integrity are frequently used, including: (1) an internal personal data policy setting out the processing of employees' personal data, including any third-country transfer; (2) an internal cybersecurity policy, setting out the internal rules for the use of IT systems, devices including policies for bring your own device (employees using private devices for work-related matters); and (3) a privacy policy as regards the processing of personal data

19 The PDA Section 33.

20 The PDA Section 34.

21 The Personal Data Regulation (1998:1191) Section 13 including Annex 1.

22 The Personal Data Regulation (1998:1191) Section 13 including Annex 2.

23 Commission Decision of 26 July 2000 (2000/520/EC), implemented in Sweden by the Personal Data Ordinance.

in relation to third parties, such as customers. Notwithstanding the above, it shall be noted that legislation within specific regulatory areas, such as electronic communication, may require the operators to implement policies to fulfil mandatory requirements with regards to integrity.

A controller acting contrary to a policy that that controller has put in place is considered as interfering with good practice.

VI DISCOVERY AND DISCLOSURE

The concept of discovery or disclosure does not apply in Sweden. In Sweden, the principle of public access to official records is of fundamental importance and is laid down in the Constitution. This principle implies the right of access for the public and the press to activities pursued by the government and other authorities, including the right of access to documentation that is handled by authorities. Consequently, all documents submitted to Swedish authorities become official documents – unless the contents of these documents may be privileged for a particular reason – and may be requested by and therefore disclosed to anyone at any time.

The PDA does not apply in the event any provisions should limit the obligations of authorities to provide personal data under the principle of public access to official records. The principle of access to public records applies only in relation to authorities and not to private organisations.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The DIB has issued binding regulations and non-binding guidance within several areas, *inter alia*, the information to be provided to data subjects and personal data security. The guidance is not binding but serves as a recommendation on how the obligations set forth in the legislation can be achieved.

Subject to request, the DIB has the right to access: (1) personal data being processed; (2) information of and documentation regarding the processing of personal data as well as the security in the processing; and (3) the premises connected to the processing of personal data. The DIB continuously supervises its area of responsibility, which is primarily made by dialogue with controllers. In the event of illegal processing of personal data or if the DIB has noted any suspected illegal processing, the DIB is required, by way of feedback or the like, to try to achieve self-correction by the controller. If correction is not possible, or in case of an urgent matter, the DIB may prohibit the processing in other ways than by storing the data. A prohibition may also be combined with an administrative penalty of fines. It is, however, unusual that the DIB uses such right. The controller shall in general be provided with the possibility to give its opinion on the DIB's decision regarding the processing, before the DIB may impose any administrative fines.

In addition to the administrative rights of the DIB, the controller shall compensate the data subject to the damage and violation of integrity caused by the processing of personal data in violation of the PDA. Furthermore, violation of certain provisions of

the PDA caused by intent or gross negligence may attract criminal penalties of fines or imprisonment of up to six months. Should, however, the violation be severe, a sentence of up to two years' imprisonment may be imposed.[24] The number of court cases where sentences of imprisonment have been passed for breach of the PDA is very limited. Where prison sentences have been imposed, there have in general also been other crimes committed.

The DIB undertakes investigations regularly. The investigations are often undertaken within certain areas of activities. Recently the DIB investigated the processing of personal data in the electronic payment services area, as well as in the health-care service sector. Many controllers accept the decisions awarded by the DIB. Should the controller not accept a decision, it may be appealed to the administrative courts.[25]

The Post and Telecoms Authority (PTA) is empowered to supervise the ECA, for example, with regard to the use of cookies and the integrity with respect to electronic communications. The PTA keeps a close dialogue with the sector in matters regarding integrity. Furthermore, the PTA and the DIB cooperate within the area of integrity, in order to exchange experiences. The PTA is currently pursuing an investigation of the handling of cookies on various websites, including banks, authorities and social media. The investigation will result in orders, which will serve as guidance for website providers within several sectors.

ii Recent enforcement cases

Since 2011 the DIB has reviewed a number of cloud services used by Swedish municipalities and has come to the conclusion that their use of Google Apps for Education and Microsoft Office 365 was not in conformity with the requirements set out in the PDA. The DIB noticed that the use was regulated by a data processor agreement which in the DIB's opinion did not properly regulate the mandatory requirements stipulated by the PDA. Hence, the DIB ordered the municipalities to comply with the PDA. The DIB's order has now been confirmed by the administrative court.

An intense debate within the sector of telecommunications and ISPs was held in the light of the invalidity of the Data Retention Directive. The ECA implementing the Directive was, however, found to be proportionate and therefore not interfering with the Charter of Fundamental Rights of the European Union, mainly due to limitations in the duration of storage of data, the limitations on the provision of data to law enforcement agencies and the protection of the data.

The DIB has also ordered the Swedish police authorities to adjust their general surveillance register in response to a flaw whereby the ethnicity of persons on the register was identifiable (see Section II, *supra*).

iii Private litigation

Private litigation with respect to data protection legislation is rare in Sweden. However, during the past year the Superior Court ruled in one case whereby the publishing of a

24 PDA Sections 48–49.

25 PDA Section 51.

judgment in a civil case on a website was considered an infringement of the personal integrity of the person named in such judgment. Hence, the plaintiff was awarded damages of 3,000 kronor, which is a standard level for such damages.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

As further elaborated above, the PDA applies not only to controllers established in Sweden, but also to controllers that are established in third countries which use equipment located in Sweden for the processing of personal data. Since cookies are considered equipment, any cookies placed on a computer in Sweden will make Swedish legislation applicable. Hence, the use of cookies shall be made with precautions and at least be subject to the provision of information to and consent by the user.

Furthermore, the use of cloud computing services is increasing. It should be underlined that the party using a provider of cloud services is always the controller of the data processed in such cloud services. The cloud service provider is the processor with whom the controller shall enter into a written agreement covering the requirements set forth in the PDA. Since the cloud service provider is likely to propose the use of its own standard agreement, it is advisable to analyse that agreement in great detail and to verify that the agreement contains required provisions.

Multinational organisations transferring data to third countries are advised to analyse those transfers in detail and to establish policies for the transfer. It is further recommended to use the EU standard contractual clauses for transfer to third countries. The use of these clauses instead of, for example, binding corporate rules will save time and money since the EU standard contractual clauses have been approved by the DIB.

IX CYBERSECURITY AND DATA BREACHES

Under Swedish legislation service provider such as ISPs and telecoms operators are required to take adequate measures to secure reasonable requirements of security. Providers are required to report integrity incidents without undue delay to the PTA, and to the user, provided that the disclosed data may have a negative impact on him or her. Further, personal data controllers and processors are required to take adequate technical (such as implementing firewalls, encryption and antivirus measures) and organisational measures (including implementations of routines, instructions and policies) to protect the data.

Cybersecurity for other organisations in general is based on an implementation of voluntary cybersecurity measures. The PTA and the Swedish Civil Contingencies Agency[26] provide advice in relation to cybersecurity. In the absence of specific mandatory requirements it is, however, the responsibility of the management of a company to safeguard cybersecurity, including deciding the applicable level of security, the risk assessment and establishment of the relevant documentations (e.g., a cybersecurity policy).

26 www.msb.se.

The EU Cyber Crime Directive (2013/40/EU) was implemented in Sweden during 2014 by minor changes to existing criminal legislation. Furthermore, Sweden is a member of the Council of Europe's Convention on Cybercrime. It has, as a result of the implementation process, been concluded that Sweden by existing legislation fulfils most requirements. The initial analysis[27] has identified few modifications in existing legislation where adjustments and amendments are required. New legislation has, however, not yet been proposed.

X OUTLOOK

The development of new technology provides possibilities of an increased supervision of individuals. New technology combined with comprehensive use of smart phones has led to an extended collection of personal data and supervision of people's everyday life. It provides new business opportunities but it also results in increased processing of personal data and further intrusions in the personal integrity. Many people are concerned that mobile apps collect data without consent and also about the use companies may make of such data. Consequently, it is even more important from the legislator's perspective to safeguard the personal integrity. Hence, the supervising authorities will continue to investigate the compliance with the legislation protecting privacy.

The new EU Data Protection Regulation, which will strengthen online data protection rights, will have direct effect in Sweden. It is generally expected that the new regulation will be finalised during 2015, providing time thereafter for adaptation to such new legislation. The most significant consequences of such regulation include the establishment of a single European supervisory authority and the increased mandate to fine companies by up to 2 per cent of their global annual turnover. Since the established practice of the DIB with regard to fines is at a significantly lower amount, the new EU regulation may increase the general awareness by controllers of the Swedish data protection legislation.

27 SOU 2013:39, p.251

Appendix 1

ABOUT THE AUTHORS

JIM RUNSTEN

Synch Advokat AB

Jim Runsten is listed by the major ranking institutes, such as *Who's Who Legal: Internet, e-Commerce & Data Protection*, *Legal 500*, *Chambers & Partners* and *PLC Which Lawyer*, as one of the leading IT lawyers in Sweden as well as for general corporate and commercial work. Jim has extensive experience advising clients both locally and internationally on a wide range of strategic and technology transactional work, including outsourcing, M&A, financing and commercial contracts, such as the largest smart-metering outsourcing deal in the Nordics.

Jim Runsten has published several articles and contributed to books on various areas, including more recently together with Charlotta Emtefall articles in the *E-commerce Law Reports* and *E-Commerce Law and Policy*.

CHARLOTTA EMTEFALL

Synch Advokat AB

Charlotta Emtefall is an experienced lawyer within the IT and telecommunications areas with nearly 15 years of experience both as an in-house lawyer and as a consultant providing legal advice to Swedish and international clients. Charlotta's experience includes commercial and regulatory advice both within telecommunications, commercial IT law and data protection-related issues as well as within the payment services and electronic money areas. In addition Charlotta has extensive experience in marketing and consumer law, including disputes at the Swedish Market Court.

SYNCH ADVOKAT AB
Box 3631
103 59 Stockholm
Sweden
Tel: +46 8 761 35 35/+46 761 761 900
jim.runsten@synchlaw.se
charlotta.emtefall@synchlaw.se
www.synchlaw.se