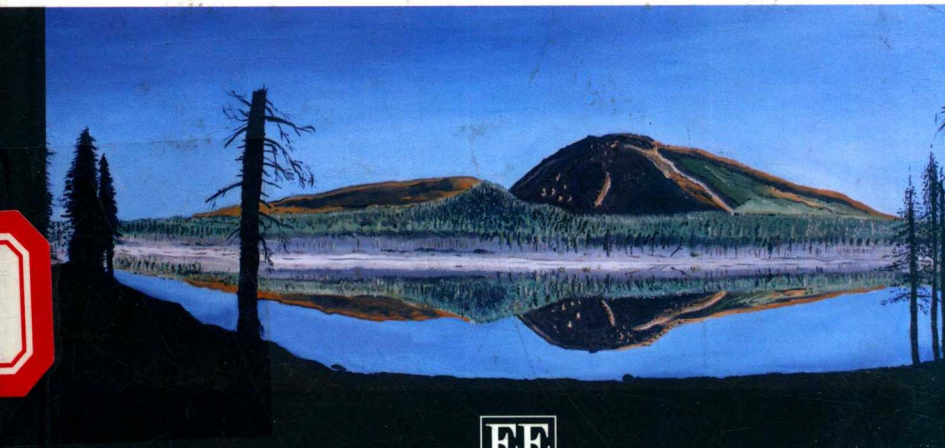
ELGAR PRACTICAL GUIDES

DETERMANN'S FIELD GUIDE TO DATA PRIVACY LAW

International Corporate Compliance

Second Edition

Lothar Determann



EE
Elgar

Determann's Field Guide to Data Privacy Law

International Corporate Compliance

Second Edition

LOTHAR DETERMANN
Baker & McKenzie LLP, USA, Freie Universität Berlin, Germany, UC Berkeley School of Law and Hastings College of the Law, USA

Elgar Practical Guides

Edward Elgar PUBLISHING

Cheltenham, UK • Northampton, MA, USA

Published by
Edward Elgar Publishing Limited
The Lypiatts
15 Lansdown Road
Cheltenham
Glos GL50 2JA
UK

Edward Elgar Publishing, Inc.
William Pratt House
9 Dewey Court
Northampton
Massachusetts 01060
USA

A catalogue record for this book
is available from the British Library

Library of Congress Control Number: 2014950853

This book is available electronically in the Elgaronline
Law subject collection
DOI 10.4337/9781783476893

MIX
Paper from responsible sources
FSC® C013056

ISBN 978 1 78347 688 6 (cased)
ISBN 978 1 78471 499 4 (paperback)
ISBN 978 1 78347 689 3 (eBook)

Typeset by Servis Filmsetting Ltd, Stockport, Cheshire
Printed and bound in Great Britain by T.J. International Ltd, Padstow

About this second edition, contributors and the author

Since the first edition of this Field Guide went to print in March 2012, data processing technologies, laws and public attention to data privacy have evolved, particularly following the media coverage of NSA programs since 2013. Some countries have enacted new data privacy laws, including Colombia, Kazakhstan, Malaysia, the Philippines, Singapore and South Africa. The enforcement of data privacy laws has picked up. In Europe, data protection authorities have increased their audit activities and issued fines. In the United States, plaintiffs' lawyers have brought numerous class action lawsuits based on data privacy and security claims against companies and the government; the U.S. Federal Trade Commission is further developing a body of data privacy and security law through complaints and consent decrees; and the State of California, where most major information technology companies are headquartered, is actively passing new laws in response to perceived new threats and abuses. But, a lot also remains the same: The European Union has still not managed to update its main, omnibus privacy law, which is going to be 20 years old in 2015. In the United States, Congress debates many, but passes few, data privacy laws. Other major jurisdictions, including Brazil and the People's Republic of China, have not enacted comprehensive data privacy laws yet. Thus, much of the practical guidance and the general direction of this Field Guide remain steady. The author is grateful for the interest and feedback regarding the first edition and looks forward to continued dialogue with users of this Field Guide.

The author thanks for valuable contributions to the first edition of this Field Guide Brian Hengesbaugh, partner, Baker & McKenzie Chicago; Theodore Ling, partner, Baker & McKenzie Toronto; Christoph Rittweger, partner, Baker & McKenzie Munich; Prof. Susan Freiwald, Professor of Law, University of San Francisco School of Law; Sarah Jain, Legal Director, Employment, Dolby Laboratories, Inc.; Dr. Ron A. Dolin, Legal Technologist and Fellow at Stanford University; Dr. Sebastian Kraska, Rechtsanwalt, Externer Datenschutzbeauftragter,

IITR GmbH; Joshua Glucoft, Stanford Law School, JD Candidate 2014; Diana Francis, Baker & McKenzie San Francisco; Emmanuel Fua, Stanford Law School, JD Graduate 2012. The author takes sole responsibility for any errors and omissions.

Lothar Determann practices and teaches international data privacy, commercial and intellectual property law. He is admitted to practice law in Germany and California and is a partner with Baker & McKenzie LLP in Palo Alto, California. He has been a member of the Association of German Public Law Professors since 1999 and teaches Data Privacy Law, Computer Law and Internet Law at UC Berkeley School of Law (Boalt Hall, since 2004), Hastings College of the Law (since 2010), Freie Universität Berlin (since 1994) and Stanford Law School (in 2011). He has previously authored three books and more than 90 articles and treatise contributions.

Key terms

Every discipline coins its own special terms, acronyms, other abbreviations and jargon. Data privacy law is no different in this respect. In the interest of serving as a quick reference and easy read, this Field Guide minimizes the use of jargon and abbreviations and employs everyday language whenever practical. But, seven 'key terms' are used throughout the guide, because you have to know them. These terms are omnipresent in data privacy literature and hard to avoid:

Personal Data	Information that relates to an individual person who can be identified, including identifying information (name, passport number, etc.) and any other data (*e.g.*, photos, phone numbers, etc.). European data protection laws tend to cover all personal data, but U.S. style data privacy laws are often more limited and focused on particularly sensitive data categories
Processing	Any activity relating to data, including collection, storage, alteration, disclosure and destruction
Data Subject	The individual person to whom data relates
Data Controller	A company that determines the purposes and means of the data processing, *e.g.*, an employer with respect to employee data
Data Processor	A company that processes personal data on behalf of a data controller, *e.g.*, an accountant or payroll service provider that assists an employer
Transfer	Transmitting data to, or making data available for access by, another organization or in another country, *e.g.*, via remote Internet access

Data Privacy Law	Laws intended to protect an individual data subject's ability to control information about him or herself, including European-style data protection laws (regulating any processing of any personal data) and common law privacy laws (protecting reasonable expectations of being left alone by other individuals, organizations and governments)

More detailed definitions follow in Chapter 1 – 'Key Concepts'. Abbreviations are defined at the end of the book.

A few other key terms should perhaps be used more sparingly and carefully. Information technologists and marketers tend to be so excited about 'the cloud' and 'big data' that they overuse these labels, extend their meaning to products on the periphery and overlook all negative connotations. When software-as-a-service providers and users talk about 'the cloud', they think about dynamic usage of computing capacity, cost savings, follow-the-sun support, connectivity, mobility and other benefits. When European data protection officers and politicians hear 'the cloud', however, they seem to think about bad visibility into where data resides and who has access to it. Similarly, when researchers get excited about opportunities concerning 'big data', they seem to forget the relatively low public preference for *big* government, *big* business, banks too *big* to fail, etc. If you are trying to sell services, features and opportunities, be mindful of your audience before resorting to these buzzwords.

Content overview

Table of contents

How to use this Field Guide

This Field Guide is not about 'roughing it'. This book guides you through an increasingly complex field of laws, regulations and technology. Generalists in corporate legal departments and private practice, privacy officers, information technology product developers, marketing managers and others are confronted with data privacy and security issues more and more frequently. Tons of information is publicly available, much of which is free of charge. Still, it can be difficult to get a handle on a practical problem quickly without getting lost in details.

This is where this Field Guide is meant to come into play. It is designed to help identify issues, provide a brief practical overview, shape questions and lead to solutions. Where the Field Guide cannot provide an answer that is detailed enough, it contains directions to further resources that are easily accessible – by providing key terminology that can be easily looked up. Footnotes with citations in 'Bluebook format' have consciously been omitted; this book is for use in the field, not in a library.

For example, in this Field Guide you will find checklists with key compliance requirements and practical suggestions on how to go about satisfying them in an efficient manner. You will also be presented with examples of jurisdiction-specific details that global companies are most likely to encounter in the field, selected for illustrative purposes, but never for all 190+ countries. Once you have your bearings and you want to determine applicable details by country and situation, for example, whether you have to appoint a data protection officer in China, this Field Guide will refer you to other resources, listed at the back of the book, including Baker & McKenzie's Global Privacy Handbook (available free of charge, the 2014 Edition covers 51 jurisdictions).

Consider a few suggestions on how to use the Field Guide: If you got this book because you are tasked with designing or implementing a new data privacy compliance program, you could start with the

following overview of 'Key Terms' and Chapter 1 – 'Key Concepts' for orientation, and then use the following five chapters of the Field Guide for navigation. If you just want to get a quick read on a particular issue, you could look up buzz words in the Index at the end of the book to zoom in on a topic that concerns you. Or, if you are faced with a particular task, you could also try one of the following paths:

Task or issue	Guidance
Draft a privacy policy	Ch. 4.1–4.8
Respond to data security breach	Ch. 6 – Breaches of Data Security
Buy or sell cloud computing services	Ch. 6 – Cloud Computing; Vendors Ch. 4.9 – Agreements
Appoint data privacy officer	Ch. 2.1–2.2
Achieve compliance re. international data transfers	Ch. 3
Prepare filings for data protection authorities	Ch. 4.12
Conduct due diligence on M&A targets, vendors	Ch. 5
Select network/employee monitoring tools	Ch. 6 – Employee Data and Monitoring; Wiretapping
Deploy cookies, tracking technologies legally	Ch. 6 – Advertising, Tracking
Comply with anti-spam laws	Ch. 6 – Unsolicited Communications
Develop product, process or service	Ch. 6 – Privacy by Design
Gather management support	Ch. 6 – Rights, Remedies, Enforcement; Y – Why Protect Privacy?

If you are new at an organization that does not have a formal data privacy compliance program, you could start with Chapter 2, prepare a task list as you go, study or skip Chapter 3 on international data transfers (depending on how domestic or global your business is), and then work through Chapter 4 as you prepare documentation and execute your task list.

If you are tackling an existing program, start with the brief Chapter 5 first and then go through Chapters 2 through 4.

If you just need a quick answer to a substantive question, check the Index at the end of the book and the summaries from A to Z in

Chapter 6 for directions and perspective. The Field Guide cannot provide definitive answers to detailed questions, but it is intended to put phenomena into context and give you practical pointers and suggestions on how to solve problems, tackle tasks and find further information.

1 Key concepts

1.01 Before entering the field, it is helpful for orientation to scope out or recall key concepts and terminology. Acronyms and abbreviations are also summarized at the back of this book.

1.1 The field: data protection, privacy and security

1.02 The terms 'data privacy' and 'data protection' are often used interchangeably, in particular in the context of comparisons of Anglo-Saxon data privacy laws and continental European data protection laws. Actually, the two terms and legislative concepts have quite different origins and purposes. Here is a simplified overview:

1.1.1 Data protection

1.03 Data protection is about protecting individuals (the data subjects) from the effects of automated data processing. When you try to understand or comply with European data protection laws, keep in mind that the default rule is 'verboten' (German for: forbidden). Businesses and other organizations are generally prohibited from processing personal data, unless they obtain consent from the data subjects or they find an applicable statutory exemption. European data protection laws are first and foremost intended to restrict and reduce the automated processing of personal data – even if such data is publicly available. My home state, the German State of Hessen, enacted the first data protection law in 1970 due to growing concerns regarding dangers of automated data processing for individual freedoms. Citizens and politicians were concerned that George Orwell's forecast for 1984 could become reality: where 'glass citizens' are observed and controlled by an omniscient 'big brother', the government. More recently, these concerns were joined by fears regarding 'little brothers', namely private companies that amass data and databases for commercial purposes, which can then be conveniently (ab)used by governments or criminals. Due to these

concerns, legislatures decided to regulate automated data processing like other dangerous activities. The Hessian data protection law – and laws of other German states and European countries – established a general prohibition and regulatory regime regarding the processing of personal data. One key feature of European-style data protection laws is a data minimization requirement: companies are prohibited from collecting, using and retaining data, unless they obtain consent or have another compelling reason to process the data. And, companies are required to minimize the amount of data they collect, the instances of processing, the people who have access and the time periods for which they retain data. In practice, many companies in Europe collect and process personal data as much as their competitors in other parts of the world. European data protection laws provide for exemptions and data subjects grant consent to allow this. But, the principal hostility to personal data processing and databases in European data protection laws is important to keep in mind for purposes of understanding and applying European data protection laws. And, this hostility is probably one reason for the fact that European companies do not lead in information-driven economy sectors such as electronic commerce, cloud computing, software-as-a-service and social networking, where much of the innovation and market leaders come from the United States and increasingly also Asia. In 2014, people in Europe reacted with outrage to revelations about large-scale surveillance regarding electronic communications by the United States National Security Agency (NSA) and European intelligence services. Yet, current drafts of the EU Data Protection Regulation continue to largely exempt data processing for national security purposes and European politicians instead push hard for a right to be forgotten.

1.1.2 Data privacy

The United States and other countries outside of Europe, by contrast, generally allow data processing. Data privacy laws are primarily intended to protect individuals from intrusion into seclusion and interception of confidential communications. Given this focus, individuals are usually not protected, unless they have a reasonable expectation of privacy in a particular situation. Companies can – and frequently do – destroy such expectations of privacy by notifying individuals of the companies' data collection and processing activities, for example, in employee handbooks, website privacy statements and in-store warnings about security cameras. Individuals receive some protection in the sanctity of their homes, for example, but communications and activities outside receive

1.04