Privacy program management is here to stay, and the need for sophisticated leaders who understand the complexities of the global digital marketplace will only increase.

Privacy Program Management: Tools for Managing Privacy Within Your Organization provides the critical tools necessary for anyone responsible for managing privacy program governance and operations within their organization.

Reorganized with expanded topics relevant to privacy program leaders, the second edition takes a global view of privacy managers' obligations and practices. Key topics covered include:

- Creating a company vision
- Structuring the privacy team
- Developing and implementing a privacy program framework
- Communicating policies and procedures to personnel
- Compliance with regulations and standards, including the GDPR
- Performance measurement

An indispensable resource, this comprehensive how-to guide also serves as the principal reference for the Certified Information Privacy Manager (CIPM®) program—the first global certification in privacy program management. The CIPM program was developed by the International Association of Privacy Professionals (IAPP) in conjunction with globally recognized privacy experts. It is accredited by ANSI under ANSI/ISO 17024: 2012 and recognized worldwide through a multilateral agreement with the International Accreditation Forum (IAF).

Executive Editor and Contributor

Russell Densmore, CIPP/E, CIPP/US, CIPM, CIPT, FIP

Russell Densmore is the global privacy compliance program manager for Raytheon. With over 30 years of experience, he brings a multidisciplinary understanding to physical security, cybersecurity, digital forensics, enterprise risk management, and privacy compliance. He has been recognized by the U.S. attorney general and the Federal Bureau of Investigation for support against cybercriminals. Densmore holds a BS in computer information systems from Regis University and is also a Certified Information Systems Security Professional (CISSP).

Contributing Authors

Susan Bandi, CIPP/US, CIPM, CIPT, FIP
João Torres Barreiro, CIPP/E, CIPP/US
Ron De Jesus, CIPP/A, CIPP/C, CIPP/E, CIPP/US, CIPM, CIPT, FIP
Jonathan Fox, CIPP/US, CIPM
Tracy Kosa
Jon Neiditz, CIPP/E, CIPP/US, CIPM
Chris Pahl, CIPP/C, CIPP/E, CIPP/G, CIPP/US, CIPM, CIPT, FIP
Tajma Rahimic
Liisa Thomas
Amanda Witt, CIPP/E, CIPP/US
Edward Yakabovicz, CIPP/G, CIPM, CIPT

$75.00
ISBN 978-1-948771-23-8
57500
9 781948 771238

An iapp publication

PRIVACY PROGRAM MANAGEMENT

SECOND EDITION

iapp

PRIVACY PROGRAM MANAGEMENT

Tools for Managing Privacy Within Your Organization

Second Edition

Executive Editor and Contributor
Russell Densmore, CIPP/E, CIPP/US, CIPM, CIPT, FIP

An iapp publication

Contents

Preface

I am privileged to have worked with so many great privacy professionals on both the first edition of this textbook in 2013 and now on this second edition in 2019. The privacy landscape has changed remarkably in this five-year period. We have seen the first major, comprehensive privacy regulation implemented in the EU, with the General Data Protection Regulation (GDPR) impacting organizations and individuals around the globe. We have come to understand that individuals expect organizations to get it right when it comes to the protection of personal information. Demands for improved legislation to protect individuals and their rights have grown exponentially, giving regulators the power they need to ensure organizations comply. Organizations fear damage to their brand, loss of consumer confidence, and regulatory fines due to data breaches. There has never been a better time for organizations to demand well-trained, well-informed privacy professionals.

The privacy program manager is a critical component of every privacy program at any organization. We have seen this field develop over the last few years from a budding program management framework to an integrated and fully functioning multidisciplinary effort. Privacy program management is definitely a team sport. Subject matter expertise is needed in multiple areas ranging from regulatory compliance, policy implementation, training and awareness, data mapping and records of processing to third-party vendor management and contracting. It requires a holistic approach, with multiple skill sets to accomplish all the required aspects of privacy program management in every organization.

Over the last few years, I have come to believe that while a privacy program manager is responsible for bringing all the needed components of the privacy program to maturity, rarely does one person have expertise in all the different disciplines required. An individual skilled in the training and awareness domain may not excel at writing policies, and vice versa. A person who excels at managing data breaches may not do well at vendor management or contracting. I hope you see the point I am trying to make. Privacy is a complex topic with diverse skill sets, which are needed by the

privacy organization to be successful. The privacy program manager should be able to understand all these areas but will most likely not be an expert in all of them. Who, then, should be the privacy program manager?

In the past, a legal expert (attorney) has often served as the chief privacy officer and the privacy program manager. Currently, I am seeing a division of duties among the chief privacy officer, the privacy program manager, and privacy engineers. The chief privacy officer may handle the legal and regulatory obligations for the organization while the privacy program manager oversees program compliance requirements, organizational functions, and execution of implementation and the privacy engineer manages the technical functions. There may be overlap, and certainly each of the different domains may serve multiple functions, but we are seeing these areas of expertise evolve.

The privacy program manager is responsible for proving to the organization that it has the proper controls in place and for helping demonstrate to regulators that the organization is handling personal data responsibly. There must be a data map showing what data the organization has and how that data is protected and processed. By definition, this is the privacy engineer's duty. The number of privacy engineers in the privacy profession is rising; in fact, the IAPP launched the Privacy Engineering Section in 2018. The value of such individuals is becoming clear. Perhaps this is the future, where the chief privacy officer, the privacy engineer, and the privacy program manager work together to cover all three roles. Certainly, the organization will need experts in each of these fields to be successful.

There appears to be no one-size-fits-all approach, especially in large multinational and complex organizations. I believe one individual may still be able to cover all of these functions for a small organization; however, I believe privacy program management has matured into a team sport and requires several teammates to be successful.

I would like to thank everyone who assisted with this textbook, especially the individual authors who contributed in their areas of expertise. They were all dedicated and supportive, proving we could work together as a holistic team to achieve success. Finally, I would also like to thank Mr. Edward Yakabovicz once again for assisting me with the final review of this text. His friendship and professional assistance are appreciated deeply.

Russell Densmore, CIPP/E, CIPP/US, CIPM, CIPT, FIP
January 2019

Introduction

In 2013, when we launched the Certified Information Privacy Manager (CIPM) program, the idea of operating a privacy program was still novel. Our profession largely evolved from law and compliance, and privacy was, in many ways, binary: The privacy pro gave the product or service a thumbs-up or thumbs-down.

Quickly, however, organizations with business models increasingly dependent on data came to realize that better management and customer trust were needed. Unless the privacy professional was involved at every step of product development, organizations faced too much risk. In public administrations, open data efforts and well-meaning attempts to unlock the value of public data were stymied. Work was wasted. Product leads were frustrated. Mistakes were made.

Further, with the passage of the EU's General Data Protection Regulation (GDPR), the idea of operational privacy, or "privacy by design," became law.

Now we see, through research conducted for our annual *IAPP-EY Privacy Governance Report*, that organizations with mature privacy operations not only have full teams of privacy professionals, they also have privacy pros embedded in various business operations and in administrative departments ranging from human resources to IT, marketing and sales. They provide privacy with multimillion-dollar budgets. They buy technology bespoke for privacy operations.

Nor is it any wonder. While the GDPR gets the headlines, there are any number of other privacy regulations around the world that require operational responses. These issues—from data subject access requests to requests for corrections or deletions and increasing requirements for data portability—require deliberate process, careful management and well-trained people.

In short, privacy program management is here to stay, and the need for sophisticated leaders who understand the complexities of the global digital marketplace will only increase. Thus, it's not surprising that the CIPM has become the IAPP's second-fastest-growing certification, behind only the CIPP/E, and that there is great demand for a new and improved textbook to support the certification program.

Yet again, Executive Editor Russell Densmore, CIPP/E, CIPP/US, CIPM, CIPT, FIP, has overseen a variety of valuable contributions in revamping *Privacy Program Management: Tools for Managing Privacy Within Your Organization*. There are more practical examples, more deep dives into the "how" of privacy management, and more information on the tools privacy professionals are using to create effective privacy programs.

For data protection officers, privacy program managers, global privacy leaders, and any number of other new titles emerging around the globe, the CIPM is the perfect tool for privacy professionals working in both the public and private sectors. This book helps unlock the benefits of CIPM and prepare those hoping to take the exam and get certified.

I am extremely pleased with the way the CIPM has been accepted around the globe as the new standard for how privacy is done on the ground and I hope you—and your organization—enjoy its benefits.

J. Trevor Hughes, CIPP
President and CEO
International Association of Privacy Professionals