

PREFACE

This second edition includes significantly expanded discussion of countries throughout the Americas, Europe, and Asia, as privacy and data security laws continue to expand. More than 65 countries now have some type of law that regulates the collection, use, and disclosure of personal information. As the workplace becomes more global, employers must recognize and comply with a myriad of privacy and data security laws (also known as “data protection” laws) that affect employees and other workers. Employers who fail to address workplace privacy and data security issues may find that they are precluded from sharing information with affiliated entities, subject to fines and scrutiny by data protection regulators, and the object of negative publicity.

Companies operating in multiple jurisdictions often struggle to try to find a method of complying with the complex and sometimes conflicting obligations imposed by data protection laws while running their businesses in a cost-effective manner. There is a tension between a desire to provide a safe and secure work environment and at the same time respect the privacy of individual employees. Global employers seek the right balance between ensuring that employees are free from sexual harassment and inappropriate conduct on the one hand and respecting legal restrictions on monitoring of Internet or email use on the other hand. Similarly, employers are seeking to streamline processes and save money by centralizing the human resources function, while at the same time limiting access to employees’ personal information on a need-to-know basis. The first step to working through any of these issues is to understand the questions that must be asked and then to develop a method of examining the issues to find solutions that are practical for each particular organization. There is no “right” answer and no magic bullet to global privacy and data security compliance. Each organization must find a solution that works within its culture and is based on the resources available to it.

The Purpose of This Book

This book is designed to help employers understand the legal landscape related to workplace privacy and data security, and begin to ask the necessary questions to make the key decisions. As more and more personal information is available, laws and regulations are being adopted to enhance an individual's right to make decisions about his or her personal information. The contours of these protections vary from state to state and from country to country. The varied social, cultural, and legal regimes that influence the development of privacy laws are significant. Human resources professionals are often surprised to learn that, in many countries, basic details such as an employee's work email address or employee ID number are considered personal information and subject to the same protections and restrictions as an employee's home address. Lawyers are surprised to learn that the same limitations apply to disclosing personal information to an affiliate as to disclosing information to an unaffiliated third party. The purpose of this book is to limit those "surprises" and to help professionals prepare for and implement cogent privacy and data security policies and programs.

How This Book Is Organized

Unlike other books on the subject, this book is organized not by the particular law or country; rather, it is organized based on the manner in which human resources professionals, privacy and compliance professionals, and lawyers think about privacy issues in the employment context. We begin with an overview of the legal landscape in the United States, European Union (EU), Japan and other key jurisdictions, while each of the remaining chapters analyzes an important topic across jurisdictions to raise awareness about the conflicts among and variation of the laws. For example, we have examined the issues confronted by human resources personnel when they wish to monitor an employee's Internet use or email across a variety of U.S. federal and state laws, the EU Member State laws, and selected countries in Asia and the Americas. Similarly we have compared the laws relating to the collection, use, and disclosure of medical information across a variety of countries.

Professionals working in this area know that having a different process or procedure for each country or state in which an organization operates is quickly becoming impractical and cost prohibitive. By understanding the key differences among the various jurisdictions for the most vexing privacy issues, organizations can begin to formulate policies and practices that balance compliance obligations with practical considerations. By organizing the book along substantive lines and then comparing the laws and regulations across countries (within the same substantive area), professionals working in this area will be able to identify the key issues, ask the right questions, and find the solutions that are practical and tailored to each organization.

Chapter Outline

Chapter 1, “Overview of Privacy and Data Security,” provides a comprehensive overview of the legal framework applied to workplace privacy issues in key jurisdictions, such as the United States, Canada, the European Union, Japan, and a number of other countries. This edition also introduces the new data protection laws adopted by Malaysia and Mexico in 2010. While each chapter of this book provides a stand-alone discussion—for instance, employers interested in Internet monitoring can go directly to Chapter 3—Chapter 1 will help to provide a greater understanding of the “big picture” approach to workplace privacy in the various jurisdictions. Additional information about EU standard clauses for cross-border transfers of personal information, which are discussed in section III.D of this chapter, is provided in Appendix B.

Chapter 2, “Background Checks and Investigations,” addresses the first topic that an employer is likely to encounter when it expands its operations to another country. The rules governing criminal background checks, credit checks, and other background inquiries vary significantly by jurisdiction, and even within the U.S. These laws also limit the information that an employer may lawfully consider in making hiring or other employment decisions. Chapter 2 compares the applicable requirements across a variety of countries in Europe, Asia, and the Americas. This edition also addresses new U.S. laws restricting the use of credit checks for

employment purposes, as well as state laws restricting the use of biometric data by employers.

Chapter 3, “Email and Internet Monitoring/Video and Physical Surveillance,” explains the increasingly complex restrictions on electronic monitoring in the workplace, both in the U.S. and internationally. This chapter includes employer monitoring of work email and Internet use, as well as the use of video and audio surveillance in the workplace. Additionally, this edition addresses the emerging issue of employer monitoring of employees’ social media activity.

Chapter 4, “Employees’ Off-Duty Conduct,” addresses limitations on an employer’s ability to monitor or take action based on an employee’s off-duty conduct. It covers topics such as union and political activities, religious observances, fraternization and romantic relationships with coworkers or others in the workplace, and “moonlighting” or outside employment. This edition includes additional detail about protections for employees’ off-duty conduct in other countries, including Argentina, Canada, Finland, France, Germany and Poland.

Chapter 5, “Confidentiality of Health Information,” describes the legal protections for employees’ health information, including data security and confidentiality obligations that apply to medical and health information. This edition explains the significant developments under the Health Information Technology for Economic and Clinical Health Act (better known as the HITECH Act). This chapter also has been expanded to address medical confidentiality requirements in a variety of other countries, including Argentina, Canada, Finland, Poland, and China.

Chapter 6, “Medical Examinations and Drug Testing of Applicants and Employees,” analyzes the highly regulated areas of medical examination and drug testing, including the applicable procedural requirements in the U.S. and representative countries in Europe and Asia. This chapter also discusses other types of physical or mental testing, such as personality tests, fingerprinting, polygraph testing, and genetic testing. This edition explains the new U.S. protections for genetic information under the Genetic Information Nondiscrimination Act as well.

Chapter 7, “Personnel Records,” describes the use and disclosure of personnel records, including employee access rights in the

U.S. and internationally. It also explains some of the potential negative consequences arising from a misuse or improper disclosure of personnel records. In this edition, Chapter 7 has been expanded to cover additional countries in the America, Europe, and Asia.

Chapter 8, “Use of Government Identifiers and Social Security Numbers,” discusses the expanding restrictions on the use of Social Security Numbers (SSNs) and other government identification numbers by employers. This is a particular focus in the U.S., due to the widespread use of the SSN for financial and credit purposes. This edition compares the U.S. approach with the laws of other countries in the Americas and Europe.

Chapter 9, “Security Breach Notification Requirements,” explains notification obligations that may be triggered by a breach of the security of employees’ SSNs or various other types of personal information. This chapter also describes the growing number of countries adopting security breach notification laws. This edition has been expanded to cover Argentina, Canada, Mexico, Uruguay, Finland, Germany, China, Hong Kong, Korea, Taiwan, and the UK.

Chapter 10, “Data Security: Maintaining an Information Security Program,” provides guidelines for developing an effective program to protect employee data, as well as other personal information. This chapter describes the process for creating an effective program, from the initial risk assessment through policy development and employee training. It also identifies specific measures for such a program, such as document classification, access controls, technical measures such as encryption, and vendor monitoring.

Each chapter begins with a discussion of the applicable privacy and data security issues under U.S. federal and state laws. This U.S. section may serve as a refresher for U.S.-based employers, or as a primer for professionals trained in non-U.S. jurisdictions as they launch operations in the U.S. Following the U.S. section, we provide a detailed explanation of the relevant data protection issues in Europe, the Asia Pacific region, and other countries in the Americas, using a variety of representative countries. This book does not seek to be an encyclopedia that covers each and every country. Instead, it is intended to provide a more global perspective on workplace issues by helping employers understand

the differing approaches to workplace privacy by region and jurisdiction.

Additional Resources

This book includes references to a variety of statutes, regulations, cases, and other legal guidance. Readers interested in reviewing these source materials can find links to online copies of many of these documents through Morrison & Foerster's online Privacy Library, available at www.mofoprivacy.com. The Privacy Library is organized by jurisdiction, allowing easy retrieval of privacy laws for a certain country (or, within the U.S., by state). Additionally, the Privacy Library includes a "Legal Updates and News" page, which provides articles and news alerts written by Morrison & Foerster's Privacy and Data Security Practice. Further information on the Privacy Library is provided in Appendix A. BNA also provides information on new developments in this area in its *Privacy and Security Law Report* (www.bna.com/products/corplaw/pvln.htm) and publishes *Privacy in Employment Law*, a companion volume focused on U.S. law.

About the Editors and Authors

This book was written primarily by an international team of attorneys in the Privacy and Data Security Practice of Morrison & Foerster LLP, a global law firm with more than 1,000 lawyers in 17 offices around the world. Today, the firm has more than 60 attorneys in our global offices addressing privacy issues, several of whom were instrumental in the drafting of key pieces of legislation in the field, as well as litigating cutting-edge privacy and data security issues. Portions of the book were also written by several international lawyers from firms around the world. Information on the individual editors and authors is provided in the "About the Editors and Authors" section following this Preface.

Morrison & Foerster advises and represents clients on a wide range of privacy issues both in and outside of the U.S., including data security and regulatory compliance; employee privacy; Web site and online privacy issues; data security, security breach notification, industry-specific privacy issues facing sectors such as financial services and health care; and international data pro-

tection. Clients include financial institutions (including banks, insurance companies, and securities firms), hardware and software companies, health care providers and health plans, payment systems providers, retailers, telecommunications networks, medical device companies, entertainment companies, and content providers.

We hope that you find this book a useful tool as you seek to find solutions to what will only become a more interesting and complicated area in the years to come.

MIRIAM H. WUGMEISTER
Editor
New York, NY

CHRISTINE E. LYON
Editor
Palo Alto, CA

June 2011