This third edition of *Data Protection & Privacy* serves as an indispensable reference guide for companies, data protection officers, academics and legal professionals on the data protection and privacy laws in over 46 countries.

Written by expert local practitioners, with deep experience in the field of data protection and privacy, every chapter contains an overview of the key elements and principles of the data protection and privacy law framework in the relevant jurisdiction as well as the latest developments and trends.

ISBN 978-0-414-05733-3

9 780414 057333

SWEET & MAXWELL

DATA PROTECTION & PRIVACY

INTERNATIONAL SERIES

THIRD EDITION

THOMSON REUTERS

THIRD EDITION

DATA PROTECTION & PRIVACY

INTERNATIONAL SERIES

General Editor: Monika Kuschewsky
Covington & Burling LLP

SWEET & MAXWELL

THOMSON REUTERS

DATA PROTECTION & PRIVACY

INTERNATIONAL SERIES

Monika Kuschewsky
Covington & Burling LLP

THOMSON REUTERS

General Editor
Monika Kuschewsky

Commissioning Editor
Emily Kyriacou
emily.kyriacou@thomsonreuters.com

Commercial Director
Katie Burrington
katie.burrington@thomsonreuters.com

Publishing Editor
Dawn McGovern
dawn.mcgovern@thomsonreuters.com

Editor
Chris Myers
chris@forewords.co.uk

Editorial Publishing Co-ordinator
Gaby Mills-O'Brien
gaby.millso'brien@thomsonreuters.com

Published in August 2016 by Thomson Reuters (Professional) UK Limited, trading as Sweet & Maxwell
Friars House, 160 Blackfriars Road, London, SE1 8EZ
(Registered in England & Wales, Company No 1679046.
Registered Office and address for service:
2nd floor, 1 Mark Square, Leonard Street, London EC2A 4EG)
A CIP catalogue record for this book is available from the British Library.

Printed and bound by CPI Group (UK) Ltd, Croydon, CR0 4YY.

ISBN: 9780414057333

CONTENTS

CONTENTS

PREFACE

Monika Kuschewsky | Covington & Burling LLP

I am very pleased to present the third edition of this multi-jurisdictional handbook on data protection and privacy.

The new edition comes timely in the wake of the EU's fundamental reform of its data protection framework – the adoption of both the General Data Protection Regulation and the Network and Information Security Directive, the pending reform of the ePrivacy Directive and the adoption of the Privacy Shield, the successor of the EU–US Safe Harbour. There is also an increasing body of case law on data protection issues. The recent landmark cases *Google Spain*, *Schrems* and *Weltimmo* before the Court of Justice of the EU are prominent examples of this trend.

As this handbook demonstrates, data protection developments are not limited to Europe. This edition features 46 major jurisdictions from five continents, eight more than the second edition and 16 more than the first edition, which reflects the continuously growing number of countries with data protection laws. In addition to a chapter on the EU, the handbook also contains two Regional Summaries on the Asia-Pacific and Latin America.

Data protection has become a global issue and regulators strengthen their cooperation globally. The modernisation of the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), which is the first binding international instrument in the field of data protection, is coming to an end. Following Uruguay, Mauritius, a second non-European country, has recently acceded to the Convention. The ratification by Turkey will enter into force in September and accession by Morocco, Senegal and Tunisia is pending.

In March 2015, the UN Human Rights Council adopted a resolution which establishes a mandate on the right to privacy in the digital age and creates a new Special Rapporteur on the Right to Privacy. This resolution followed an earlier resolution on the right to privacy in the digital age adopted by the UN General Assembly in December 2014.

The Global Privacy Enforcement Network (GPEN), which aims to promote cross-border cooperation in data protection and privacy enforcement, has grown from 13 privacy enforcement authorities in 2010 to 59 authorities across 43 jurisdictions in 2015, with plans to further expand across Africa, Asia and South America. In 2015, GPEN undertook a major cooperative global sweep (which is the third of its kind) of websites and apps targeted at or popular with children, examining the privacy practices of approximately 1,500 apps and websites. Within GPEN, regulators share experience on hot topics of global relevance, such as children's privacy and big data.

The third edition of this handbook covers the major developments and trends that have occurred in the two years since the second edition was published. Like before, this edition covers, in summary form, key aspects of existing data protection and privacy laws and pending legislation; the data protection authorities; the legal basis for data processing and data quality requirements; information, registration and security obligations; rules on outsourcing and on international data transfers; rights of individuals; and enforcement trends, sanctions, remedies and liability. The handbook also addresses major elements of accountability, in particular, data protection impact assessments, audits, seals, data protection officers and industry self-regulation by codes of conduct. Moreover, it covers data protection aspects of major technological developments, such as big data, mobile apps, cloud computing, Bring Your Own Device (BYOD) and cybersecurity.

PREFACE

We have kept the reader-friendly Q&A format, which allows for easy cross-jurisdictional comparisons on key issues. Obviously, this book does not endeavour to cover the topics comprehensively and cannot substitute for the advice of local counsel. Rather, our goal is to provide a starting point for companies, legal professionals and data protection officers, reflecting the status of the law at the time of writing.

I would like to thank the contributors to this book, who are leading local practitioners and experts in the field of data protection and privacy, and also welcome back the data protection officer of the European Commission as a contributor. The book not only demonstrates the diversity in approach to data protection and privacy, but also highlights a number of commonalities. I therefore hope that it will not only help readers to gain a better understanding of the different rules, but also point the way towards greater interoperability and convergence among the various data protection frameworks, which is urgently needed.

Finally, I want to acknowledge the contributions and support of my colleagues and staff members at Covington & Burling LLP, as well as the publisher.

August 2016

FOREWORD

Giovanni Buttarelli | The European Data Protection Supervisor

Personal data moves around the world on a massive scale and in an instant. This is not just a by-product of globalisation; it is also increasingly, due to big data and the Internet of Things, a key driver of value for both businesses and governments.

Every time personal data is collected, stored, analysed or transferred, an individual is affected. For decades now, Europe has led the way in protecting the rights and interests of people about whom data is flowing constantly and more than ever before without their knowledge. The EU has promoted personal data processing as integral to the dynamic freedoms which underpin the internal market, while at the same time establishing, through the Charter for Fundamental Rights, a concise right to the protection of personal data, distinct from yet reinforcing the right to respect for privacy. It is extraordinary that, in the short time since the last edition of this important resource for privacy and data protection professionals, most countries in the world, in every continent, have now emulated the safeguards and standards which Europe has pioneered.

The third edition of *Data Protection & Privacy* documents, and coincides with, a rare watershed in data protection law. 2016 has seen the birth of a new generation of rules governing how personal data should be handled in the internet age. The EU, after more than four years of tough and passionate negotiations, has now adopted a comprehensive and ambitious framework in Regulation 679/2016, the General Data Protection Regulation and Directive 2016/680 on data protection in the police and criminal justice area. The Council of Europe is on the brink of finalising its modernisation of Convention 108 on the protection of individuals with regard to automated processing of personal data, which is in many ways the grandparent of all data protection laws. The EU is now considering how to update the protection of confidentiality of electronic communications – currently addressed by the ePrivacy Directive 58/2002/EC, an instrument formulated in a very recent but already almost unrecognisable era when people still communicated largely by fixed line and mobile telephony.

Meanwhile, the courts, and in particular the Court of Justice of the European Union (CJEU), are applying the rights and freedoms of individuals in the digital age with remarkable vigour and precision. As data flows across the globe, so flow the rights of individuals who are concerned by this data. This is most acutely the case with the intense debates over the necessity and proportionality of access to personal data by state authorities for the purpose of combating crime and terrorism. In the wake of the CJEU's landmark *Schrems* judgment of 2015, the EU and the United States have aimed to set a new and sustainable precedent for transfers of data from the EU.

All of these rapid developments in data processing and communications, pervading every aspect of commercial and civic life, point to a renewed, vital role for independent data protection and privacy authorities, such as my own institution. The CJEU has in the last few years established with crystal clarity the need for actual and visible independence of action and initiative on the part of these authorities, which are at once supervisors, ombudspersons, policy advisors and citizens' champions. It is therefore impossible to overstate the importance of how effectively and consistently these authorities apply the new generation of rules in cooperation with one another, such as through the European Data Protection Board set up under the General Data Protection Regulation.

The proliferation of data protection and privacy laws aims to provide clarity amid global economic and geopolitical uncertainty. This new edition of *Data Protection & Privacy* offers a valuable *vademecum* for anyone needing to navigate the growing body of complex yet converging global norms.

FOREWORD

Isabelle Falque-Pierrotin | Chair of the CNIL (Commission nationale de l'informatique et des libertés) and Chair of the Article 29 Data Protection Working Party

Our lives have gone digital. Not only has data become a ubiquitous buzzword that now rings to the ears of even the less tech savvy; it has also been for years now at the centre of our world. It has become key to business strategies, to governments and administrations. Our everyday lives now produce and consume massive amounts of data, and the trend is always stronger as the Internet of Things and cloud computing are growing at an impressive rate.

These developments make privacy & data protection one of the key issues of our times. No wonder the readers of the present book do not need being convinced of it. What is new, on the contrary, is the growing awareness in the general population of what is at stake. After years of what might now be seen as an age of "digital innocence", data protection is no longer a matter of interest only for specialised lawyers or privacy activists. Our societies begin to make out the main features of a digital world they have been living in for years without always being fully aware of all its implications. The Snowden disclosures have played a major role in triggering this phenomenon. Increasingly frequent headlines about data breaches and cybersecurity threats contribute to perpetuating and enhancing this new mood.

This rising anxiety is also a major opportunity. As data protection is turning into a matter of concern for consumers, citizens and businesses, it is also becoming a competitive argument and a lever for innovation. The launch of privacy-friendly search engines onto the market in the last few years illustrates how entrepreneurs have already begun to answer these new social expectations.

Data protection is also at a turning point in the legal and political realm, and Europe is at the forefront of it.

The recently adopted General Data Protection Regulation will enter into force in 2018. It will set the new legal framework of the digital Europe for the 21st century, having a significant impact on the public authorities, the citizens and private companies. The GDPR brings about new rights for the individuals. To put it more precisely, it upgrades data protection and the humanist values upon which our legal system is based so as to make them more effective in the digital world. It also imposes new compliance obligations on the companies. No doubt the data protection officers will take up a decisive role in the privacy community in the coming years. Last but not least, the GDPR sets up a new governance model, decentralised and integrated at the same time. Based on powerful and independent national data protection authorities (DPAs), it will also imply more coordination between the latter. This major organisational shift will enhance Europe's negotiating capabilities. However, its implementation and the one-stop-shop mechanism will demand significant adaptation by the DPAs in the coming years. To fulfil their mission, they will have to strengthen the collaborative culture they have begun to forge within the Article 29 Data Protection Working Party (Working Party).

The GDPR paves the way for a much more co-regulated data protection. In this new context, ensuring a high level of data protection does not rest on the DPAs alone; it also becomes a task to be carried out by private companies and individuals. The very way the Working Party is preparing for the coming into force of the new regulation has to reflect this co-constructed approach. That is why the DPAs have invited the stakeholders to share their views on the GDPR and to take part in a kind of policy "Fab lab" on the GDPR in July 2016. This initiative embodies a major cultural change in the field of data protection in Europe towards more collaborative thinking and action.

FOREWORD

The second significant shift in the realm of data protection is to be found in the aftermath of the striking down of the Safe Harbour Agreement by the Court of Justice of the European Union (CJEU) in October 2015. This ruling has indeed reshaped the international data landscape. Adequacy decisions are particularly impacted. They will hitherto require the taking into account not only of the national data protection legislation, but also of the national judicial system in its entirety. The CJEU ruling also raises fundamental issues about sovereignty and the overlap of national jurisdictions in the age of data. At the time of writing, no one knows what the final result of the Privacy Shield negotiations will be. What is certain, though, is that the need for international standards in order to secure the environment of big data is pressing. This is a very positive element in the making of an international governance of data flows.

It is therefore obvious that the data protection community in Europe is facing major challenges for the coming years. At the core of these challenges is an unprecedented need to cooperate and build bridges between national or regional legal systems.

It is one of the many virtues of a comprehensive publication like this to provide professionals with the necessary material to build such bridges, beyond the indispensable task of advising their clients on compliance, users' expectations and regulators' requirements. I therefore wish to congratulate the editors for taking the initiative to publish a third edition of this handbook. It will, no doubt, contribute to making progress in the implementation of data protection and privacy laws in the EU and elsewhere.

LITHUANIA

Dr Jaunius Gumbis and Dr Julius Zaleskis | Valiunas Ellex/Vilnius University Law Faculty

1. LEGISLATION

1.1 Name/title of the law

In Lithuania, the collection and processing of personal data is regulated by the Law on Legal Protection of Personal Data of the Republic of Lithuania (Data Protection Law).

The Data Protection Law implements the EU Data Protection Directive 95/46/EC (the Directive). Lithuania passed the Data Protection Law on 11 June 1996, and it has since been amended on 17 July 2000, 22 January 2002 and 21 January 2003 in order to transpose the provisions from the Directive. The latest modifications to the Data Protection Law came into force on 1 September 2011. They include amendments and new regulations on public polls, credit-referencing agencies and public governance of data protection. Enforcement is carried out by the State Data Protection Inspectorate (the Inspectorate).

In addition, protection of privacy in the area of electronic communications is governed by the Law on Electronic Communications dated 15 April 2004, which has transposed the ePrivacy Directive 2002/58/EC, as amended by Directive 2009/136/EC, and the Data Retention Directive 2006/24/EC.

The Inspectorate has issued only a limited number of guidelines on particular data protection issues. Opinions and recommendations of the Article 29 Data Protection Working Party (the Working Party) are often followed by the Inspectorate and Lithuanian courts while interpreting abstract provisions of the Data Protection Law.

1.2 Pending legislation

There is no pending legislation that would affect or amend the Data Protection Law. Currently there is no indication as to how Lithuania will implement the EU General Data Protection Regulation.

1.3 Scope of the law

The Data Protection Law applies to both the private and public sectors.

1.3.1 The main players

- The "data controller" is any legal or a natural person which alone or jointly with others determines the purposes and means of processing personal data. Where the purposes of processing personal data are laid down in laws or other legal acts, the data controller and/or the procedure for his/her nomination may be laid down in such laws or other legal acts.
- The "data processor" is any legal or a natural person other than an employee of the data controller who is processing personal data on behalf of the data controller. The data processor and/or the procedure for his/her appointment may be laid down in laws or other legal acts.

- The "third party" is any legal or a natural person, with the exception of the data subject, the data controller, the data processor and persons who have been directly authorised by the data controller or the data processor to process personal data.
- The "data recipient" is a legal or a natural person to whom personal data is disclosed, except certain authorities supervising the implementation of the Data Protection Law as well as other state and municipal institutions and agencies which obtain personal data in response to a specific request for the purposes of fulfilling their control functions laid down in laws.

1.3.2 Types of data

The Data Protection Law distinguishes two types of data – personal data and sensitive data. "Personal data" is defined as any information relating to a natural person (the "data subject") who is known or who can be identified directly or indirectly by reference to such data as a personal identification number or one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. The Data Protection Law does not protect data on companies.

In addition, the Data Protection Law defines "sensitive data" as data concerning racial or ethnic origin of a natural person, his/her political opinions or religious, philosophical or other beliefs, trade union membership, and his/her health, sex life and criminal convictions.

1.3.3 Types of acts/operations

The Data Protection Law regulates relations arising both in the course of the processing of personal data by automatic means and during the processing of personal data by other than automatic means in "filing systems": any structured set of personal data arranged in accordance with specific criteria relating to the person, allowing an easy access to personal data in the file (lists, card indexes, files, codes and so on).

"Processing" is defined as any action carried out with personal data: collection, recording, accumulation, storage, classification, grouping, connecting, changing (supplementation or correction), provision, publication, use, logical and/or arithmetical operations, search, dissemination, destruction or any other action or set of actions.

1.3.4 Exceptions

The Data Protection Law does not apply if personal data is processed by a natural person only for his/her personal needs not relating to business or profession. When personal data is processed for the purposes of state security or defence, the Data Protection Law shall apply to the extent that other laws do not provide otherwise.

Furthermore, only a limited number of provisions of the Data Protection Law apply to the processing of personal data by the media for the purpose of providing information to the public for artistic and literary expression.

1.3.5 Geographical scope of application

The Data Protection Law shall apply to the processing of personal data where:

- Personal data is processed by a data controller established and operating on the territory of Lithuania as a part of his/her activities. Where personal data is processed by a branch office or a representative office of a data controller of a another state of the EEA, established and operating in Lithuania, such a branch office or

representative office shall be subject to the provisions of the Data Protection Law applicable to Lithuanian data controllers.

- Personal data is processed by a data controller established and operating in a non-EEA country if the data controller uses personal data processing means (equipment) in Lithuania, except where such equipment is only used for the transit of data through the territory of Lithuania, the EU or another state of the EEA.

1.3.6 Particularities

Not applicable.

2. DATA PROTECTION AUTHORITY

The body responsible for the supervision and control of enforcement of the Data Protection Law in Lithuania is the Inspectorate:

The State Data Protection Inspectorate
(Valstybinė asmens duomenu apsaugos inspekcija)
Juozapavičiaus str 6
LT-09310 Vilnius
Lithuania
t +370 5 279 1445
f +370 5 261 9494
w www.ada.lt

2.1 Role and tasks

The Inspectorate's mission is to ensure a high level of data protection by monitoring and enforcing the Data Protection Law. The Inspectorate tries to ensure that data controllers and providers of public communications networks and publicly available electronic communications services fulfil the data protection requirements. The Inspectorate holds a public register of data controllers.

2.2 Powers

The powers of the Inspectorate are laid down in the Data Protection Law. The Inspectorate has the power:

- To obtain from legal and natural persons all the information and documentation necessary for the discharge of the Inspectorate's functions of supervision of personal data processing.
- To obtain access to premises of the person being checked, or to the territory where the documents and equipment relating to the processing of the personal data is kept.
- To make recommendations and give instructions to the data controller on personal data processing and protection issues.

- To take part in legal proceedings concerning violations of the provisions of international and national law on personal data protection.
- To grant permission to process personal data in Lithuania and to transfer it outside the EU/EEA.

For enforcement powers, see *Section 14* below.

2.3 Priorities

The Inspectorate publishes its work programme and priorities on its website. According to the 2016–18 Strategic Action Plan, the main priority of the Inspectorate is to increase data controllers' awareness of data protection requirements.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

"Consent" is defined as an indication of will given freely by a data subject indicating his/her agreement with the processing of his/her personal data for the purposes known to him/her.

3.1.2 Form

There is no requirement for consent to be in a written form. Consent should be given voluntarily. Consent can be either implicit or explicit. Electronic consent is possible; however, it is customary to obtain consent in a written form for evidential purposes. The burden of proof for the existence of the consent is on the data controller.

Consent with regard to sensitive data must be expressed clearly, in a written or equivalent form, or any other form giving unambiguous evidence of the data subject's free will.

3.2 Other legal grounds for data processing

Personal data may also be processed if one or more of the following grounds are present:

- Processing is necessary for a contract to which the data subject is a party or a contract concluded with the data subject.
- It is a legal obligation of the data controller under law to process personal data.
- Processing is necessary in order to protect vital interests of the data subject.
- Processing is necessary for the exercise of official authority vested by laws and other legal acts in state and municipal institutions or a third party to whom the personal data is disclosed.
- Processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party to whom the personal data is disclosed, unless such interests are overridden by the interests of the data subject.

The Data Protection Law prohibits the processing of sensitive data, except in the following cases:

- The data subject has given his/her consent.
- Such processing is necessary for the purposes of employment or civil service while exercising rights and fulfilling obligations of the data controller in the field of labour law only in the cases laid down by law.
- It is necessary to protect vital interests of the data subject or of any other person, where the data subject is unable to give his/her consent due to a physical disability or legal incapacity.
- Processing of personal data is carried out for political, philosophical or religious purposes, or for purposes concerning trade unions, or by a foundation, association or any other non-profit organisation as part of its activities, on condition that the personal data processed concerns solely the members of such organisation or other persons who regularly participate in such organisation in connection with its purposes. Such personal data may, however, not be disclosed to a third party without the data subject's consent.
- The personal data has been made public by the data subject.
- The personal data is necessary, in the cases laid down by law, in order to prevent and investigate criminal or other illegal activities.
- The personal data is necessary for a court hearing.
- It is a legal obligation of the data controller under law to process such data.

3.3 Codes of conduct

Not applicable.

4. SPECIAL RULES

The Data Protection Law contains specific rules in the areas of social security, health data processing, elections, scientific research, statistics, public polls, direct marketing, video surveillance, debtors' data processing and credit referencing.

4.1 Employment

The Data Protection Law does not provide for any specific rules regarding processing of personal data in the employment relationship or for employees' personal data, except for the specific legal ground that may justify the processing of sensitive data for the purposes of employment (*see Section 3.2 above*).

In practice, the Inspectorate usually does not accept an employee's consent as a legal basis of processing an employee's personal data unless the employer can prove that the employee could refuse consent without facing negative consequences.

The Data Protection Law stipulates that, for the purposes of social insurance and social assistance, administrative institutions of the State Social Insurance Fund and legal persons providing or administering social assistance shall exchange personal data without the data subject's consent.

4.2 Health

Personal data on a person's health has the status of sensitive data; therefore, it may be processed only on the basis of special grounds (*see Section 3.2 above*). Information on a person's health is subject to professional secrecy under the Civil Code, laws regulating patients' rights and other legal acts. Prior authorisation by the Inspectorate is required for the processing of health-related personal data by automatic means and for scientific medical research purposes.

4.3 Finance

The Data Protection Law provides for special rules regarding personal data processing for the purpose of evaluating a person's solvency and managing his/her debt.

The data controller has the right to process and disclose the personal data of data subjects who have failed to fulfil, in a timely and proper manner, their financial and/or property obligations vis-à-vis the data controller for the purpose of evaluating their solvency and managing their debt to third parties having legitimate interests.

Credit institutions and financial undertakings providing financial services relating to risk acceptance or credit rating have the right to process and to receive from each other the personal data of the data subjects to whom the credit institutions and financial undertakings have rendered or intend to render financial services and of the data subjects providing security for obligations to the above-mentioned institutions and undertakings, for the purposes of evaluating a person's solvency and financial risk, as well as debt management, on the condition that the data subjects have given their consent.

Where the data subject gives his/her consent, his/her personal data may be processed for the purposes of evaluating his/her solvency, financial risk and debt management, and may be regularly updated in consolidated files of financial risk under the data disclosure contracts concluded between financial institutions.

4.4 Telecommunications

The rules regarding the processing of telecommunications data are provided in the Law on Electronic Communications. This law prohibits listening, tapping, storing or otherwise intercepting information or related traffic data, or gaining secret access to such information or related traffic data without the consent of the actual users of electronic communications services, except when legally authorised to do so.

It is also forbidden to disclose the content of information transmitted over electronic communications networks and/or related traffic data without the consent of the actual users of these services or to create conditions for gaining access to such information and/or related traffic data.

Pursuant to the Law on Electronic Communications, traffic data held by public electronic communications services providers (CSPs) must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication. However, traffic data can be retained if:

- It is being used to provide a value-added service.
- Consent has been given for the retention of the traffic data.

- It is required for the investigation of a serious crime.

Traffic data can only be processed by a CSP for:

- The management of business needs, such as billing or traffic.
- Dealing with customer enquiries.
- The prevention of fraud.
- The provision of a value-added service.

Location data may only be processed for the provision of value-added service with consent. The CSPs are also required to take measures, including by implementing a policy, to ensure the security of the personal data they process.

4.5 Historical, statistical and scientific research purposes

The Data Protection Law provides an exemption from the general rule and states that personal data collected for other purposes may be processed for statistical, historical or scientific research purposes only in the cases laid down by law, provided that adequate data protection measures are laid down in said law.

Personal data may be processed for the purposes of scientific research on condition that the data subject has given his/her consent. Without the data subject's consent, personal data may be processed for the purposes of scientific research only upon obtaining authorisation by the Inspectorate. In this case, the Inspectorate must carry out a prior check and issue an authorisation (*see Section 12.2 below*).

Personal data which has been used for the purposes of scientific research must be altered in a manner which makes it impossible to identify the data subject. In cases where the conducted research does not require personal data, the data controller should provide to the data recipient such data from which identification of a person is not possible (anonymised data). Research results can be published together with the personal data on the condition that the data subject has given his/her consent to the publication of his/her personal data.

Processing of personal data for statistical purposes shall mean the carrying out of statistical surveys and disclosure and storage of the results. Such data can be compared and combined only on condition that the personal data is protected against unlawful use for other than statistical purposes. Sensitive data can be collected for statistical purposes solely in a form which does not permit direct or indirect identification of the data subject, except in the cases laid down by law.

4.6 Children

Not applicable.

4.7 Whistleblowing

There are no specific data protection rules or guidance regarding whistleblowing; however, in practice, the Inspectorate follows the opinion of the Working Party.

4.8 Email, internet and video monitoring

There are no specific data protection rules applicable to the monitoring of email and internet use. In practice, the Inspectorate follows the opinion of the Working Party regarding these issues.

Video surveillance is allowed for the purpose of ensuring public safety, public order and protecting a person's life, health, property and rights and freedoms, but only in cases where other ways or measures are insufficient and/or inadequate for the achievement of the above-mentioned purposes unless they are overridden by the interests of the data subject. In addition, video surveillance is subject to notification to the Inspectorate. In all cases, data subjects must be warned about video surveillance.

4.9 Direct marketing and cookies

The Data Protection Law and the Law on Electronic Communications require individuals to consent to the processing of their personal data for direct marketing purposes in advance (that is, a right to "opt in").

There is one exception to the opt-in requirement, providing instead for an opt-out scheme: namely, unsolicited electronic marketing, including emails, can be sent without consent if:

- The contact details have been provided in the course of a sale and the data subject is an existing customer.
- The marketing relates to a similar product.
- The data recipient was given a means of refusing the use of his/her contact details for marketing when the contact details were collected.
- The data recipient did not object to the direct marketing use at the time when his/her personal data was collected.

Direct marketing communication must not disguise or conceal the identity of the sender. SMS marketing is included within the regulations, applicable to all direct marketing.

Under the Law on Electronic Communications, the use and storage of cookies require: (i) clear and comprehensive information provided to data subjects; and (ii) the consent of the website user. Consent is not required for cookies that are: (i) used for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) strictly necessary for the provision of a service requested by the user.

The Inspectorate has published recommendations about the method of obtaining consent for the use of cookies. The recommendations confirmed that consent can be obtained through pop-ups, banners or website registration, whereas relevant settings contained within current browsers are not likely to form a valid consent. According to the recommendations, the users must be given a genuine opportunity not to consent. There is no clear guidance on the possibility of obtaining implied consent.

4.10 Big data

Not applicable.

4.11 Mobile apps

Not applicable.

5. DATA QUALITY REQUIREMENTS

The Data Protection Law stipulates a number of requirements for the quality of the personal data. The data controller must ensure that personal data is collected for specified and legitimate purposes and is not subsequently processed for purposes incompatible with those purposes before the personal data concerned is collected. Data should be processed accurately, fairly and lawfully, and be up to date. Inaccurate or incomplete data must be rectified, supplemented or erased, or its further processing must be suspended.

Furthermore, the personal data should be relevant, adequate and not excessive in relation to the purpose for which it is collected and further processed. It should be kept in a form which permits identification of data subjects for no longer than necessary for the purpose for which it was collected and processed.

6. OUTSOURCING AND DUE DILIGENCE

6.1 Outsourcing

Where the data controller authorises a third party to process personal data on his/her behalf, he/she must choose a data processor providing guarantees in respect of adequate technical and organisational data protection measures and ensuring compliance with those measures. The data controller must conclude a contract with the data processor, including obligations to follow the data controller's instructions and to implement appropriate organisational and technical measures to protect personal data against accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

6.2 Due diligence

Not applicable.

7. INTERNATIONAL DATA TRANSFERS

7.1 Applicable rules

Data controllers can transfer personal data within the EU/EEA without any additional restrictions. All cross-border transfers of personal data within the EU/EEA (the EU countries plus Norway, Liechtenstein and Iceland) takes place under the same conditions and in accordance with the same procedure applicable to data recipients in Lithuania.

Data transfers to countries which have been recognised by the European Commission as providing an adequate level of protection are also recognised as such by the Inspectorate. Otherwise, cross-border data transfers outside the EU/EEA are subject to special authorisation from the Inspectorate unless the exceptional conditions for cross-border data transfer are satisfied (*see Section 12.2.3 below*).

Authorisation to transfer personal data outside the EU/EEA by the Inspectorate is granted if the data controllers demonstrate an adequate level of legal protection for the data in the course of the transfer. Data controllers can

demonstrate an adequate level of legal protection by using data transfer agreements or binding corporate rules (BCRs) (*see Section 7.2 below*).

7.2 Legal basis for international data transfers

7.2.1 Data transfer agreements

Data transfers under the standard contractual clauses approved by the European Commission, or other agreements incorporating these clauses, are recognised by the Inspectorate as demonstrating an adequate level of legal protection.

7.2.2 Binding corporate rules

BCRs are recognised as demonstrating an adequate level of legal protection provided that they are approved by a data protection authority of an EU member state. However, Lithuania does not participate in the mutual recognition procedure of BCRs. In any case, authorisation must be obtained from the Inspectorate for data transfers on the basis of BCRs. According to available information, no BCRs have been specifically authorised by the Inspectorate.

7.2.3 Safe Harbour and Privacy Shield

After the annulment of the European Commission's Safe Harbour decision in the *Schrems* case of the Court of Justice of the EU (CJEU), the Inspectorate issued the following guidance:

The Inspectorate shall issue decisions to authorise the transfer of personal data to the US based on the approval of the standard contractual clauses or BRCs.

Previously issued decisions of the Inspectorate to authorise the transfer of personal data to the US on the basis of adherence to the Safe Harbour principles shall remain valid; however, the Inspectorate recommends the use of standard contractual clauses or BRCs in order to ensure the legitimacy of the transfer of personal data to the US.

In case the Inspectorate receives a data subject's complaint regarding the transfer of his/her personal data to the US, when issuing a decision the Inspectorate shall take into account, among other circumstances, the time of the transfer of personal data to the US (before or after the CJEU's decision on Safe Harbour) and the existence of additional agreements imposing mutual obligations between companies in the course of the transfer.

7.2.4 Other legal bases

Personal data can be transferred to a non-EU/EEA country or to an international law enforcement organisation without an authorisation from the Inspectorate if:

- The data subject has given his/her consent to the transfer of his/her personal data.
- The transfer of the personal data is necessary for the conclusion or performance of a contract concluded between the data controller and a third party in the interests of the data subject.
- The transfer of the personal data is necessary for the performance of a contract between the data controller and the data subject, or for the implementation of pre-contractual measures to be taken in response to the data subject's request.

- The transfer of personal data is necessary (or required by law) for important public interests or for the purpose of legal proceedings.
- The transfer is necessary for the protection of vital interests of the data subject.
- The transfer is necessary for the prevention or investigation of criminal offences.
- The personal data is transferred from a public data file in accordance with a procedure laid down in a law or other legal act.

7.3 E-discovery and law enforcement requests

There are no particular rules or guidance regarding the data protection implications of third-country e-discovery and/or law enforcement requests in Lithuania. The Inspectorate is likely to follow the opinion of the Working Party on this question. It is noteworthy that the Data Protection Law allows the transfer of personal data outside the EU/EEA without the authorisation of the Inspectorate if necessary (or required by law) for the purpose of legal proceedings in a court.

7.4 Representative

Non-EEA data controllers must appoint a representative, for example, an established branch office or a representative office, in Lithuania if they process personal data by using personal data processing equipment established in Lithuania. The representative is bound by the provisions of the Data Protection Law applicable to the data controller.

8. Information obligations

8.1 Who

The burden to inform data subjects lies with the data controllers.

8.2 What

The following information should be provided to data subjects:

The identity and permanent place of residence of the data controller and its representative, if any (where the data controller or its representative is a natural person), or the name, identification code and address of the registered office (where the data controller or its representative is a legal person).

The purpose of the processing of the data subject's personal data.

Additional information (the data recipient and the purpose for disclosure of the data subject's personal data; the particular personal data that the data subject must provide and the consequences of his/her failure to provide the data; the right of the data subject to have access to his/her personal data; and the right to request the rectification of incorrect, incomplete and inaccurate personal data) to the extent that it is necessary for ensuring fair processing without infringing the data subject's rights.

8.3 Exceptions

Data controllers have no obligation to provide data subjects with the above-mentioned information if the data subject already has it.

Furthermore, in cases when the data controller does not obtain personal data from the data subject directly, an exemption from the information obligation applies in case of processing of personal data for statistical, historical or scientific research purposes where the disclosure of such information is impossible or too complicated (owing to the large number of data recipients, the outdated character of the data or excessively large cost); the procedure for collecting and disclosing the data is laid down by law; and where the data subject's contact details (address, phone number) are processed for the purposes of a social and public opinion survey until the first direct contact with the data subject. In these cases, the data controller must duly notify the Inspectorate thereof and the Inspectorate must carry out a prior check (*see Section 12 below*).

In addition, general exceptions regarding the obligation to enable data subjects to exercise their rights are applicable (*see Section 9.3 below*).

8.4 When

Where the data controller does not obtain personal data from the data subject directly, he/she must inform the data subject thereof before commencing the processing of the personal data. If the data controller intends to disclose the personal data to third parties, it must inform the data subject thereof at the latest when the data is first disclosed.

The Data Protection Law does not explicitly provide the point in time at which the information should be provided to data subjects in cases where the data is collected directly from the data subjects; however, systematic interpretation of the law requires that the data subject be informed at the latest when the data processing starts.

8.5 How

The Data Protection Law does not provide in what form or how the information must be provided to data subjects; however, it is customary to provide the information in a written form for evidential purposes.

9. RIGHTS OF INDIVIDUALS

9.1 Who

Data controllers have an obligation to enable data subjects to exercise their rights under the Data Protection Law.

9.2 What

Data subjects have the following rights:

- To know (be informed) about the processing of their personal data.
- To have access to their personal data and to be informed of how it is processed.

- To request rectification or destruction of their personal data or suspension of further processing of their personal data, with the exception of storage, where the data is processed in violation of the provisions of the Data Protection Law or other laws.
- To object to the processing of their personal data.

9.3 Exceptions

Exceptions apply in cases laid down in laws where it is necessary to ensure:

- The security or defence of the state.
- Public order and the prevention, investigation, detection or prosecution of criminal offences.
- Important economic or financial interests of the state.
- The prevention, investigation and detection of violations of official or professional ethics.
- The protection of the rights and freedoms of the data subject or other persons.

9.4 When

As a general rule, having received a request from the data subject, the data controller must reply to him or her within 30 calendar days from the date of the data subject's request. The data controller must disclose to the data subject the requested data no later than within 30 calendar days from the receipt of the data subject's enquiry. The data controller must suspend the processing of data subjects' personal data and inform data recipients of the rectification, destruction or suspension of the processing of that data without delay.

9.5 How

If justified, data controllers must comply with data subjects' requests and, for instance, provide the requested information with regard to the processing of their personal data, rectify, destroy or suspend further processing of their data or, where the personal data has been processed on the basis of a data subject's consent, stop the relevant processing.

The data controller must respond to data subjects' requests. Where the request of the data subject is submitted in writing, the data controller's reply must also be given in writing.

9.6 Charges

The data controller can charge the data subject only for exercising his/her right of access to his/her personal data and only if the data subject exercises such right for a second or subsequent time in a given year. The data controller can set the fee; however, it cannot exceed the actual expenditure of the data controller.

10. SECURITY OF DATA PROCESSING

10.1 Confidentiality

Employees of the data controller, the data processor and their representatives who process personal data have an obligation to respect the confidentiality of personal data, unless such personal data is intended for public disclosure. This obligation shall continue after the employee leaves public service or transfers to another position, or the expiry of his/her employment or contractual relation.

10.2 Security requirements

Lithuanian data protection legislation obliges the data controller and the data processor to implement appropriate organisational and technical measures intended for the protection of personal data against accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing. These measures must ensure a level of security appropriate to the nature of the personal data to be protected and the risks represented by the processing. Moreover, they must be defined in a written document (personal data processing regulations approved by the data controller, a contract concluded by the data controller and the data processor, and so on) in accordance with the general requirements of the organisational and technical data protection measures laid down by the Inspectorate. Key measures taken shall be disclosed to the Inspectorate in the process of notification or authorisation.

Specific data security requirements are set forth by General Requirements for Organisational and Technical Data Security Means approved by Order No 1T-71(1.12) of 12 November 2008 of the Director of the Inspectorate.

10.3 Data security breach notification obligation

10.3.1 Who

The providers of publicly available electronic communications services have the obligation to notify personal data breaches to the Inspectorate. Other data controllers do not have a general obligation to notify the Inspectorate or data subjects of a data security breach. Such notification may only be advisable as part of bona fide obligations in order to minimise civil liability.

"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service.

10.3.2 What

The providers of publicly available electronic communications services must provide the following information to the Inspectorate (and the data subjects):

- The nature of the data security breach.
- Recommended measures imposed to reduce the negative influence of the breach.
- Consequences of the breach.
- Measures which were taken to investigate the breach.

- Contacts for more information.

10.3.3 Exceptions

The provider of publicly available communications services has no obligation to notify the subscriber or individual of the breach in cases where the provider has demonstrated to the satisfaction of the Inspectorate that it has implemented appropriate technological protection measures (for example, encryption) and that those measures were applied to the personal data concerned by the security breach.

10.3.4 When

The providers of publicly available electronic communications services should notify the personal data breach to the Inspectorate without undue delay.

10.3.5 How

When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider must notify not only the Inspectorate, but also the subscriber or individual, of the breach. 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 Inspectorate, having considered the likely adverse effects of the breach, may require it to do so.

10.4 Cybersecurity

There are no particular data protection rules concerning cybersecurity or providers of critical infrastructure in Lithuania.

11. DATA PROTECTION IMPACT ASSESSMENTS, AUDITS AND SEALS

Pursuant to the General Requirements for Organisational and Technical Data Protection Measures approved by the Inspectorate, it is recommended for data controllers who are processing sensitive data to assess the risks relating to personal data processing and perform an audit or assessment of the implemented organisational and technical security measures of personal data processing.

There is no regulation or guidance on data protection seals.

12. REGISTRATION OBLIGATIONS

12.1 Notification requirements

12.1.1 Who

Data controllers who process personal data by automatic means must notify the Inspectorate of any data processing in Lithuania.

12.1.2 What

The purpose of the data processing and the personal data processed must be notified. The Data Protection Law does not link notification to databases or specific data processing operations; thus, in terms of notification, it is

irrelevant if personal data is processed in one or more database, or the kind of data processing operation that is performed.

12.1.3 Exceptions

No notification is required in cases where personal data is processed:

- For the purposes of internal administration (including group-level administration).
- For political, philosophical, religious or trade union-related purposes by a foundation, association or other non-profit organisation on the condition that the personal data processed relates solely to the members of such organisation or to other persons who regularly participate in its activities in connection with the purposes of such organisations.
- By the media for the purpose of providing information to the public for artistic and literary expression.
- In accordance with regulations on state secrets and official secrets.

12.1.4 When

Notification must be made before the start of any data processing. After notification, data controllers are registered in the State Register of Personal Data Controllers, which is administered by the Inspectorate. Data controllers have an obligation to update the information provided in the notification form within one month from the changes. A request to update the information at issue should be provided to the Inspectorate.

12.1.5 How

When notifying the Inspectorate of data processing, the data controller has to submit a standard notification form – available on the Inspectorate's website – which includes information about:

- The purpose of the data processing.
- The categories of data subjects.
- The sources of the personal data.
- The categories of the data recipients of the personal data.
- The categories of personal data that are being processed.
- Personal data transfers to foreign countries.
- The personal data retention period.
- The data processors.
- The list of security measures.

The notification form should be completed in the Lithuanian language. Documentation confirming the right of a representative of the data controller to sign the notification form should be attached to the form.

The notification procedure typically lasts one month from the receipt of notification by the Inspectorate. If the data processing meets the requirements of the Data Protection Law, the Inspectorate issues a decision regarding the registration of the data controller in the State Register of Personal Data Controllers.

12.1.6 Charges

The notification and registration of data controllers is free of charge.

12.2 Authorisation requirements

12.2.1 Who

The obligation to request an authorisation is placed on data controllers.

12.2.2 What

Authorisation is required for the processing of sensitive data and other cases listed in the Data Protection Law as set out below where the Inspectorate conducts a prior check of the processing of personal data:

- Processing public data files (a state register or any other data file which, pursuant to laws or other legal acts, is intended for the disclosure of information to the public and which may be lawfully used by the public) by automatic means.
- Where the data controller of state or institutional registers or information systems of state and municipal institutions intends to authorise a data processor to process personal data.
- Processing data on a person's health and for scientific medical research purposes by automatic means.
- Processing data for the purposes of scientific research without the data subject's consent.
- Processing consolidated debtor files for the purpose of disclosing such data to third parties having legitimate interests so that they could evaluate the solvency of the data subject and manage his/her debts.
- Processing of personal data listed in the Data Protection Law for the purposes of evaluating a person's solvency, financial risk and debt management in consolidated files of financial risk data under the data disclosure contracts concluded with financial institutions.
- Processing of personal data for statistical, historical or scientific research purposes, where the disclosure of information to data subjects is impossible or too complicated, or where the procedure for collecting and disclosing of data is laid down by law.
- Processing of the data subject's contact details for the purposes of a social and public opinion survey until the first direct contact with the data subject.

Authorisation is also required for data transfers outside the EU/EEA.

12.2.3 Exceptions

Sensitive data can be processed without authorisation in cases where the data is:

- Processed for the purposes of internal administration.

- Necessary, in the cases laid down in laws, in order to prevent and investigate criminal or other illegal activities.
- Necessary for a court hearing.

Public data files can be processed by automatic means without authorisation if laws or other legal acts lay down a procedure for the disclosure of the data.

The data controller of state or institutional registers or information systems of state and municipal institutions can instruct the data processor to process personal data without authorisation if laws or other legal acts establish the right of the data controller to instruct a particular data processor to process personal data or where the data processor is a legal person established by the data controller.

12.2.4 When

Authorisation of processing sensitive data should be requested and obtained before the start of the data processing at issue. The data controller has an obligation to update the information provided in an authorisation form within one month from the moment when the changes take place. A request to update the information at issue should be submitted to the Inspectorate.

As regards data transfers outside the EEA, authorisation should be requested and obtained before the start of the data transfer. In case of changes in the categories of personal data, new authorisation should be requested with regard to this new data.

12.2.5 How

In order to authorise processing of sensitive data, the data controller has to submit a standard form available on the website of the Inspectorate. The form includes information about:

- The legal basis for the authorisation.
- The purpose of data processing.
- The legal basis of the data processing.
- The reason why it is impossible to inform the data subjects about the processing of their personal data (where applicable).
- The categories of data subjects.
- The categories of personal data.
- The sources of the personal data.
- The approximate number of data subjects.
- The storage and destruction of the personal data.
- The rights of the data subjects.
- The international transfer of personal data outside the EEA.

- The data processors.
- The form with regard to data transfers outside the EU/EEA should include information about:
- The purpose of the data transfer.
- The data subjects whose data will be transferred.
- The personal data which will be transferred.
- The countries to which the personal data will be transferred.
- Information regarding an adequate level of legal protection.

The forms should be completed in the Lithuanian language. Documentation confirming the right of a representative of the data controller to sign the form should be attached, as well as evidence confirming an adequate level of legal protection.

The duration of the authorisation procedure is two months from the receipt of the request by the Inspectorate. If the requirements for data transfers established in the Data Protection Law are met, the Inspectorate issues an authorisation decision.

12.2.6 Charges

The authorisation procedure is free of charge.

12.3 Other registration requirements

Not applicable.

12.4 Register

The Inspectorate is responsible for managing the State Register of Personal Data Controllers. All information notified to the Inspectorate, except for security measures, is published and open at the Inspectorate's website to any person wanting to see it free of charge. No information with regard to requests to grant authorisation for international data transfers is published in the register.

13. Data protection officer

13.1 Function recognised by law

Under the Data Protection Law, data controllers have a right (but not an obligation) to designate a person to be responsible for the data protection (data protection officer). The data controller must notify the Inspectorate of the appointment or withdrawal of the data protection officer within 30 days. If no data protection officer is appointed, the CEO of the data controller may be *ex officio* deemed responsible for data protection compliance and may also be personally liable for any legal violations of the Data Protection Law.

13.2 Tasks and powers

The data protection officer has the following tasks and powers:

- Make public (for example, publish on the internet) the processing of personal data actions carried out by the data controller in accordance with the procedure established by the government.
- Supervise whether personal data is processed in compliance with the provisions of the Data Protection Law and other legal acts on data protection.
- Initiate the preparation of the notifications to the Inspectorate in case of prior checking.
- Monitor the processing of personal data carried out by the data controller's employees.
- Present proposals and findings to the data controller regarding the establishment of data protection and processing measures, and supervise their implementation and use.
- Undertake measures to eliminate any violations regarding the processing of personal data without delay.
- Train employees authorised to process personal data regarding the provisions of the Data Protection Law and other legal acts on personal data protection.
- Initiate the preparation of applications to the Inspectorate regarding processing and protection of personal data.
- Assist data subjects in exercising their rights.
- Notify the Inspectorate in writing where the data controller processes personal data in violation of the data protection laws and refuses to rectify these violations.

14. ENFORCEMENT AND SANCTIONS

14.1 Enforcement action

Any violation of data protection rules or breach of the rights of the data subject causes administrative liability. The Inspectorate has no power to impose penalties for violations, although the Inspectorate can issue a statement on an administrative offence, according to which national courts can impose fines. These administrative sanctions may only be applied to individuals, and legal entities/companies may not be subject to administrative prosecution. If a company commits a violation, the data protection officer or the CEO of the entity will be held responsible for such an administrative offence.

Pursuant to established case law it is the person responsible for data protection compliance – that is, the data controller or the data processor – not the direct offender (for example, an employee), who may face sanctions for a violation of the Data Protection Law.

In addition, the public prosecutor can theoretically take criminal law enforcement action for serious privacy-related misconduct.

14.2 Sanctions

Fines for violations of the Data Protection Law vary from EUR 144 to EUR 579. There are some criminal sanctions established for serious violations of privacy; however, with respect to usual data processing activities, these are enforced extremely rarely.

14.3 Examples of recent enforcement of data protection rules

Enforcement examples:

The Inspectorate concluded that a data controller cannot transfer personal data to another data controller abroad if an obligatory provision – namely, stating the purpose of processing personal data – is not contained in a data transfer agreement, which must be concluded between the parties transferring personal data. Therefore, on 14 March 2014 the Inspectorate ordered the company at stake to include such provision in a data transfer agreement. In its decision dated 3 November 2015, *Case No eA-831-261/2015*, the Lithuanian Supreme Administrative Court upheld position of the Inspectorate, stating that the provision of the Data Protection Law which requires the inclusion of the purpose of data transfer in a data transfer agreement is imperative and cannot be ignored even in cases where data processing and transferring are legitimate.

The Inspectorate initiated administrative proceedings for a violation of the Data Protection Law against a data controller who sent a notice regarding debt collection to a data subject via the fax of his/her employer. In its decision dated 24 April 2014, *Case No ATP-431-628/2014*, the Vilnius County Court upheld the position of the Inspectorate and stated that sending such document via fax constitutes personal data processing by automatic means, and therefore the Data Protection Law applies to such processing. The court decided that the data controller acted unlawfully by disclosing personal data of a data subject to a number of other persons. The fine of LTL 500 (approximately EUR 143) which had been imposed on the data controller was upheld by the court.

15. REMEDIES AND LIABILITY

15.1 Judicial remedies

Data subjects can enforce their rights by:

- Lodging a claim with the Inspectorate.
- Bringing an action in a court regarding civil liability of a data controller.
- Lodging a claim with law and order institutions regarding criminal liability of a data controller.

15.2 Class actions

Under the general rules of the Civil Procedure Code, individuals have a right to file a class action; however, there is no case law regarding class actions in relation to breach of the Data Protection Law yet.

15.3 Liability

Individuals who are affected by the breach of the Data Protection Law are entitled under the same law to claim pecuniary and moral damages. However, such claims are not common in practice. Any data controller, data processor or other person violating the provisions of the Data Protection Law is responsible for the damages that result from the unlawful processing of personal data or any other acts (omissions).