Brought to you by:

Data Privacy

for dummies®
A Wiley Brand

Discover the privacy compliance drivers

Understand the business requirements to scale

Implement a reliable data privacy solution

Informatica Special Edition

Lawrence C. Miller

About Informatica

Digital transformation changes expectations: better service, faster delivery, with less cost. Businesses must transform to stay relevant, and data holds the answers. As the world's leader in Enterprise Cloud Data Management, Informatica is prepared to help you intelligently lead — in any sector, category, or niche. Informatica provides you with the foresight to become more agile, realize new growth opportunities, or create new inventions. With 100 percent focus on everything data, the company offers the versatility needed to succeed. Informatica invites you to explore all that it has to offer — and unleash the power of data to drive your next intelligent disruption. For more information, call +1 650-385-5000 (1-800-653-3871 in the U.S.), or visit **www.informatica.com**.

Connect with Informatica on social media:

 **https://linkedin.com/company/informatica**

 **https://twitter.com/Informatica**

 **https://facebook.com/InformaticaLLC**

Data Privacy

Informatica Special Edition

By Lawrence C. Miller

for dummies®
A Wiley Brand

Data Privacy For Dummies®, Informatica Special Edition

Published by
John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-60452-5 (pbk); ISBN: 978-1-119-60451-8 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor:
Carrie Burchfield-Leighton

Acquisitions Editor: Katie Mohr

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Special Help from Informatica:
Dan Everett, Nathan Turajski, Gary Patterson, Joe Bracken, Patti Garon Lee, Shino Kizaki

Table of Contents

Introduction

Global privacy regulations, personal data growth, escalating data losses, and new customer expectations demand organizations to optimize and scale their intelligence and protection of personal and sensitive data. Security breaches and regulatory non-compliance have raised enforcement, driving organizations to develop new data privacy and security governance policies, and strategically integrate their communication and enforcement with a comprehensive data protection solution. Operationalizing data protection requires automated next-generation tools to define data use and purpose; discover, classify, and monitor data movement and access; map identities; continuously analyze and track risk; automate and orchestrate controls; and effectively demonstrate readiness. Organizations must also quickly respond to requests on data use, deletion, and transfers or third-party sales. Error-prone manual processes won't scale to meet these new challenges — an automated, reliable approach is needed.

About This Book

Data Privacy For Dummies, Informatica Special Edition, consists of five chapters that explore the following:

- The need for data privacy (Chapter 1)
- What it takes to ensure data privacy at scale (Chapter 2)
- How to implement an intelligent data privacy solution (Chapter 3)
- Real-world data privacy use cases (Chapter 4)
- Keys to successfully implementing a data privacy solution (Chapter 5)

Foolish Assumptions

You are a chief data officer, privacy officer, data protection officer, information security officer, marketing officer, or similarly, an executive with "data" in your job title or description, responsible

for security and privacy. This book is primarily for non-technical readers to learn about innovative solutions to help successfully implement data privacy policies and processes. If this describes you, this book is for you with important takeaways that you will want to share.

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:


REMEMBER

This icon points out information you should commit to your non-volatile memory, your gray matter, or your noggin — along with anniversaries and birthdays.


TIP

Tips are appreciated, never expected — and I sure hope you appreciate these tips. This icon points out useful nuggets of information.


WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but they do offer practical advice to help you avoid potentially costly or frustrating mistakes.

Beyond the Book

If you find yourself at the end of this book, thinking, "Where can I learn more?" take a look at the following resources:

- **www.informatica.com:** The Informatica website offers videos, e-books, solution frameworks, and white papers on data privacy products and solutions.
- **blogs.informatica.com:** This blog gives you articles and news about privacy and related data topics and industry-specific insights.
- **https://infa.media/TDWIChecklistRC:** For help complying with privacy legislation, visit this site.

IN THIS CHAPTER

- Recognizing the growth of data volumes and uses
- Looking at data security breaches and loss
- Surveying the regulatory landscape
- Taking a comprehensive approach to data privacy
- Dealing with empowered customers and individuals
- Enjoying the business benefits of effective data privacy

Chapter 1
Understanding the Data Privacy Imperative

In this chapter, you take a journey through the evolution of data privacy, as well discover the opportunities and benefits of an effective data privacy program and solution for your business.

Expanding Data Volumes and Uses

Digital transformation enables organizations around the world to create competitive advantages and develop brand new products and services. This transformation is fueled by vast amounts of data, as companies are collecting, processing, analyzing, and storing more personal data than ever before, and protecting and governing this data is an increasingly complex challenge.

The speed at which data moves around and between organizations is also increasing and the data itself is evolving. The purpose, quality, and location of practically any data asset can change in the blink of an eye.

Today, managing data has never been harder for organizations. In Data 1.0, from the 1960s to 2000, data was used in specific business applications, such as payroll automation, airline reservations, and retail transactions. Business solutions like Extract Transform Load (ETL) and data integration defined this era.

In Data 2.0, during the last 15 to 20 years, data was used to support enterprise-wide business processes like supply chain, straight-through processing, and quote to cash. Solutions for data quality, master data management (MDM), cloud data integration, data security, data archiving, and other data services evolved during this era.

Data 3.0 is the next generation of data in which data enables entire businesses to be transformed through new business models and processes. Five key technology shifts are all converging at the same time in the Data 3.0 era:

- **Explosion in data volume:** 15.3 zettabytes per year in global data center traffic
- **New users:** 500 million business data users and growing
- **New data types:** 20 billion connected devices (mobile, social, Internet of Things [IoT])
- **Data in the cloud:** Over 92 percent of data center traffic from the cloud
- **Machine learning/artificial intelligence (AI):** One billion workers assisted by machine learning or AI

Any one of these technology shifts would represent a significant trend by itself. All five together creates a generational market disruption.

WARNING

This perfect storm of surging volume, constant change, and accelerating data velocity is creating more personal data in more locations and for more uses, which increases the scope and complexity of compliance programs:

- In addition to traditional structured data in transactional applications and relational databases and documents in file systems, huge volumes of Internet of Things (IoT) sensor data and social media data that may contain personal information are streaming into data lakes.

- The desire to use data for analytics, process improvements, and machine learning increases the risk of unintentionally using, copying, and combining data in ways that violate contractual and regulatory obligations.
- Ethical use of data is influencing your customers' loyalty decisions on what companies they do business with.
- The growing sophistication of threat actors and the potential for malicious activities both inside and outside of your business are accelerating.
- The number of data privacy regulations around the world and the associated fines for non-compliance are growing.

Increasing Threat of Data Breaches and Data Loss

High-profile data breaches and stories of data misuse have made data privacy front-page news in recent years. Cybercriminals and other threat actors are using increasingly sophisticated tools and techniques to breach network defenses and steal sensitive data at an alarming scale. As a result, more data is being lost or stolen than ever before.

Personal data is targeted because it's valuable. Cybercriminals and other threat actors can use this data to steal identities, compromise bank accounts, and access other valuable data. For example, a cybercriminal can use email addresses to find phone numbers. Then, once the threat actor has that, the cybercriminal may have enough data to hack the victim's email account and gain access to other private information.

In addition to the direct costs of a breach, which can include regulatory fines and civil penalties, and recovery efforts (such as remediation, forensics, and notification), indirect costs can be significantly higher. Those costs include damage to brand reputation, resulting in lost business and customer loyalty, just like these statistics:

- 69 percent of global consumers are prepared to boycott any company they believe doesn't take data protection seriously.

- 62 percent blame the company first in the event of a data breach, rather than the hacker.
- 83 percent of United States consumers will stop spending for several months after a breach or serious incident is made public.
- 21 percent of United States consumers will never return to a brand that has suffered a data breach.

WARNING

Customers are increasingly interested in what data businesses collect and how they use the data responsibly. And they mistrust enterprises that don't have clearly defined and transparent security and privacy policies.

Growing Complexity in Data Regulations

As privacy threats and citizen concerns have grown, governments around the world are responding with new and more stringent regulations. Privacy regulations typically focus on specific types of personal data, often referred to as personally identifiable information (PII). Personal data includes

- Name
- Social Security Number (SSN)
- Data and place of birth
- Mother's maiden name
- Email address
- Physical address
- Location (such as IP address)
- Biometric records
- Medical, educational, financial, or employment information

Some examples of relevant data security and privacy regulations, standards, and agencies around the world include

- **The California Consumer Privacy Act (CCPA):** The CCPA establishes consumer privacy rights for California residents. Learn more at `www.caprivacy.org`.

- **The European Union (EU) General Data Protection Regulation (GDPR):** The GDPR establishes privacy rights for EU residents (not just citizens). Learn more at `eugdpr.org`.
- **U.S. Health Insurance Portability and Accountability Act (HIPAA):** HIPAA establishes data privacy and security requirements for safeguarding protected health information (PHI). Learn more at `www.hhs.gov/hipaa/index.html`.
- **U.S. Health Information Technology for Economic and Clinical Health (HITECH) Act:** The HITECH Act establishes data breach reporting and notification requirements for entities subject to HIPAA, and extends HIPAA privacy and security requirements (including civil and criminal penalties) to business associates of entities subject to HIPAA. Learn more at `www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html`.
- **U.S. Federal Information Security Management Act (FISMA):** FISMA establishes a mandatory framework for information security applicable to U.S. Federal Government agencies. Learn more at `www.dhs.gov/fisma`.
- **U.S. Sarbanes-Oxley (SOX) Act:** SOX establishes new or expanded governance and auditing requirements for U.S. public companies. Learn more at `www.sec.gov/spotlight/sarbanes-oxley.htm`.
- **U.S. Gramm-Leach-Bliley Act (GLBA):** GLBA requires financial institutions to explain their information sharing practices to their customers and to safeguard sensitive data. Learn more at `www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act`.
- **U.S. Privacy Act:** The Privacy Act establishes information practices to govern the collection, maintenance, use, and dissemination of information about individuals. Learn more at `www.justice.gov/opcl/privacy-act-1974`.
- **The Personal Information Protection and Electronic Documents Act (PIPEDA):** PIPEDA establishes governance for private sector organizations that collect, use, and disclose personal information. Learn more at `www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda`.

- **Notifiable Data Breaches (NDB) Act (2017):** The NDB establishes notification requirements in the event of a data breach that is likely to result in serious harm to affected individuals. Learn more at `www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme`.
- **China Information Security Technology Personal Information Security Specification (GB/T 35273-2017):** GB/T 35273-2017 establishes requirements for consent and the collection, use, and sharing of personal information. Learn more at `http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=4FFAA51D63BA21B9EE40C51DD3CC40BE`.
- **Singapore Personal Data Protection Act (PDPA):** The PDPA establishes data protection requirements in Singapore. Learn more at `www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview`.
- **Indian Personal Data Protection Bill (2018):** The Personal Data Protection Bill establishes privacy rights for individuals (referred to as *data principals*) and obligations for organizations (referred to as *data fiduciaries*). Learn more at `meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf`.
- **New York State Department of Financial Services (NYDFS):** NYDFS provides oversight and advice for various federal and New York state privacy laws and regulations. Learn more at `www.dfs.ny.gov`.
- **Payment Card Industry (PCI) Data Security Standards (DSS):** PCI DSS is a global information security standard applicable to organizations that process credit and debit cards. Learn more at `www.pcisecuritystandards.org`.
- **Financial Industry Regulatory Authority (FINRA):** FINRA is a non-governmental organization that is responsible for protecting investors and regulating member brokerage firms and exchange markets. Learn more at `www.finra.org`.

REMEMBER

More than 80 countries have data privacy laws, and Turkey, India, China, Brazil, Singapore, and other countries are clamping down on data security malpractice and rigorously enforcing national and regional laws regarding personal and sensitive information. Additionally, 11 states in the United States passed or updated privacy laws in 2018.

Holistic Approach

Organizations can no longer rely on siloed and legacy approaches to discovering, analyzing, protecting, and monitoring personal and sensitive data. With the threat of massive data breaches, substantial penalties, and the need to maintain customer trust, organizations today urgently need to shift to a new data-centric security paradigm that takes a holistic approach with

- Centralized data security governance that automates data discovery and classification, and efficiently handles policy definition and mapping to data elements
- Implementation of security and protection, such as access and data movement controls, masking, and encryption at the data element level
- Identity-based intelligence, which provides global and granular linking of sensitive data based on identity to support data subject access requests and integration with consent management
- Continuous monitoring and risk analysis to automate remediation, prioritize activities and investments, and simplify audit and reporting

Until relatively recently, traditional security and data protection were point-in-time activities that involved protecting a well-defined perimeter. This approach no longer works. Privacy requirements are forcing protection activities to be centered on the data itself and integrated by design into everything an organization does with data. Effective privacy strategy includes continuous protection that can be adapted in line with shifting priorities and emerging threats at the asset level.

Greater Individual Rights

Regulations such as the GDPR and the CCPA empower individuals to be more proactively involved in the management of their personal data. For example, the GDPR provides individuals with the following rights, among others:

- Right of access (including the purposes of personal data collection and processing, categories of personal

data collected and processed, recipients of personal data)

- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to data portability (receive personal data about yourself in a structured, commonly used, and machine-readable format)
- Right to object (for example, profiling and automated decision-making based on personal data)

REMEMBER

Independent of any regulatory requirements, people expect organizations to ensure proper and ethical use of their data and implement appropriate safeguards to protect it.

Recognizing the Business Benefits of Data Privacy

What used to be an IT concern is now an urgent issue for customers as well as your board, your partners, and regulators. This issue puts pressure on you and your team, but it also creates opportunities. There are clear business benefits to embracing data privacy. A well-managed, robust data privacy program that includes well-defined policies and properly deployed controls offers numerous business benefits:

- **Increasing customer trust:** People want to do business with organizations that are demonstrably taking data privacy seriously. According to Capgemini, 77 percent of consumers consider cybersecurity and data protection when choosing a retailer. PwC found that 27 percent of consumers say they'll pay more for better security and privacy features, yet few businesses are meeting this demand as only 25 percent of consumers believe companies handle sensitive personal data responsibly.

  The opportunity here is clear. Prove your data privacy and ethics credentials through strong policies and a clean record, and you'll earn all-important trust that forms the foundation of longstanding customer relationship loyalty.

TIP

- **Reducing overall business risk:** Organizations can reduce security, privacy, and compliance risk by discovering, identifying, cataloging, and protecting their sensitive data. More importantly, they can reduce risk to brand reputation, customer purchasing behavior, and business with partners.
- **Accelerating digital transformation:** Data privacy and governance programs give you the opportunity to establish a data foundation for digital transformation. They help you discover where data resides across the organization; understand the processes, systems, and people that use the data; and create policies and business rules for quality, protection, and use of the data. These discovery, cataloging, mapping, and governance activities are beneficial to digital business initiatives such as
  - **Analytics and machine learning** — less time required for data scientists to find data and determine if they can use it in a compliant manner
  - **Business process optimization** — simplified, automated, and compliant data exchange between systems
  - **Customer experience** — increased understanding of what data is available and how it can be used responsibly to preserve customer rights across commerce channels
- **Driving cultural change:** Data privacy and ethics require change in the way people think and act regarding the use of data. Providing a comprehensive and centralized view of policies, processes, and responsibilities helps everyone understand his or her role. And a data privacy approach that focuses on applying the right method at the right time to the right type of data encourages collaboration.


TIP

Cyber insurance companies integrate data security into their actuarial analysis. Privacy, security, and data governance programs help you demonstrate a strong risk management posture that can lower your premiums. These examples are just a few — the bottom line is that data privacy isn't just a compliance issue; it's a business imperative for any company to stay competitive by safely unleashing new value creation from data.

IN THIS CHAPTER

- Creating data privacy policies
- Prioritizing investments and resources through collaboration
- Consolidating data privacy management for worldwide compliance
- Eliminating manual processes
- Taking action on customer and regulator requests
- Ensuring readiness and measuring results
- Providing data access on a need-to-know basis

Chapter 2
Defining Requirements for Data Privacy at Scale

In this chapter, you explore some important business requirements that enable you to scale your data privacy program to meet your organization's needs.

Specifying How Data Can Be Used and by Whom

Data policies that specify how data can be used and by whom are at the heart of data privacy and governance. Corporate policies that reflect regulatory requirements and customer expectations must be documented to form the foundation of your data governance efforts.

REMEMBER

Some important data governance policies that need to be documented and maintained include

- **Data accountability and ownership:** These policies spell out which senior business leaders, or combinations of business leaders (such as a steering committee), are accountable for the quality, privacy, and security of critical data. The policy must outline what ownership means and define the rights and responsibilities of the owners.
- **Organizational roles and responsibilities:** These policies document and make clear the responsibilities of your business and IT data stewards, data governance driver, and other dependent stakeholders.
- **Data capture and validation standards:** These policies define minimum required data capture standards, data validation rules, reference data rules, and so on. The goal is to ensure the people, processes, and systems that capture, import, update, transform, or purchase critical data do so in a consistent, standardized manner with a focus on quality.
- **Data access and usage:** Data usage policies ensure appropriate use of data by appropriate stakeholders. Limiting access to sensitive or confidential information supports compliance with the European Union (EU) General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other privacy legislation. Organizations should enforce "need to know" and the "principle of least privilege" (individuals should only have access to the minimum data and have the minimum permissions necessary to perform their assigned duties) approaches to authorizing data access and use.
- **Customer communication privacy preferences:** These policies help support compliance with customer and subject rights such as the right-to-be-forgotten, transparency, erasure, and objection to sale or transfer. These policies are meant to be transparent, customer-facing documents.
- **Data security:** These policies define what data can be accessed by whom and clarify how it needs to be protected (masked, blocked, encrypted, and so on). These also ensure consistency across multiple applications and database instances. The access of data depends on role and use and

varies for business users, researchers, testers, customer service, application testing, and other mission critical roles.

- **Data retention and deletion:** Retention policies must balance the desire to archive and purge unused data to reduce storage costs and business risk with business and legal discovery retention management requirements. These policies will clarify what data needs to be stored for how long, in what format, applying what rules, with what level of masking or encryption, and with what access guidelines.

Fostering Collaboration among Key Stakeholders

Many different business functions have responsibilities and oversight with regard to data and data privacy within an organization. Collaboration among key stakeholders is key, ensuring investments and resources are prioritized appropriately to support your data governance and privacy programs. Stakeholders include privacy, security, and data officers and their teams. Decision makers need to track overall privacy readiness and key risk indicators (KRIs), while practitioners need to collaborate on new risks, alerts, and subject requests.

Managing Different Regulations and Geographies

There are literally hundreds of data security and privacy regulations and standards at various levels of government and industry around the world (see the examples listed in Chapter 1). These regulations are complex and may introduce conflicting or differing requirements across the different mandates with which your organization must comply.

The growing mountain of legislation and other legal and industry requirements call for an integrated privacy solution rather than "one-off' customized solutions. With an integrated solution, organizations can track privacy readiness by regions and/or policies to understand readiness for specific privacy requirements as well as their overall privacy posture.

Automating Manual Processes

Manual processes and siloed solutions don't scale, and consolidation and normalization of their outputs is time-consuming and error prone. To provide consistent results in a timely manner, organizations need to automate their data management and privacy processes. Automation enables businesses to leverage real-time analytics, machine learning, and artificial intelligence (AI) to improve consistency and objectivity, and to support standardization and scaling across the enterprise.

Responding to Customer and Regulator Requests

Customers and regulators expect and demand that companies respond promptly to their privacy and audit requests. Regulations such as the GDPR mandate specific requirements for responses to subject access requests (typically 30 days) and breach notifications (typically 72 hours). Failure to comply with provisions such as these can subject an organization to stiff fines and penalties, and erodes customer confidence and loyalty.

Companies must proactively define and, to the extent possible, automate their policies and business processes to enable them to respond promptly and accurately to requests from customers, regulators, auditors, and others.

Monitoring Readiness on a Continuous Basis

Continuously monitoring readiness and compliance is imperative to ensure organizations don't run afoul of regulators and customers. The volume and velocity of data today, as well as the scale and sophistication of data breaches (I discuss these in Chapter 1), render point-in-time monitoring solutions ineffective for ensuring adequate data security and privacy. Organizations can monitor KRIs such as anomalous use, unexpected data movement, and excessive access by users.

Ensuring Appropriate Data Access and Usage

To ensure sensitive data isn't improperly accessed or used, organizations need to bound data access to identities and provide access to users on a need-to-know basis. With data security policies, user access can be controlled by individuals, groups/roles, and environments. This is potentially the most critical factor in ensuring the proper use and access of personal data: that is, by tightly controlling data access based on the validated and authorized business purposes for each user.

IN THIS CHAPTER

- Establishing a data governance program
- Discovering and identifying your personal and sensitive data
- Linking identities to individuals
- Understanding data risk
- Protecting data and managing privacy requirements
- Tracking compliance and other key measurements

Chapter 3
Implementing an Intelligent Data Privacy Solution

Organizations today deal with huge volumes of data moving faster and further than ever before. If you can apply security controls at an asset level for data privacy, you can protect data wherever it resides — even when it leaves your organization.

Implementing an effective data privacy program is challenging, but it's not insurmountable. In this chapter, you find out how an intelligent data privacy solution can help you effectively address these challenges.

Define and Manage Governance Policies

Understanding the purpose, use, systems, and people related to the processing of personal data helps you build privacy policies, assign accountability, and provide transparency for data subject rights. The organization can clearly define what business processes data supports, who is using the data, and the regulations that govern it. Data governance programs are often driven by regulatory compliance requirements.


TIP

New data governance programs often need to start small, taking on one project at a time to work through the policies, processes, and procedures for the new program. For compliance, this means that programs need to focus on the groundwork that's needed around a privacy regulation, while also looking for opportunities to govern data holistically as a high-value enterprise asset as the program grows.

When setting up a new program or working through the guidelines of a new privacy regulation, you need to identify several key items. You need to build out high-level, internal policies such as who can safely access the data and how team members will work together with the data across organizational boundaries. You will also need to build out a business glossary or data dictionary. The glossary will become the single source of truth for a data element (for example, defining who exactly a "customer" is for all team members).

In practice, this means your organization will be empowered to

- Collaborate across business functions to capture and align policy definitions and requirements
- Document the processes for fulfilling and managing subject rights requests
- Track privacy program adoption and success throughout the organization

Next, you need to assign ownership and accountability for enforcement, management, response, and remediation of each data governance and privacy policy.

TIP

To help you define and manage your governance policies, look for a data privacy solution that can

- Manage all data policies as part of an integrated solution, rather than a separate application
- Map system and business process flows for sensitive data
- Visualize privacy and protection outcomes in context
- Report outcomes to all affected stakeholders
- Provide an audit trail over all governed artifacts
- Automate responses to data subject requests at the point of interaction

Discover, Classify, and Understand Personal and Sensitive Data

Traditional data discovery and classification tools identify databases and repositories that contain personal data by listing the locations, and table and column names, where that data resides. While this approach offers some insight into where protection may be needed, it does not provide any guidance on where to start, where the sensitive data proliferates through other data stores, or whether the data has already been protected. Today, most data resides outside traditional databases, and these resources must be accounted for to have a full picture of data privacy risk and protection needs.

To effectively discover, classify, and understand personal data in your organization, you need a data privacy solution that automatically locates the data, ranks risk, and classifies data to provide a broad and deep understanding of where data resides and how it proliferates throughout your organization.

TIP

Find personal data across your organization, wherever it exists, and classify its sensitivity and importance based on internal policies and external regulations. Examples include structured data across traditional relational databases, such as mainframes; semi-structured data such as comma-separated values (CSV), eXtensible Markup Language (XML), and JavaScript Object Notation (JSON) on Hadoop Distributed File System (HDFS) and

Amazon S3; unstructured data on Common Internet File System (CIFS) Network File System (NFS); and SharePoint traditional structured data stores.

The solution should also be able to import data protection methods and status from data stores that are already protected. In addition, look for these features to ease administration and scaling:

- Agentless scanning
- Ability to schedule scan jobs
- False positive detection and handling
- Ability to configure scans to leverage artificial intelligence (AI) and machine learning, with configurable options to optimize performance and accuracy

Next, you need the capability to discover and classify personal data, which involves creating and modifying search definitions for sensitive data domains (such as credit card numbers, addresses, names, or other personal information) and creating custom classification policies as necessary to comply with privacy regulations.

Ideally, the solution should come with out-of-the-box data rules and policies for compliance with major regulations and industry standards, such as the European Union (EU) General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), U.S. Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS). The solution should also provide the ability to

- Leverage classification policy templates to quickly create private data definitions and specify the data's sensitivity level
- Support customization of rules and classification policies to cover additional requirements
- Create search definitions for both metadata and data, using pattern matching, reference tables, and complex combination rules
- Create advanced search rules
- Minimize false positives through conformance scoring
- Estimate the cost of data loss

Data proliferation involves determining and tracking where sensitive data has moved to other data stores in your organization, and providing drill-down capabilities to understand, monitor, and protect data wherever it proliferates.

Ideally, the solution should come with out-of-the-box tools to

- Track sensitive data movement through data stores from third-party metadata providers (for example, Microsoft, Cloudera, Hortonworks), and provide a drill-down capability to view which personal data domains and columns are proliferating between two selected systems
- Ingest custom proliferation data
- Provide rich visualizations of your organization's personal data and its proliferation patterns across geographies and logical boundaries

REMEMBER

Make sure to identify international transfers and understand the regulatory requirements based on region.

Map Identities

Identity is core to privacy. To support many privacy requirements, personal and sensitive data must be accurately and holistically mapped to the individuals it represents in various systems. This helps you address data subject access rights, and data breach notification requirements.

Mapping identities supports compliance with regulatory requirements for data privacy, such as the GDPR and the CCPA, to locate data subjects (that is, individuals) whose personal data is retained in your data stores, and includes

- Identifying the individuals represented in your organization's personal data
- Understanding what personal data your organization retains for each individual
- Understanding personal data by individual identities, with information about various attributes (for example, location, data stores, risk, protection status, and use of each individual's sensitive data)

- Locating an individual's sensitive data quickly to support privacy requests, such as "What data do you hold on me?" and "Please remove all my data!"

Analyze Data Risk and Establish Protection Plans

Modeling and evaluating privacy risk based on data stores, locations, and policies helps you plan and prioritize risk remediation across functions, geographies, and lines of business. An intelligent data privacy solution calculates sensitive data risk costs based on defined policies in a common risk framework that compares data stores to each other to generate a risk score that drives the protection effort. The solution should include multiple adjustable factors in its risk framework to calculate the risk for each data store. Look for factors such as

- Classification/sensitivity level of the data
- Amount of sensitive data
- Protection status of the data
- Number of sensitive fields
- Liability cost of the data
- Sensitive data movement to other data targets
- Number of users with access to the data
- User activity against the sensitive data
- User-defined custom fields to adjust the risk model to your operating environment

You should be able to fine tune the individual weights of each of these factors based on your organization's operating environment. The platform should also include the capability to simulate and record the risk, exposure, and liability cost for each individual data store, with details about how the risk is calculated, before and after implementing protection controls.

Leveraging user access and activity on sensitive data improves risk scoring by capturing who has access to sensitive data and how it is used. It should be able to report on users and groups with

access to sensitive data by user(s), data store, time of occurrence, and other criteria, and incorporate this user activity into overall risk scoring.

Risk analytics achieve highest accuracy when a data privacy solution can continuously discover and classify sensitive data and know where it proliferates, scale for data growth, apply protection methods at the data level, incorporate custom risk criteria, monitor and track user behavior, and generate estimated costs of data loss. Figure 3-1 shows you the cycle of improving risk analytics with an intelligent data privacy solution.

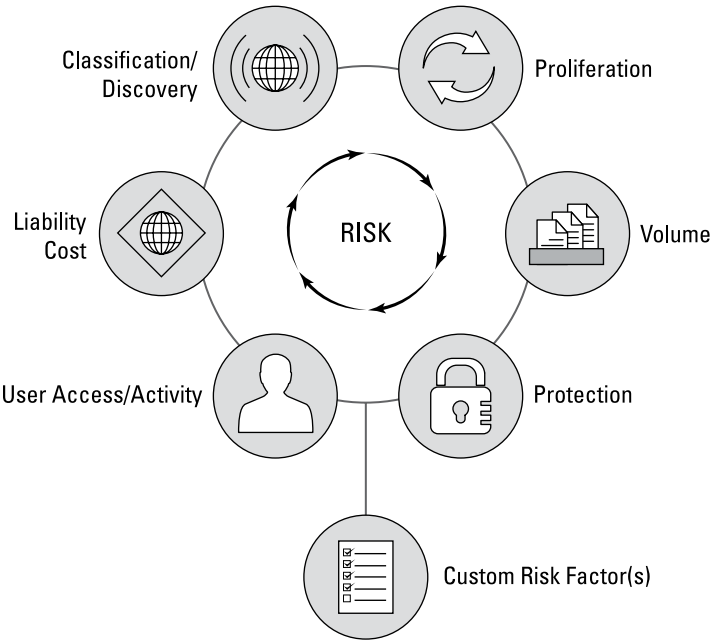

FIGURE 3-1: Improving risk analytics with an intelligent data privacy solution.

The following describes each point in the risk analytics cycle:

- **Classification/Discovery:** Define and discover physical and logical locations of sensitive data.
- **Proliferation:** The movement of data inside and outside of the organization.
- **Volume:** The number of records.

- **Protection:** How the data itself is protected.
- **Custom Risk Factor(s):** Define, measure, and argue any other criteria as risks.
- **User Access/Activity:** Frequency and volume of user activity.
- **Liability Cost:** Value of data loss to the organization.

Protect Data, Manage Subject Rights and Consent, Respond to Policy Violations

To effectively protect data, manage subject rights and consent, and respond to policy violations, you must implement access controls and encoding mechanisms such as encryption, anonymization, and pseudonymization. You also need the capability to track and monitor data use and movement and automate consent management and data subject rights requests.

An intelligent data privacy solution automatically applies defined protection policies to encrypt, mask, or otherwise protect data. You should also be able to launch these policies directly within the target data store or by initiating a protection workflow.

For data protection, the data privacy solution should support manual and automated workflows for persistent data masking, dynamic data masking, encryption, access controls, ticketing systems (for example, ServiceNow), third-party data protection (such as Ranger and Sentry), and other data protection methods. Protection policy creation should be bi-directional: Protection rules should be built within the platform and pushed to protection tools, and vice versa.

Remediation should also include capabilities to automate notifications and alerts to inform users of exceptions and other defined conditions that require their attention. It should also include the capability to create scripts that trigger automatic actions in response to an alert: for example, moving users from one Lightweight Directory Access Protocol (LDAP) group to another.

TIP

To provide comprehensive data protection, look for these features in a data privacy solution:

- Protection tools that operate across all supported data store types
- Data-centric protection, such as encryption, masking, and fine-grained access controls
- Integration with third-party tools, such as Active Directory (AD)/LDAP, Apache Ranger, Apache Sentry, and ServiceNow, and email and notifications
- A common policy framework for discovery and protection

For data subject rights, you need clear information about all the personal and sensitive information related to customer, employee, and third-party identities that your organization holds. The data must also be actionable so you can respond to data subject rights requests. Automated workflows should provide the capability to support privacy tasks such as reporting, portability, deletion, masking/anonymization, and consent management. You should also have instantaneous information about individuals, such as where their data is used and the associated privacy risk. Data privacy and compliance centers on the individual (that is, whether an individual's data is protected and whether individuals can control their own data).

TIP

Master data management (MDM) can provide automated and robust support for consent management in organizations with or considering MDM. MDM provides trusted, accurate, complete data for your customer experience program, marketing and sales operations, omnichannel retailing, supply chain optimization, governance efforts, compliance initiatives, and more. Key capabilities include

- A single view of the data, unifying multiple sources of disparate, duplicate, and/or conflicting information sources
- 360-degree view of critical data and its business relationships with other data
- Complete view of all interactions, linking all transactions for a full view of customer behavior

Measure, Communicate, and Audit Response

Tracking compliance and risk indicators enables you to align your privacy strategy and operations. In a data privacy solution, this capability provides visualizations and reports to support cross-functional collaboration and satisfy auditors. Moreover, you can continuously measure your organization's risk to gauge how well policies and processes impact data risk.

In order to meet the data privacy interests and requirements of business function stakeholders, the platform should provide dashboards and visualizations that track data privacy key risk indicators (KRIs), such as

- **Risk score:** Based on risk metrics such as protection status, access, and liability cost, tracks the risk of privacy data across the enterprise
- **Protection status:** Provides overall data protection status of personal and sensitive data
- **Residual risk:** Provides tracking of overall data risk (monetary value) based on personal and sensitive data access, protection status, and classification
- **User access:** Tracks user access of protected and unprotected data


TIP

In addition to the capabilities already discussed in this chapter, some additional key requirements for an intelligent data privacy solution include

- **Automation of processes and controls:** Given the volume of data, users, and applications to scan and protect, automation is key to ensuring predictable and reliable results and scaling for enterprise coverage.
- **Standardization, consistency, and auditing:** To protect thousands of data stores, organizations need to standardize data definitions and associated protection and governance policies. Without centralized policy management, organizations can't consistently manage policy changes, or audit and track compliance.

- **Accuracy and effectiveness:** To maintain a high, reliable level of accuracy in a constantly changing environment, a data privacy solution requires data context, subject identity mapping, user behavior analytics, and risk analysis. Without them, the organization won't have the intelligence to effectively prioritize data protection resources and investments and monitor data use for potential privacy violations.
- **Continuous protection without interruption:** A data privacy solution must be flexible enough to maintain data protection and compliance insights in an environment where data, usage, users, and regulations are in constant flux. If a solution cannot support policy customization and regular reassessment of risk, it can't provide truly continuous protection of private data.
- **Out-of-the-box deployment readiness:** Pre-defined data policies and domains for regulations and common personal data types help organizations quickly access privacy risks and map their privacy data. Additionally, with integrations to popular security solutions and application programming interfaces (APIs), organizations can rapidly integrate and leverage existing investments in enterprise security controls, such as single sign-on (SSO), password management, and data protection such as masking, encryption, and tokenization solutions.
- **Support for hybrid environments:** Any solution you choose must cover all your data sources, whether managed in traditional on-premises systems, multi-cloud environments, or big data anywhere — consisting of either structured or unstructured data formats.

IN THIS CHAPTER

- Complying with privacy legislation
- Earning customer trust and reducing risk with data privacy
- Accelerating time-to-market and business agility with DevOps

Chapter 4
Exploring Data Privacy Use Cases

In this chapter, I give you some common data privacy use cases and real-world customer success stories.

Privacy Compliance

The European Union (EU) General Data Protection Regulation (GDPR) went into force in May 2018, affording enhanced protection to the personal data of EU residents. The GDPR applies to any organization established in the EU and to any organization (anywhere in the world) that processes the personal data of EU data subjects (*identified* or *identifiable* natural persons) when offering them goods or services or when monitoring or tracking their activities.

The GDPR can have a significant impact for many organizations in how they manage data pertaining to customers, consumers, partners, staff, and other data subjects. The GDPR impacts the storage, processing, access, transfer, and disclosure of an individual's data records, and imposes some potentially very large penalties for violations.

The GDPR requires organizations to fully understand how they use current and future information assets to incorporate these new data privacy requirements and enhance privacy rights. For many organizations, the associated changes to information management practices will require a thorough evaluation of current and future data capabilities.

On the heels of the GDPR is the California Consumer Privacy Act (CCPA). The CCPA requires organizations that collect or sell data about California residents to respond to rights requests by California residents and to take reasonable measures to protect their data.

The CCPA joins a growing movement of worldwide privacy legislation designed to provide privacy rights to individuals and to give them greater control over the use of their personal information. The CCPA grants consumers rights to control use of their personal data and prevents businesses from discriminating against them for exercising those rights. In particular, consumers can ask about the categories and specific elements of personal information a business has collected about them and the purposes for which the business uses that information. Consumers can ask the business to delete personal information it has collected about them or request that their personal data not be sold to third parties. The CCPA also obligates businesses to implement and maintain reasonable data security policies and procedures appropriate to the nature of the information.

The CCPA also creates a private right of action (with potentially high liability for businesses) for any breaches of that obligation that result in unauthorized access to personal information covered by California's breach notification law.

Privacy officers and security teams need automated tools to effectively manage data privacy readiness. Unfortunately, privacy officers are often frustrated by the inability to identify, locate, and assess personal information; facilitate cooperation and collaboration among business, privacy, and IT; and effectively protect and monitor personal information.

TIP

Visit `www.informatica.com` for more info on the GDPR. Search for *GDPR Compliance For Dummies* and download your free copy.

PRIVACY COMPLIANCE

A North American insurance company with more than 2,500 employees is among the top 100 insurance organizations in the country based on net written premiums. Maintaining the trust of its clients and policyholders is a top priority for the company. In order to keep all data private, meet privacy rights requirements, and deploy solutions for data discovery and data masking, the organization had the following goals:

- Respond to rights requests such as data access, right-to-be-forgotten, and do not sell
- Secure sensitive, private data of policyholders and clients to remain compliant with industry regulations such as the GDPR, the CCPA, Health Insurance Portability and Accountability Act (HIPAA), and others
- Lower risk associated with the modernization of systems, including Microsoft SQL Server and Atlassian Jira
- Become more adaptive to market changes while moving products to market faster

To successfully address its key business goals, the company defined the following as priority challenges:

- Establish data privacy methodologies in a more agile environment
- Obtain actionable data discovery and classification, risk scoring, behavioral analytics, and automated protection in a single solution
- Identify personal data by identities to support rights and access requests

After implementing Informatica data discovery and data masking solutions, the company achieved the following results:

- Full scope of visibility into sensitive data and risk
- Enhanced capabilities to effectively respond to rights requests
- Modernized, agile environment created by transformed data systems
- Continuous, accurate compliance measurement of privacy data with dashboards to track status and risk indicators
- Data remediation prioritization via data masking, access controls, and encryption using risk and protection simulations
- Access and movement monitoring for violations of policies

TIP

GDPR and CCPA compliance offer new opportunities to implement best practices through automation that can optimize future data handling and use.

Data Protection

Beyond regulatory compliance requirements, organizations must ensure robust data protection programs to reduce risk and earn customer trust. Data protection must be woven into the fabric of your organization. It must be applied on an enterprise-wide scale and it must involve everyone — because everyone uses data and needs to do so responsibly.

REMEMBER

Consumer awareness of data privacy and security continues to grow. Trust assurance has become an increasingly key factor — more important than price — in many purchase decisions.

DATA PROTECTION

A major North American healthcare organization is transforming how it does business, including operations and enterprise architecture. These changes will enable the organization to have superior agility to deal with dynamic customer and market conditions. It's leveraging this transformation to infuse data protection and privacy across the hybrid architecture. From the top down, the organization has identified customer trust as its top goal. For the data protection program, it had the following goals:

- Ensure that the data protection program covers all customer personal and sensitive data
- Implement data protection that doesn't create operational differences for users of its applications and services
- Meet the requirements of the GDPR, the CCPA, HIPAA, and other regulatory requirements for anonymization

Based on the company's operating challenges, it needed to address the following business requirements:

- Improve the usability and access of its services
- Protect information to prevent misuse or data loss to maintain and grow customer trust
- Protect data in operations, DevOps, and analytics

To address these goals and requirements, the organization implemented a data protection solution to accomplish the following:

- Identify where personal and sensitive data resides
- Anonymize data used for test and analytic environments
- Dynamically mask data for operations based on user's role, location, and time of access

With data protection across all its personal and sensitive data, the organization has achieved the following results:

- Reduced the risk of data misuse and loss
- Implemented controls that don't negatively impact transformation
- Improved privacy readiness and reduced data privacy risks

DevOps Privacy

DevOps enables more frequent, timely, higher quality software delivery by deploying automated tools for test, release, configuration management and continuous integration, while fostering collaboration across the various teams involved in a release. Ideally, test data used in the DevOps test environment presents a subset of representative production data. This data must be protected for data privacy in the same way as other sensitive data in the organization.

Many quality assurance (QA) teams prefer using production data for testing because it represents the most realistic environment to test. However, production data contains personal information that should not be exposed to developers and testers, especially when testing is outsourced or offshored. This data can be anonymized when used in non-production environments using various masking techniques (such as encryption, substitution,

aging, pseudonymization, and anonymization) to ensure no user can view or easily deduce the original data. Masking ensures no user can view or easily deduce the original data, while maintaining the original characteristics of the data and consistency across related masked data, thus ensuring test data quality.

DEVOPS PRIVACY

A leading global provider of on-demand marketing solutions empowers businesses to market more effectively through email, web, print, mobile, and social media channels. This provider had the following business needs:

- Provide better service to customers and gain faster time-to-value
- Enable customers to create complex time- and behavior-driven marketing campaigns across multiple channels
- Control IT development costs
- Protect personal and sensitive data from misuse and unauthorized access

With these needs, came several challenges:

- Support the launch of new on-demand marketing products
- Build a scalable data-integration platform for business growth
- Manage complex data movements across numerous systems
- Enable tester efficiency with on-demand access to test data

After implementing a data protection solution, the company has achieved the following results:

- Removed private and sensitive data from test environments
- Enabled self-service provisioning of test data
- Reduced software development time by 50 percent
- Accelerated customer onboarding by up to 40 percent
- Helped ensure successful launch of a new Software as a Service (SaaS) offering
- Will cut R&D and support resources by 50 percent
- Will handle expected 20 percent increase in event-data volume

IN THIS CHAPTER

- Defining how data is used and how to protect it
- Understanding your data's value and risk
- Ensuring rapid response and management of rights
- Baselining user activity and identifying anomalies
- Leveraging analytics and automation
- Measuring progress

Chapter 5
Ten Keys to Successfully Implementing a Data Privacy Solution

In this chapter, you get the ten keys to implementing an effective data privacy solution in your organization.

Define How Data Is Used

Implementing an effective data privacy solution requires you to first understand what data your organization collects, processes, and stores, and for what business purposes. The data itself also needs to be understood in terms of how it is used within the organization. This enables data to be accurately classified and identified, and appropriate safeguards and controls to be implemented.

Here are key questions for defining your data:

- What types of data are we using and for what purposes?
- What legislation regulates our use and security requirements?
- Who are the business and technical owners of the data?


TIP

Read Chapter 2 to learn more about defining how data is used within your organization and other business requirements for data privacy.

Know Your Data's Value and Risk

With definitions of what data your organization holds, you can determine the value and risk associated with your data and identify appropriate protective policies, procedures, and technologies. Understanding the potential liability arising from breach or misuse of data you hold provides insight to prioritize privacy resources and investments.

Risk also accounts for the transient nature of data. If one characteristic of a data asset changes — say, its volume, location, usage, or proliferation, protection, and so on — its risk score can be adjusted accordingly.


TIP

Chapter 3 provides more information about analyzing data risk.

Many of the criteria behind your risk framework will be unique to your business, but to help guide your thinking, here are a few questions:

- How frequently is the data accessed, and is access controlled?
- Is the data protected?
- What is the volume of data?
- Does it proliferate across borders, departments, and functions?

Organizations should discover and classify data and understand its movement and uses. Then, based on how the data is used, where it is located, and how many people access it, determine its relative risk to the organization. This intelligence provides the

baseline for the privacy program to measure progress and determine remediation.


TIP

You probably won't be able to answer these questions alone, so reach out to the people who use this data daily. Conducting interviews, surveys, and assessments with application owners, security analysts, database administrators (DBAs), business analysts, and frontline staff will expose data types and shed light on user roles, data owners, and business uses. Today many tools can help automate and support your efforts.

Ensure Rapid Response and Management of Rights Requests

The European Union (EU) General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other privacy legislation put individuals more in control of their data rights. Although each law has unique provisions, privacy readiness needs to account for the rapid response and management of rights requests. Organizations must respond in a timely and thorough manner to rights requests, applicable to the jurisdiction, such as access requests, the right to be forgotten, erasure or change of consents, and other requests as required by various legislation.


TIP

Chapter 1 provides a brief summary of the GDPR, the CCPA, and various other privacy regulations and standards, as well as helpful links to these regulations and standards. By understanding what data belongs to which individuals, the organization has the foundation for managing rights requests.

The mapping of identities should be to the data stores that contain their personal data. Organizations will also need workflows that leverage automation to manage consent and respond to rights requests.

Take a Phased Approach


WARNING

Because of the scale of challenges to data privacy and protection, don't attempt to perfect and automate all your processes at once. Not only is this approach unrealistic but also, more importantly, it's dangerous. The further you stretch your capabilities, the more likely it becomes that something will slip through the net.

A phased program makes more sense. Start off with your most sensitive data, a small group of people, and a clear objective. Then once you've achieved demonstrable results, you can scale your program to tackle new challenges.


REMEMBER

By understanding the data value and risk (as highlighted in the previous sections), organizations can address their privacy program systematically. They can prioritize departments, processes, and/or regional systems that will have the most impact on their privacy readiness. Very few organizations, if any, can simultaneously address all their privacy risk and issues. Organizations can also take the guesswork out of expected outcomes through risk simulations, which can help organizations determine the impact of new controls and safeguards before they are implemented.

Don't Compromise on Access

New data protection and privacy regulations have placed fresh emphasis on the importance of making personal information accessible, based on business need. Under the GDPR, you need to be able to delete or amend customer data in line with customer demands. You also need to honor customer requests to withdraw or grant consent. Chapter 2 discusses customer requests such as withdrawing and granting consent, and other privacy rights requests.

These requirements mean that you need immediate and granular control of data. Personal data may need to be removed or obfuscated based on rights requests, and controls may need to be adjusted to the permissions granted by the individual. These actions must be taken across all systems where the individual's data is used and/or stored (unless exceptions are permitted by the relevant regulations).

Trigger Alerts for Policy or Behavior Expectations

Data doesn't compromise itself — in the majority of cases, insider mistakes or malicious actions are at fault. To determine why and how, the security team needs to leverage automation with intelligence from analytics based on artificial intelligence (AI) and

machine learning to easily and quickly identify unusual user behavior such as excessive access. Suspicious events are then more easily detected and more accurately reported, so IT can take proactive steps and remediate potential threats faster.

Assigning specific protection tools and techniques for each type of policy, noncompliance category, or suspicious activity makes the security team more efficient and effective. In some cases, it might work best to take a fully integrated, automated approach to sensitive data protection. For example, when an intelligent solution detects that a user is accessing more Social Security number (SSN) records than normal, a script could automatically activate to dynamically mask the data or move the user to a high-risk user group. In other cases, the security team might simply want to generate an alert that requests or requires manual intervention by the data owner or application owner.

In addition, organizations should establish security policies for data movement or purpose. For example, data moving across geographic or logical boundaries, data being used for a purpose other than the original captured purpose, or data without a purpose. Automation can notify or even create service management tickets to ensure proper tracking, action, and resolution.

TIP

As the security team configures and rolls out the data protection solution, it will need to perform the following activities:

- Define what protection methods or actions to use for each asset type and user.
- Ensure that subjects' personal data is protected in compliance with applicable privacy regulations.
- Monitor the effectiveness of the solution continuously and adapt as required.
- Expand the scope to more users and more information asset types.

Focus on the Data

Knowing where personal and sensitive data resides, how it's being used, and who is using it is critical to determining how to protect it. Regardless of location, layered data controls provide

the best protection. Personal and sensitive data should always be encrypted at rest and a combination of data masking and access controls provide the safeguards to help support the proper access and use of personal and sensitive data. Data lakes accessed by multiple users and applications will need to take location, time, and necessary levels of privileges into account when setting up access rules.

Test environments pose their own challenges. Functional testing environments need realistic data to continue operating smoothly. Protection (for example, anonymization) applied to columns of personal data needs to ensure that the relationships between tables remain intact.

In cross-system business processes, protecting sensitive columns must not break the process. Persistent masking can be deployed in reporting, analytical, and test environments that have little or no need to restore the protected data to its original value.

In production systems, organizations should protect data at rest and data in use appropriately for different groups of users. In these cases, data needs to be completely protected from some users and only partially protected from or entirely available to others. A banking call center provides an obvious example of this: Database administrators (DBAs) don't need to see a caller's SSN at all; customer service reps need to see the last four digits; and back office users who validate the caller's credit history need to see the full SSN. This fine-grained access control needs to take place dynamically.

Make Protection a Team Sport

Application owners and privacy analysts must work together closely with the DBAs who are responsible for maintaining data operationally on a day-to-day basis. A business process orchestration tool can automate and measure the handoff process among these three by ensuring the right level of data privacy at all times, updating internal systems to reflect that data is protected, and recalculating the risk associated with the data so the privacy analyst who initiated the protection request can be confident the protection job is complete.

Lead the Way forward with Intelligent Automation

A policy-based, intelligent, automated data privacy solution leverages analytics based on AI and machine learning for compliance reporting, risk analysis, user behavior monitoring, and security orchestration and remediation ensures that even in a fast-changing environment, data remains up-to-date and secure. Discover more about analytics, AI, and automation in Chapters 2 and 3.

Best practices are to implement rules that continuously scan new data and changes to metadata. If a data-related anomaly emerges, the data protection solution can automatically create an alert for a policy violation and send a notification to the appropriate stakeholder to suggest corrective action.

For example, a solution that leverages automation can alert an application owner to take corrective steps to protect data if a new column that contains account numbers appears in an existing system due to a metadata change.

In addition, the solution can combine AI with automation for faster response to user behavior that could signal a security threat. When user access, roles, and profiles are clearly defined, and user and entity behavior analytics (UEBA) are leveraged, an intelligent solution can efficiently spot user activity that diverges from normal behavior patterns or signals unauthorized access to sensitive records, and then provide notification or automated remediation.

Continuously Monitor and Measure Progress

By implementing a reliable and systematic approach that sets an organization on its data privacy journey, the requirements of today's new privacy mandates can now be achieved and measured. In addition, the essential pieces are now in place enabling business to scale with future data growth safely, no matter how various compliance mandates may evolve over time that require adjustments.

As such, organizations now need to track compliance and risk indicators continuously to align privacy strategy, investments, resources, and business operations to ensure ongoing progress toward established organizational goals and compliance requirements. Having a reliable approach to routine audits that enable privacy control attestation can help avoid future headaches in the event of a potential breach alert or an investigation that requires taking quick and decisive action.

The good news is that a monitored, measured data privacy program also helps lay the groundwork for improved data governance — enabling IT optimization from better data quality and new business value creation from untapped opportunity as a result. Organizations with a data privacy understanding are better in position to leapfrog the competition by unleashing the upside of digital transformation. Safe access and use of personal and sensitive data can now generate new opportunities with trust assurance built in to support customer loyalty from responsible data use.

TIP

Organizations can track key risk indicators (KRIs) and metrics, such as the percentage of data protected, and overall data risk based on automated risk measurements.

Informatica

Data Privacy is a Business Imperative

Although market forces are fueling data privacy regulations, it's important to remember that it's not just about compliance. The strong data governance and protection policies and programs required by legislation will also materially impact business success. Your customers, employees, and partners expect you to handle their data ethically and responsibly.

New technologies can help automate tasks, increase transparency, and orchestrate collaboration with precision. With a holistic approach and a unified technology strategy, you can be ready for the constantly evolving data privacy landscape. We invite you to explore all that Informatica has to offer—and unleash the power of data to drive your next intelligent disruption.

For more information on Informatica data privacy and protection solutions, please visit https://infa.media/DGforCustomerData

Develop trust & opportunity with data privacy

Digital transformation is driven by data with opportunity for new insights and cloud economies. But to unleash its potential, personal and sensitive data must be handled responsibly. While evolving privacy mandates threaten non-compliance penalties, the true cost is lost customer confidence when a security breach or abuse impacts trust and brand value. The good news is data privacy best practices enable the governance you need to safely expose data for improved business outcomes. Start your journey today.

Inside...

- Understand the data privacy imperative
- New compliance mandates (GDPR, CCPA)
- Business requirements to scale privacy
- Implementing a reliable solution
- Exploring data privacy use cases
- Ten keys to successful data privacy
- And much, much more

Informatica

Lawrence C. Miller has worked in information technology in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 150 *For Dummies* books on numerous technology and security topics.

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-60452-5
Not For Resale

for dummies®
A Wiley Brand

Also available as an e-book

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.