What is data protection and why is it important?

April 2024

TechTarget

In this guide:

Data protection is the process of safeguarding data and restoring important information in the event that the data is corrupted, compromised or lost due to cyberattacks, shutdowns, intentional harm or human error. It embraces the technologies, practices, processes and workflows that ensure rightful access to data, so the data is available when it's needed. Use this guide to explore more about data protection, including key principles, best practices, technologies and trends.

What is data protection and why is it important?

RON KARJIAN, INDUSTRY EDITOR

Data protection is the process of safeguarding data and restoring important information in the event that the data is corrupted, compromised or lost due to cyberattacks, shutdowns, intentional harm or human error. It embraces the technologies, practices, processes and workflows that ensure rightful access to data, so the data is available when it's needed.

To protect data and ensure access, proper data protection can depend on several different technologies and techniques, including the following:

- Magnetic or solid-state drive storage devices, storage servers and storage arrays.
- Traditional data backups, continuous data protection and high-availability techniques.
- Storage tiering for more important or frequently accessed data.

To ensure data is retained and handled in a suitable manner, data protection must be supported by data inventory, data backup and recovery, and a strategy to manage the data throughout its lifecycle:

- Data inventory determines the amounts and types of data present across the enterprise and ensures all detected data is included in data protection planning and lifecycle management.
- Backup and recovery safeguards data against hardware failures, accidental loss or intentional malfeasance, tracks the frequency of backups and outlines the process of data recovery.
- Data lifecycle management involves the tools and processes to oversee how data is classified, stored, protected and eventually destroyed according to internal data protection policies as well as industry standards and privacy laws.

WHY IS DATA PROTECTION IMPORTANT?

We collectively create about 2.5 quintillion (million trillion) bytes of data worldwide every day. How enterprises collect, process, store and monetize much of this data determines their business future. Establishing policies and implementing technologies to protect the integrity of and rightful access to this vital asset is paramount.

The task is not easy. Today's data protection climate is far different and more complex than just a few years ago. Data protection and privacy challenges abound. "In industry circles, consumer data is often compared to plutonium -- powerful and valuable but terribly dangerous to the handler if abused," said Mike Pedrick, vice president of cybersecurity consulting at managed security services provider Nuspire.

In this guide:

Major issues businesses and their data protection teams confront almost daily include the following:

- Managing, retaining and monetizing massive amounts of collected data.
- Determining when data has overstayed its welcome and becomes a liability.
- Preventing new and more sophisticated cybersecurity threats and data breaches.
- Securing data and files across increasingly distributed cloud environments.
- Integrating the latest technologies into existing IT and business environments.
- Realizing the full potential of AI, machine learning and now generative AI technologies.
- Complying with new and updated international and state data protection and privacy laws.
- Adjusting to stricter and sometimes nonspecific regulatory provisions that carry severe penalties.
- Coping with fluctuating budgetary and spending issues due to geopolitical events beyond the control of most businesses.

In this guide:

Data protection concerns confronting businesses

- **Data overload.** Sensitive corporate information, including intellectual property, trade secrets and other structured data, plus unstructured data, like audio, video and remote meetings, can overwhelm businesses.
- **Data privacy policies.** Implementing a data privacy program requires identifying data types, such as personal data associated with employees, customers and suppliers, plus security measures.
- **Ransomware attacks.** Attackers increasingly target data backups and storage, requiring software functions and other data resiliency features to protect against attacks.
- **Data loss prevention.** Effective implementation of DLP tools for endpoints, on-premises networks and multi-cloud environments can create problems plus drain resources and slow productivity.
- **Data access and authorization.** Hybrid workforces can set their own hours and use multiple access methods when logging in from remote and on-site locations on their computers and mobile devices.
- **Human error.** Lost smartphones, shared credentials or an accidental email containing confidential information sent to unauthorized employees or people outside the organization.
- **AI and generative AI.** Some AI models have strong management frameworks with strict policies against using real personal data or data from the internet or social media to train them, while others don't.
- **Distributed cloud environments.** Concerns surround data breaches, locality, misconfigurations, lack of patching, shadow IT, insecure APIs and vulnerabilities in cloud storage.

PHOTOGRAPH: SERGEYNIVENS/GETTY IMAGES

DATA PROTECTION VS. DATA PRIVACY VS. DATA SECURITY

The three key aspects of safeguarding data are protection, security and privacy. The three functions are sometimes considered interchangeable, but each one plays a distinctive role, depending on the organization, industry, application and geographical location.

Essentially, *data protection* safeguards information from damage, corruption or loss and ensures that data is readily available to users through backup, recovery and proper governance. *Data privacy* is about controlling access to specific data. *Data security* aims to protect the integrity of the data against internal and external threats of manipulation and malware.

DATA PROTECTION

Data protection embraces the technologies, practices, processes and workflows that ensure the availability of data, including the data's preservation, immutability and retention. In many organizations, a data protection officer or someone in a similar position is responsible for ensuring the storage of data throughout its lifecycle meets business requirements and complies with industry and government regulatory provisions.

"Today most of our laws and regulations and references to data protection have to do with protecting privacy," said Rebecca Herold, founder and CEO of consultancy

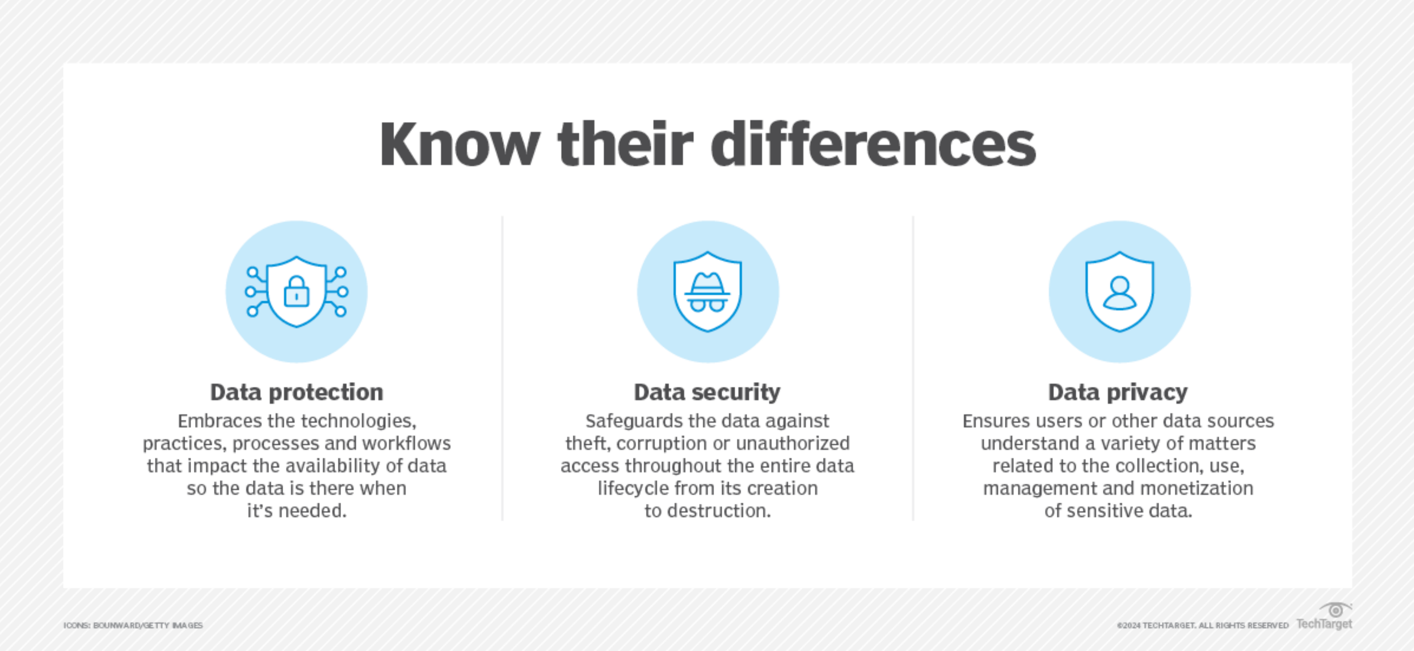
Rebecca Herold and Associates and NIST Privacy Framework participant. "And even though the term *data* is a generic term, when it is used with the word *protection*, it is typically talking about protecting personal data and information about individuals."

DATA PRIVACY

Data privacy safeguards the collection, use, alteration, retention and disclosure of personal and sensitive data. It advocates for the right of individuals to keep their information private and confidential, including the right to be forgotten. Personal data is typically information classified as personally identifiable information (PII), personal health information or financial data but can also include information that's not necessarily personal.

Businesses that exercise good data privacy practices show they're transparent about how they collect, store and use personal data so customers understand why their personal data is collected, how their data is used or shared, how their data is managed and protected, and what are their rights to add, change or limit their data and its use. A data privacy officer is responsible for developing, implementing and communicating privacy policies and procedures related to data access.

In this guide:



Know their differences

Data protection
Embraces the technologies, practices, processes and workflows that impact the availability of data so the data is there when it's needed.

Data security
Safeguards the data against theft, corruption or unauthorized access throughout the entire data lifecycle from its creation to destruction.

Data privacy
Ensures users or other data sources understand a variety of matters related to the collection, use, management and monetization of sensitive data.

ICONS: BOUNWARD/GETTY IMAGES

DATA SECURITY

Data security plays a vital role in regulatory compliance and business governance, safeguarding data against theft, corruption, improper alteration or unauthorized access throughout the entire data lifecycle.

Proper data security involves technologies and processes, storage devices, servers, network devices and the physical computing environment within the data center and throughout the enterprise. Data security also involves access control systems such as identity and access management; logging, monitoring and tracking data access;

and encryption technologies for data at rest, in use and in flight. A data security officer implements policies and procedures detailing how data is secured and accessed as well as approaches to managing security breach incidents.

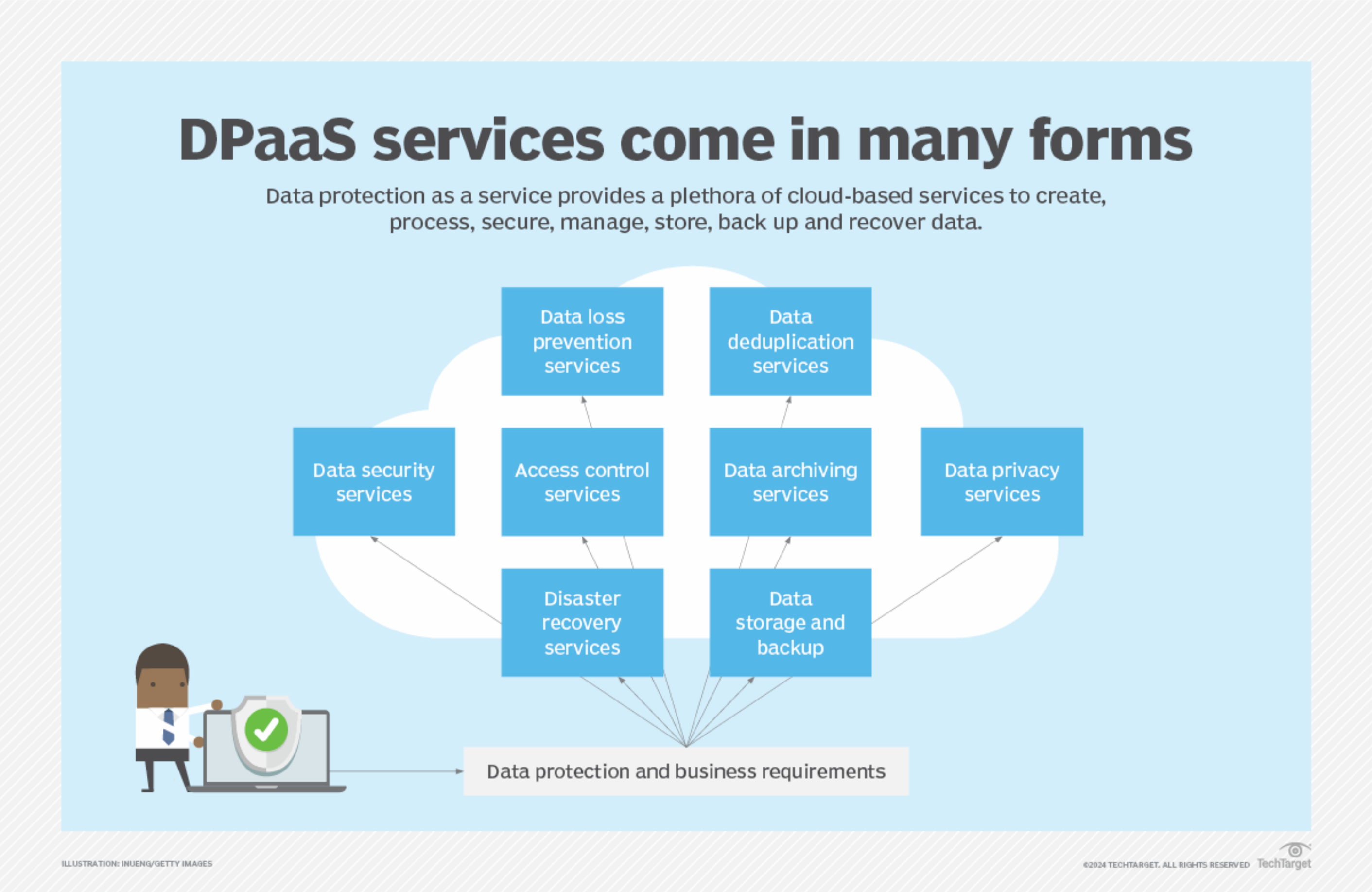
DATA PROTECTION TECHNOLOGIES

Greater frequency and sophistication of cyberthreats have forced companies to make larger investments in tools, technologies and processes that better protect and provide safer access to data. Data protection technologies provide a range of capabilities and features, including the following:

- Data backup makes copies of production data, which a business can use to replace its data in the event a production environment is compromised.
- Data portability transfers data among various cloud environments, which enables individuals to manage and reuse their personal data and protect them from cloud lock-in.
- Data recovery tools streamline or automate the process of restoring lost data and the systems that depend on them after a data breach, corruption or loss event.
- Data discovery capabilities help locate the data that businesses need to protect but might not realize exists within their complex IT environments.

- Data mapping recognizes common templates, fields or patterns and matches the data from the source to the best possible options at the destination.
- Data loss prevention for network, endpoint and cloud applications detects and prevents the loss, leakage or misuse of data through breaches, exfiltration transmissions and unauthorized use.
- Data monitoring automatically tracks access to databases and other assets to identify anomalies that could signify attempts to view, modify or delete sensitive data.

Data protection as a service (DPaaS) is considered a one-stop shop for data management and protection functions associated with creating, processing, securing, managing, storing, backing up and recovering data, all packaged in a managed service supported by cloud-based resources. DPaaS can typically reduce the need for floor space to house physical equipment and enable deployment of services faster compared to an on-site arrangement. But businesses should consider the risks of vendor lock-in when working with a single DPaaS provider. Also, managed service and cloud service providers store all of an organization's data, which could raise security concerns. Vendors should be able to encrypt data in transit and at rest as part of their DPaaS services.



DPaaS services come in many forms

Data protection as a service provides a plethora of cloud-based services to create, process, secure, manage, store, back up and recover data.

Data loss prevention services
Data deduplication services
Data security services
Access control services
Data archiving services
Data privacy services
Disaster recovery services
Data storage and backup
Data protection and business requirements

ILLUSTRATION: INUENG/GETTY IMAGES

©2024 TECHTARGET. ALL RIGHTS RESERVED TechTarget

In addition to technologies specific to data protection, dozens of new tools and techniques have emerged to help companies digitally transform, safely migrate their data, applications and workloads to the cloud, and better protect and govern their data. New architectures, concepts and frameworks have gained momentum, such as

DataOps, data mesh, lakehouse and zero trust, to cope with the increasing amount and sophistication of cybersecurity threats, ensure the secure flow of e-commerce customer data transmitted over multiple channels and conform to regulatory compliance edicts.

Data protection vs. data backup

Data backup systems enable companies to make copies of critical files, applications, databases and system configurations and store them in different locations. The data can then be recovered and restored to its most recent state if it's corrupted or lost because of human error, system failures, cyberattacks or natural disasters, thereby minimizing downtime. Data backup is a critical component of many organizations' business continuity and disaster recovery programs.

Data protection and backup are getting a closer look as the makeup of networks changes. Legacy backup systems used physical media such as tapes and disks, but today companies are increasingly adopting SaaS-based backup as a service. "Not everybody can back up to the cloud, but the vast majority of companies can, and the cloud offers significant recovery options from a disaster recovery standpoint," said W. Curtis Preston, technology evangelist at consultancy Sullivan|Strickler and host of the Backup Wrap-up podcast.

Adding complexity to the task of data protection is the development of generative AI, large language models and chatbot interfaces capable of creating manufactured content. These rapidly developing technologies have democratized the use of artificial intelligence and the data it digests, processes and produces. But generative AI has spawned a litany of legitimate data protection-related concerns, including data quality, content accuracy, data privacy, plagiarism, copyright infringement, bias and hallucinations, that are altering business data protection policies and procedures.

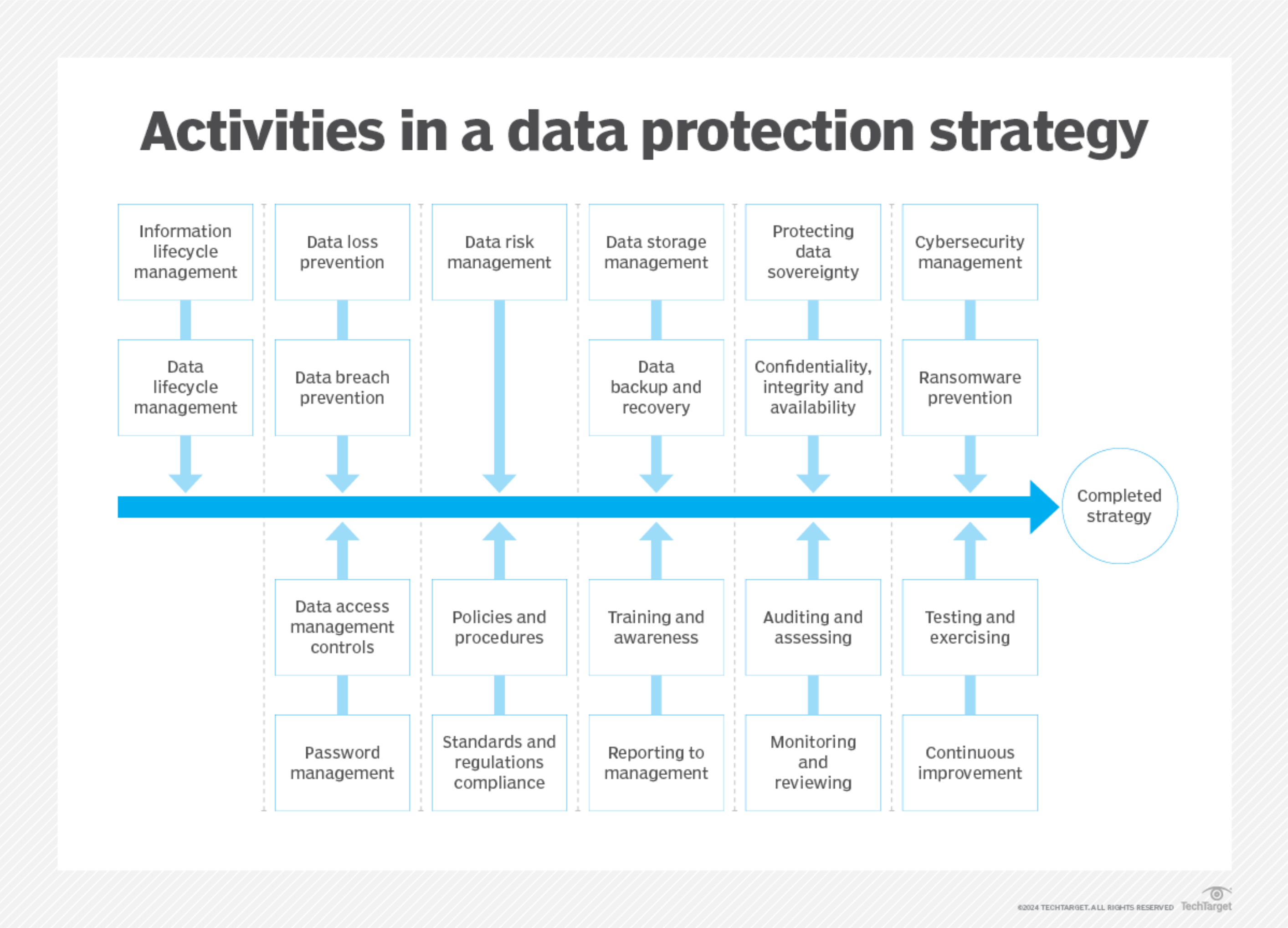
CONVERGENCE OF DATA BACKUP AND DISASTER RECOVERY

Two other aspects of data protection sometimes seen as one and the same are *data backup* and *disaster recovery*. Backup is the process of making copies of data and files, while disaster recovery (DR) entails the planning and process for using those copies so enterprises can quickly reestablish access to applications, data and IT resources and maintain business continuity after a network outage, shutdown, natural disaster or cyberattack.

Businesses can have a data backup process in place without a DR plan, but a DR plan must include data backup to recover data, in addition to an up-to-date communication strategy, a prepared staff and monitoring capabilities. Many cloud-based platforms converge backup and recovery as well as several other data

In this guide:

protection capabilities under one roof, in accordance with industry compliance regulations.

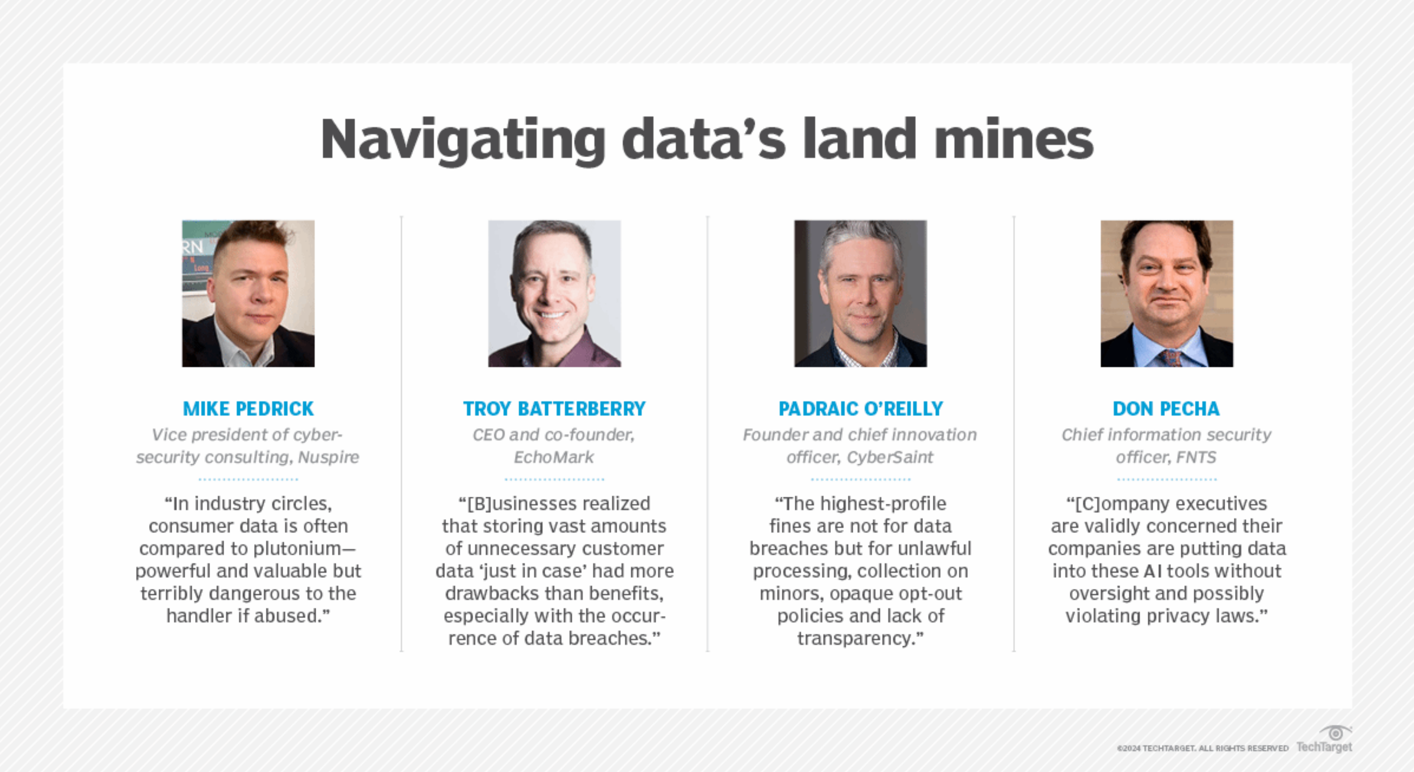


MOBILE DATA PROTECTION

Passwords, account numbers, emails, text messages, photos and videos are among the sensitive personal data that individual and corporate cell phones, laptops and other mobile devices can harbor.

Storage technologies affected by mobile data protection (MDP), according to Gartner, include magnetic hard-disk drives, solid-state drives, self-encrypting drives, flash drives and optical media. MDP products can delegate all or part of the encryption process typically done by hardware elements to native capabilities in the OS. There are also protection capabilities for network storage, some of which support cloud-based storage environments as an extension to the desktop.

Most mobile devices provide the necessary tools and features to ensure mobile security. When assessing the potential mobile device risks to companies of lost or stolen data, businesses and IT professionals should consider three elements of an MDP management policy: device management, OS updates and malware. IT should also determine what device features and capabilities are essential from both the organization's and end user's perspective.



Navigating data's land mines

MIKE PEDRICK
Vice president of cyber-security consulting, Nuspire

"In industry circles, consumer data is often compared to plutonium—powerful and valuable but terribly dangerous to the handler if abused."

TROY BATTERBERRY
CEO and co-founder, EchoMark

"[B]usinesses realized that storing vast amounts of unnecessary customer data 'just in case' had more drawbacks than benefits, especially with the occurrence of data breaches."

PADRAIC O'REILLY
Founder and chief innovation officer, CyberSaint

"The highest-profile fines are not for data breaches but for unlawful processing, collection on minors, opaque opt-out policies and lack of transparency."

DON PECHA
Chief information security officer, FNTS

"[C]ompany executives are validly concerned their companies are putting data into these AI tools without oversight and possibly violating privacy laws."

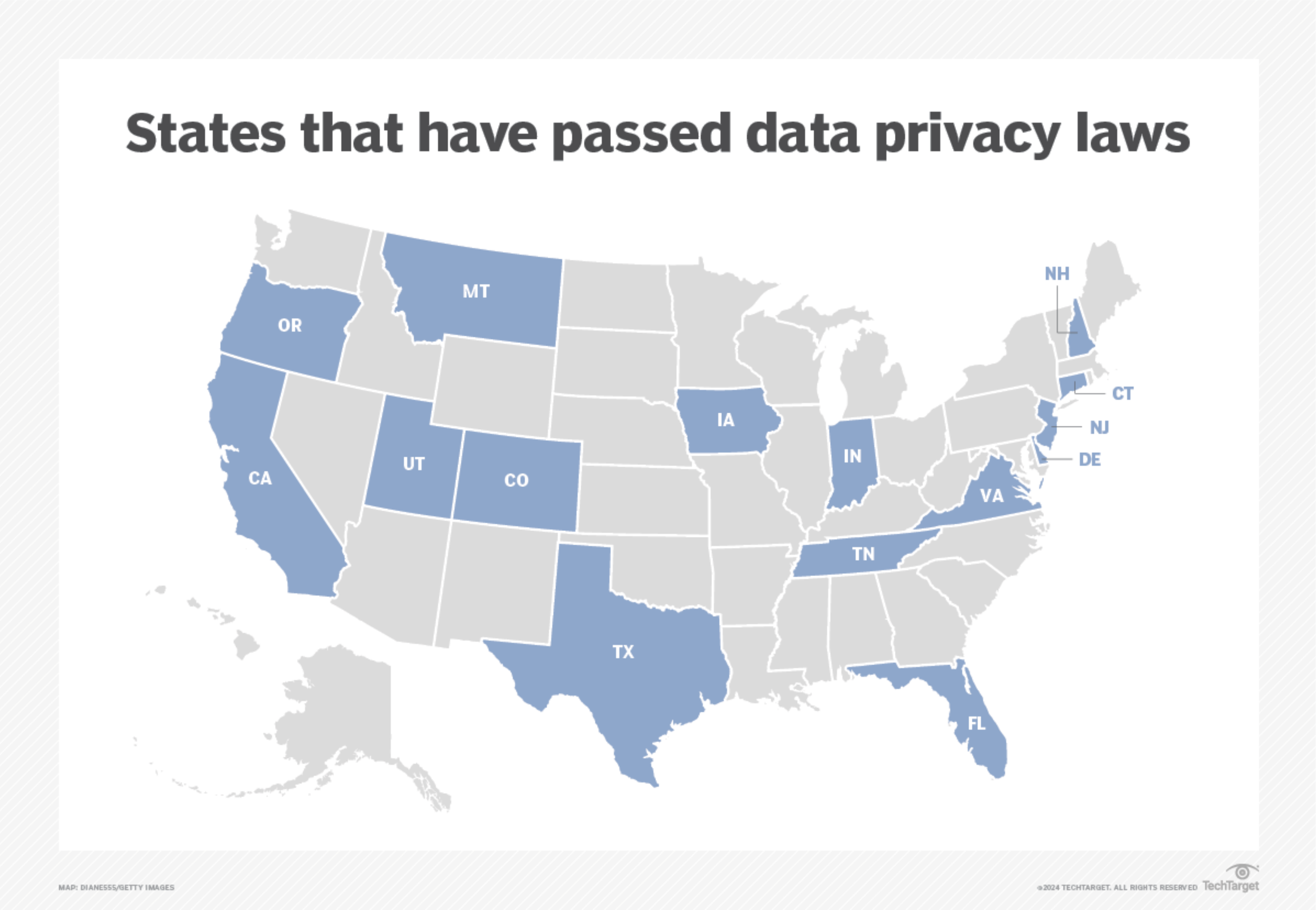
DATA PROTECTION AND PRIVACY REGULATIONS

Data protection and privacy regulations such as the GDPR and state laws like the California Consumer Privacy Act (CCPA) have forced businesses to change the way they collect, process, store and eventually erase their data. The right of individuals to have some degree of control over their personal data collected by businesses, including the right to be forgotten, goes to the heart of many of these regulations.

Businesses that operate in a market governed by data protection and privacy regulations are subject to serious fines and reputational harm for noncompliance. On the flip side, compliance might well serve as a badge of honor that companies can display to consumers and investors.

But while the EU and several countries have their own versions of data protection and privacy laws, the U.S. does not. Instead, state laws have been dotting the U.S. landscape in recent years following in the shadow of California's groundbreaking privacy law enacted in 2018.

In addition to California, 14 other states have enacted data privacy legislation, including Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah and Virginia. Major U.S cities, including New York, Chicago, Los Angeles, San Francisco and Washington, D.C., have enacted local laws addressing personal data privacy and might also actively enforce state data protection legislation.



States that have passed data privacy laws

MAP: DIANE555/GETTY IMAGES

©2024 TECHTARGET. ALL RIGHTS RESERVED TechTarget

To provide some continuity nationally and perhaps bring greater clarity to businesses wrestling with ways to comply with various state-specific data protection laws, Congress has put forth a long-awaited bipartisan bill called the American Privacy Rights Act of 2024 to "establish national consumer data privacy rights and set standards for data security."

Internationally, Australia, Brazil, Canada, China, England, France and Japan are among the countries that have been enforcing their own versions of data protection and privacy laws -- some long before the GDPR -- to guide businesses on collecting, storing, using and disclosing the personal information of individuals. India joined the list last year by enacting its version of the GDPR, called the Digital Personal Data Protection Act, 2023.

WHAT ARE THE KEY PRINCIPLES OF DATA PROTECTION?

Safeguarding sensitive data and ensuring availability under all circumstances is the fundamental principle of data protection. The GDPR, considered the gold standard of data protection laws, lays out seven principles for processing personal data. Outlined in Article 5 of the law, the principles pertain to companies conducting business in the EU, but the data protection challenges these principles address are ubiquitous. Here's how the GDPR's seven principles are described in the law.

1. LAWFULNESS, FAIRNESS AND TRANSPARENCY

"Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject [individual person]."

2. PURPOSE LIMITATION

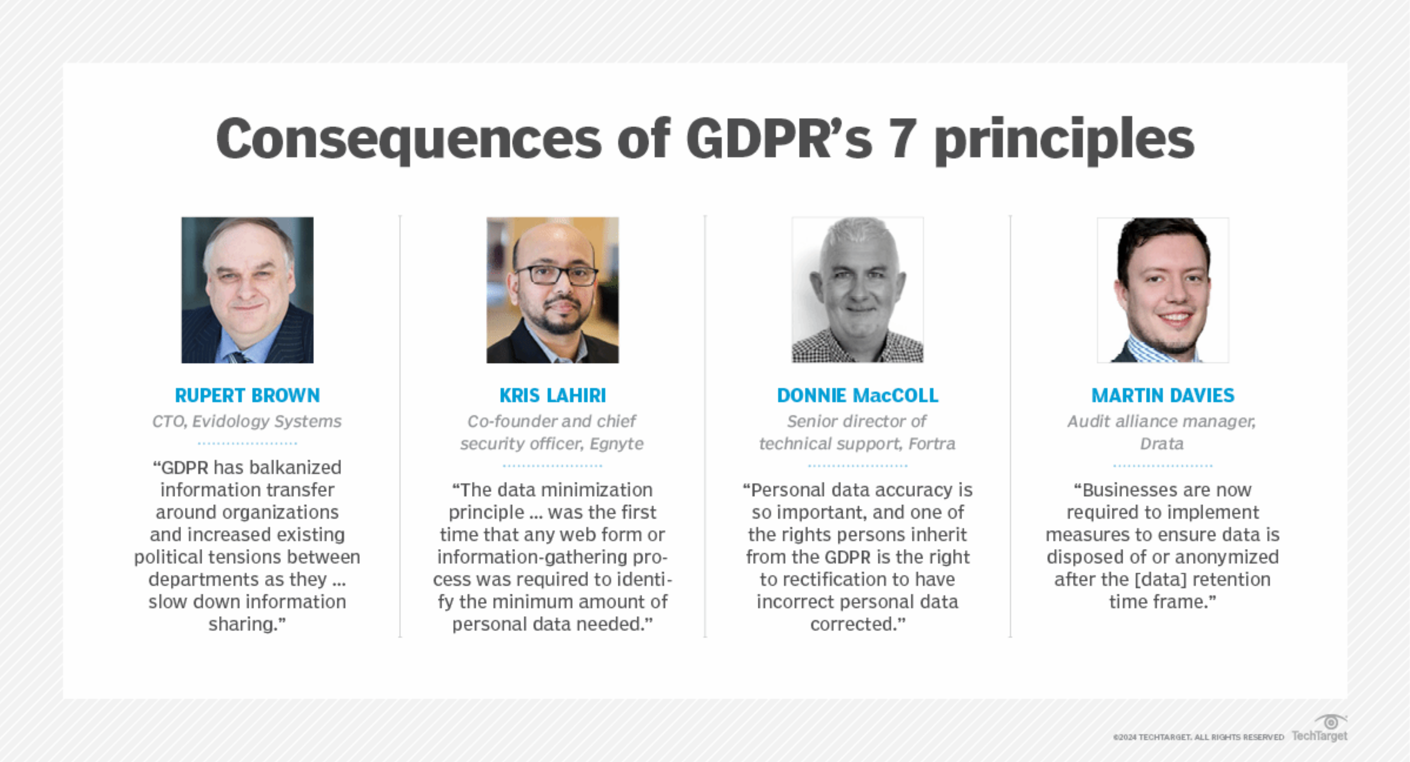
"Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes."

3. DATA MINIMIZATION

"Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."

4. ACCURACY

"Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay."



Consequences of GDPR's 7 principles

RUPERT BROWN
CTO, Evidology Systems

"GDPR has balkanized information transfer around organizations and increased existing political tensions between departments as they ... slow down information sharing."

KRIS LAHIRI
Co-founder and chief security officer, Egnyte

"The data minimization principle ... was the first time that any web form or information-gathering process was required to identify the minimum amount of personal data needed."

DONNIE MacCOLL
Senior director of technical support, Fortra

"Personal data accuracy is so important, and one of the rights persons inherit from the GDPR is the right to rectification to have incorrect personal data corrected."

MARTIN DAVIES
Audit alliance manager, Drata

"Businesses are now required to implement measures to ensure data is disposed of or anonymized after the [data] retention time frame."

5. STORAGE LIMITATION

"Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject."

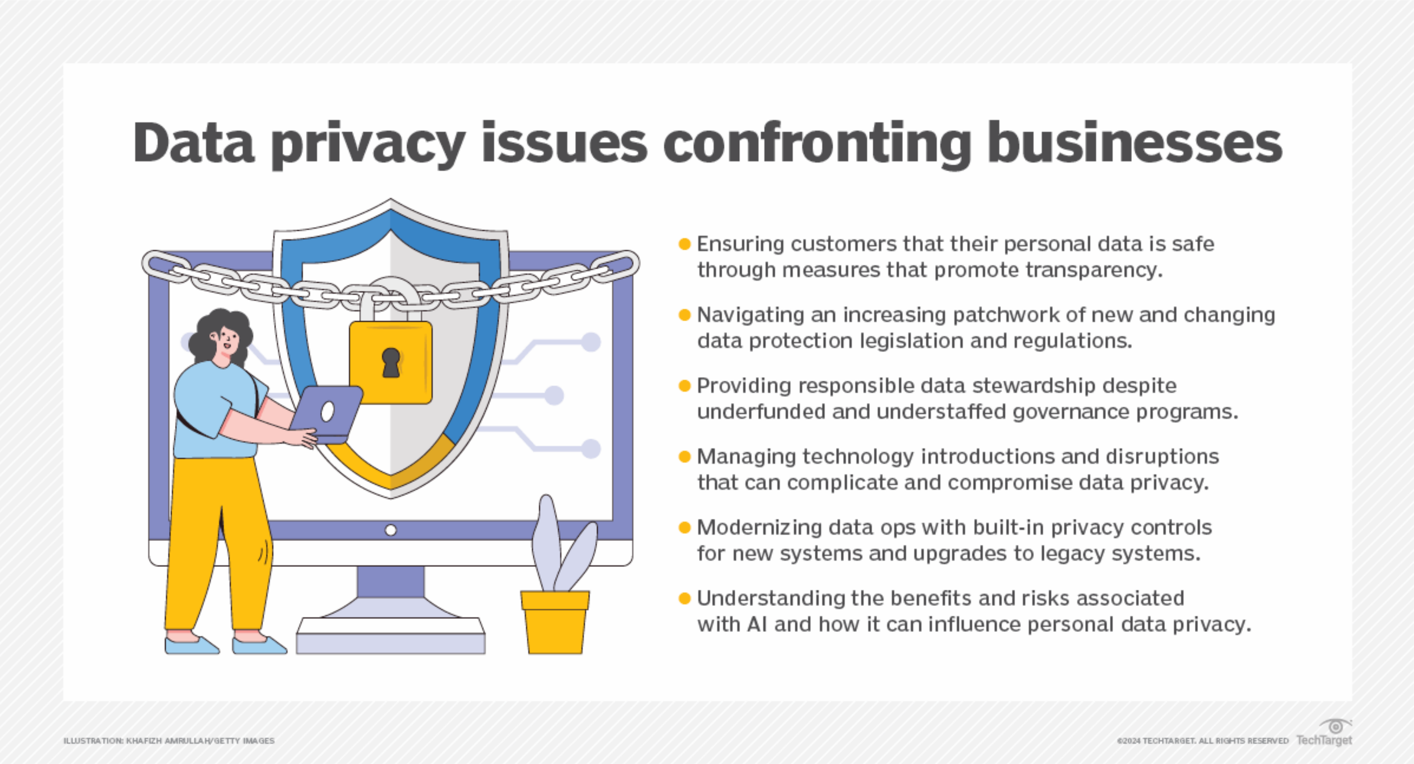
6. INTEGRITY AND CONFIDENTIALITY

"Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures."

7. ACCOUNTABILITY

"The controller [corporate officer in charge of data protection practices] shall be responsible for, and be able to demonstrate compliance with, [the first six principles]."

In this guide:



Data privacy issues confronting businesses

- Ensuring customers that their personal data is safe through measures that promote transparency.
- Navigating an increasing patchwork of new and changing data protection legislation and regulations.
- Providing responsible data stewardship despite underfunded and understaffed governance programs.
- Managing technology introductions and disruptions that can complicate and compromise data privacy.
- Modernizing data ops with built-in privacy controls for new systems and upgrades to legacy systems.
- Understanding the benefits and risks associated with AI and how it can influence personal data privacy.

ILLUSTRATION: KHAFIZH AMRULLAH/GETTY IMAGES

HOW GDPR COMPLIANCE IMPROVES DATA PROTECTION

For enterprises conducting business within EU countries, adhering to the GDPR is not only about appeasing regulators and avoiding severe penalties. The GDPR's principles and objectives force companies to institute internal policies and procedures that can improve data protection efforts in several key areas: business continuity, data governance and stewardship, data backup and recovery, cloud migration, transparency and discoverability, and data monetization. These areas are critical to data protection for the following reasons:

- Enhanced business continuity increases the chances that organizations can recover critical systems and restore operations quickly after a data breach.
- A clear data governance strategy as well as discoverability and transparency capabilities expedites locating, processing, protecting and securing data and makes the process more scalable to maximize and monetize data resources.
- Businesses complying with the GDPR demonstrate to regulators, customers and partners that they take data protection seriously and are responsible stewards of personal data, potentially increasing the trustworthiness of the brand and providing an edge over competitors.

GDPR COMES UP SHORT ON AI GUIDANCE

Initially, the GDPR's nonspecificity and lack of a centralized enforcement agency raised questions early on whether its regulations would have the teeth to be enforceable. Any doubts were put to rest when the GDPR levied numerous fines against major global entities:

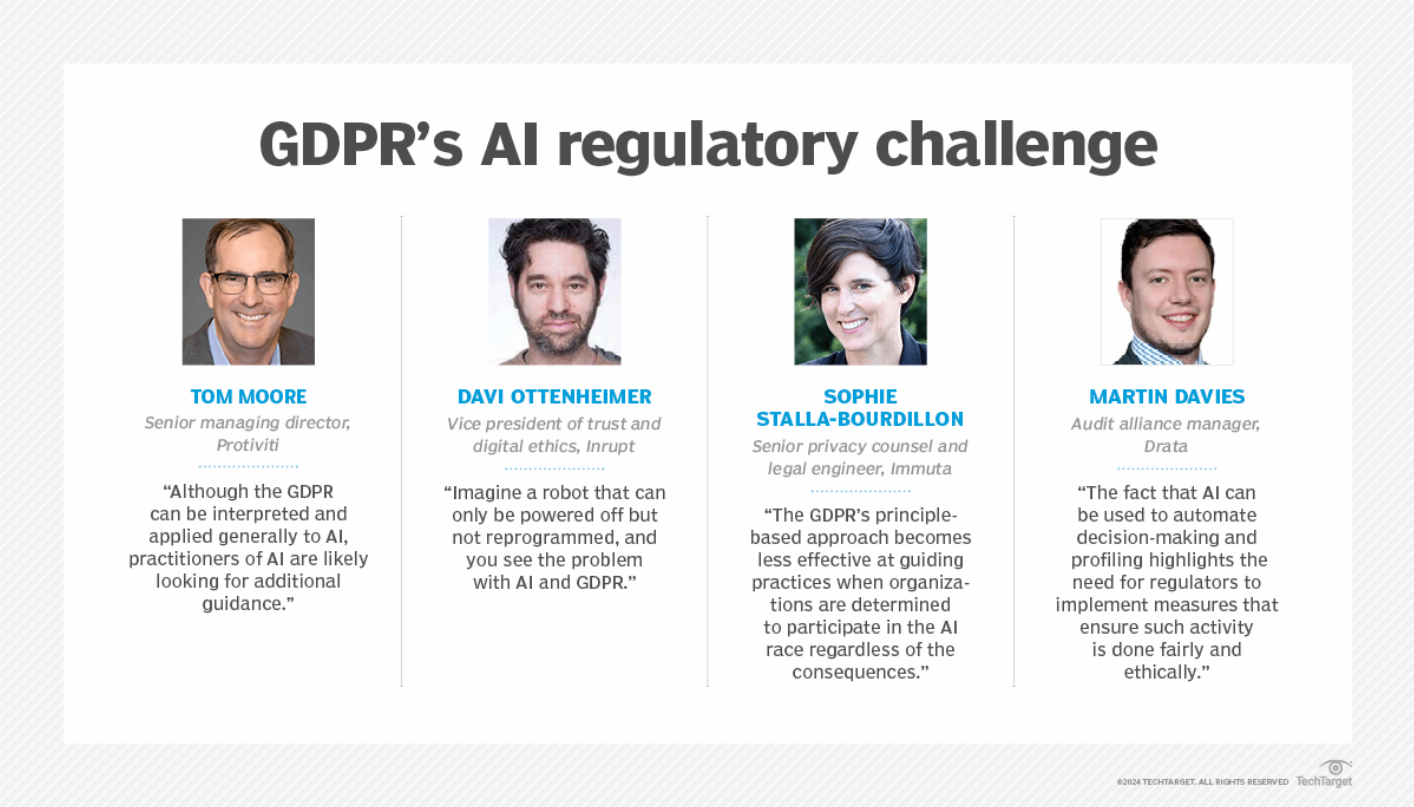
- Meta was fined a record-setting $1.3 billion in 2023 for transferring PII across borders without adequate data protections.
- Amazon was fined in 2021 for using targeted advertising without consumers' consent.

- TikTok was fined in 2023 for violating the GDPR's data processing and transparency requirements.
- Google was fined multiple times between 2019 and 2022, primarily for lacking sufficient consent and transparency in ad-personalization products.

However, the issue of the GDPR's nonspecificity has reemerged as companies face the prospect of stiff penalties without specific guidance on the use of AI, machine learning and generative AI in the collection, processing, storing and distribution of personal data.

"The GDPR's principle-based approach becomes less effective at guiding practices when organizations are determined to participate in the AI race regardless of the consequences," said Sophie Stalla-Bourdillon, senior privacy counsel and legal engineer at data security platform provider Immuta. "Imagine a robot that can only be powered off but not reprogrammed, and you see the problem with AI and GDPR," added Davi Ottenheimer, vice president of trust and digital ethics at data infrastructure software provider Inrupt.

In this guide:



GDPR's AI regulatory challenge

TOM MOORE
Senior managing director, Protiviti

"Although the GDPR can be interpreted and applied generally to AI, practitioners of AI are likely looking for additional guidance."

DAVI OTTENHEIMER
Vice president of trust and digital ethics, Inrupt

"Imagine a robot that can only be powered off but not reprogrammed, and you see the problem with AI and GDPR."

SOPHIE STALLA-BOURDILLON
Senior privacy counsel and legal engineer, Immuta

"The GDPR's principle-based approach becomes less effective at guiding practices when organizations are determined to participate in the AI race regardless of the consequences."

MARTIN DAVIES
Audit alliance manager, Drata

"The fact that AI can be used to automate decision-making and profiling highlights the need for regulators to implement measures that ensure such activity is done fairly and ethically."

The GDPR, according to Tom Moore, senior managing director at consultancy Protiviti, doesn't directly address the issue of algorithmic bias that could be present in the training data; doesn't fully capture the complexity of AI supply chains and who's responsible when harm occurs and multiple parties are involved; doesn't directly address broader societal concerns and ethical questions related to AI beyond data protection; and doesn't cover industry-specific risks and challenges.

The EU's Artificial Intelligence Act, a recently enacted "regulatory framework for AI," attempts to provide greater clarity relating to AI practices, high-risk AI systems and other AI systems, as well as concepts such as general-purpose AI systems and models. "Until and even after the authorities provide implementation details," Moore conjectured, "industry practitioners will want to work with their advisors to help assess the law's implications."

DATA PROTECTION STRATEGY BEST PRACTICES

Businesses encounter numerous data protection challenges that require a set of best practices to uphold the fundamental principles of and reduce the risks associated with collecting, processing, storing, monetizing and erasing data.

CONSUMER TRUST

Mistrust is rooted in a lack of transparency. Consumers are largely unaware of how their data is being managed and shared and left wondering if their data is safe. Businesses must build trust among consumers by ensuring data privacy consent agreements are in plain language and a consumable length, giving consumers a complete 360-degree view of their information and offering consumers an easy opt-out option for their data being used.

LAW AND REGULATION FRAGMENTATION

Businesses must navigate proliferating data protection legislation and regulations. Companies should plan and allocate sufficient resources to ensure impacted stakeholders are up to speed with regulatory requirements and align consumer consent terms with data protection regulations.

Know these data protection terms

What is continuous data protection (CDP)?

What is data minimization?

What is data processing?

What is the Data Protection Act 2018 (DPA 2018)?

What is data protection management (DPM)?

What is electronic data processing?

What is erasure coding?

What is privacy impact assessment (DPIA)?

What is storage snapshot?

In this guide:

DATA GOVERNANCE

Businesses are responsible for stewarding data privacy, compliance and oversight. Governance should be at the forefront of any new data initiative. Establish a framework based on policies and standards governing personal data privacy across the enterprise. Understand the organization's data and how it's used, establish a data privacy council and foster collaboration.

TECHNOLOGY DISRUPTION

Technology is a double-edged sword in data protection practices. It enables businesses to better protect personal data and cybercriminals to attack and compromise data. It also introduces risk. Businesses need to assess new technologies, their potential risks and how to mitigate those risks. Place data privacy at the forefront of new technology decisions, establish data privacy literacy and collaboration across the enterprise, and resist financial pressures to implement new technologies without due diligence.

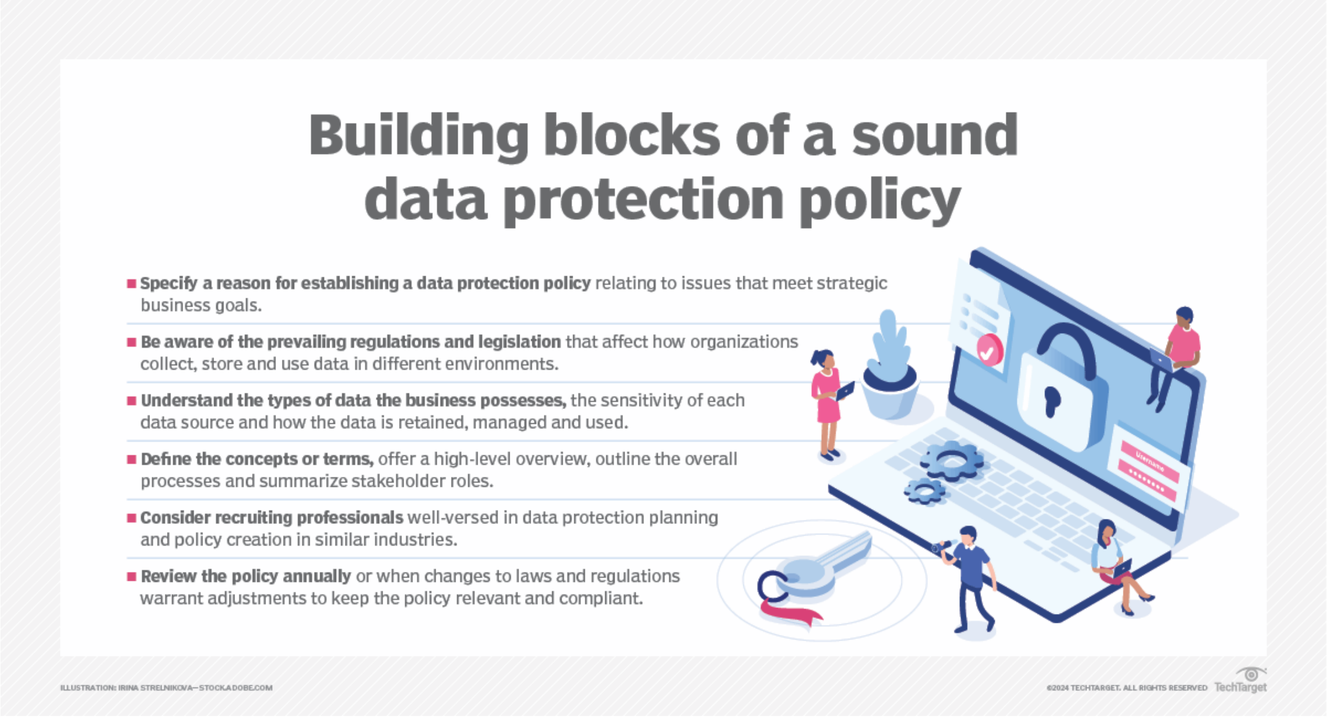
DATA OPERATIONS

To cope with the massive amounts of personal data flowing into corporate coffers, businesses need to operationalize privacy controls in modern systems and retrofit older systems. Only collect, retain and share data as needed to run the business, design systems with data privacy in mind and implement policy-based intelligent automation.

In this guide:

AI ADOPTION

AI has permeated virtually every aspect of business operations, producing smoother processes and greater productivity. Yet the safety layers or guardrails for AI are often inadequate and sometimes [compromised by bias and inaccuracies]. The introduction of generative AI compounds the risk. Businesses need to understand associated AI risks and proceed with caution. Carefully plan the shift of data privacy management from humans to machines, continuously assess and test algorithmic bias, starting with data acquisition through delivery, and align AI values to business values.



Building blocks of a sound data protection policy

- **Specify a reason for establishing a data protection policy** relating to issues that meet strategic business goals.
- **Be aware of the prevailing regulations and legislation** that affect how organizations collect, store and use data in different environments.
- **Understand the types of data the business possesses,** the sensitivity of each data source and how the data is retained, managed and used.
- **Define the concepts or terms,** offer a high-level overview, outline the overall processes and summarize stakeholder roles.
- **Consider recruiting professionals** well-versed in data protection planning and policy creation in similar industries.
- **Review the policy annually** or when changes to laws and regulations warrant adjustments to keep the policy relevant and compliant.

ILLUSTRATION: IRINA STRELNIKOVA—STOCK.ADOBE.COM

BUILDING A DATA PROTECTION POLICY

To safeguard their sensitive information, comply with an array of regional laws and avoid stiff penalties, companies by necessity establish and implement internal data protection policies that coincide with business goals and data privacy regulations. But the steps for building a data protection policy can be as varied as the data collected and the privacy laws companies must accommodate.

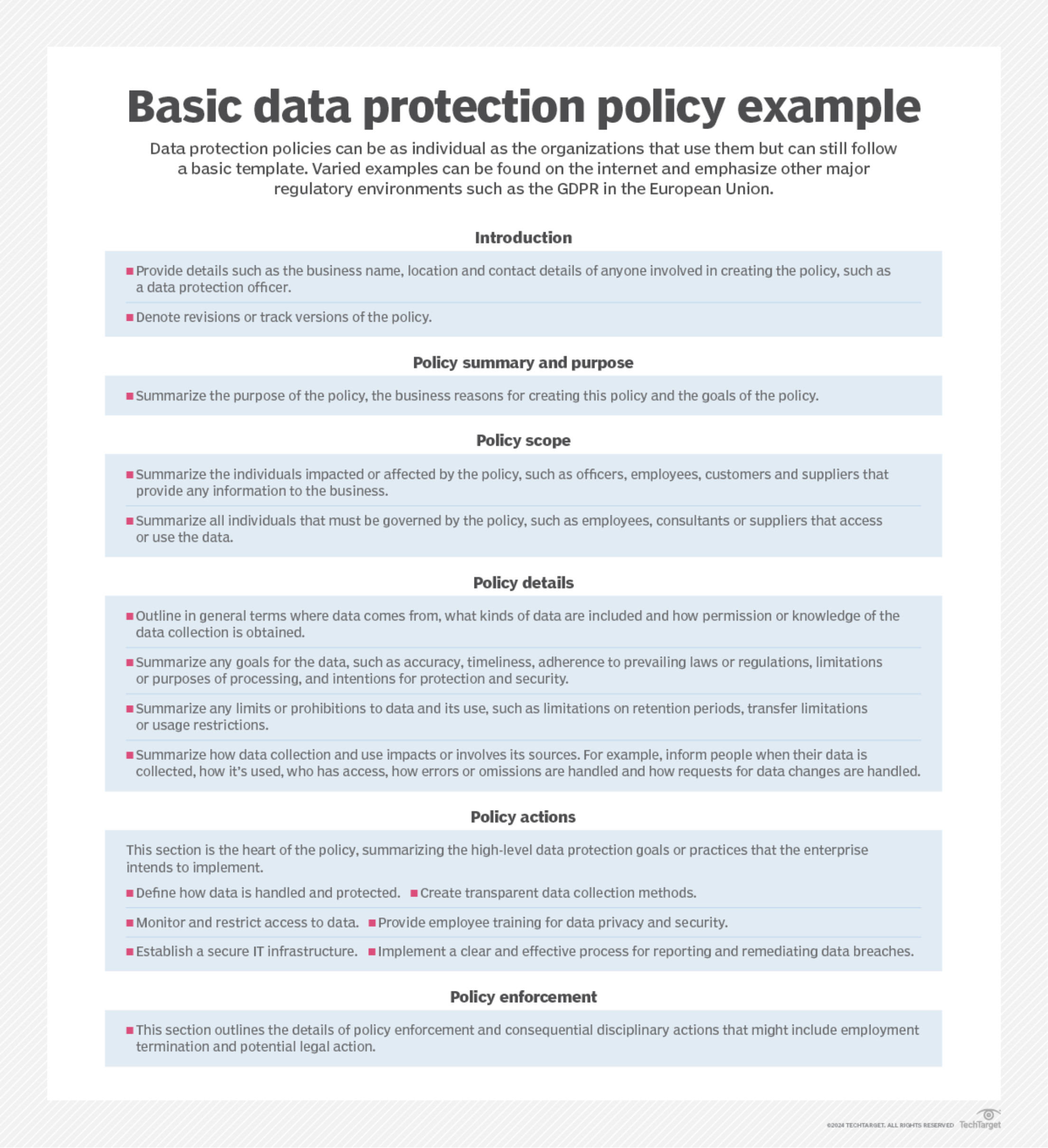
Before building a data protection policy, it's important to conduct a data privacy audit, a comprehensive review process to assess the organization's handling of personal information. The audit requires careful scrutiny of the data collected, the means of processing the data and the security measures in place to protect it. Its scope typically encompasses policies, procedures and practices that ensure compliance with applicable laws and regulations, such as the forecited GDPR and CCPA.

One of the best and most efficient ways to further assess the security and protection of a company's critical data is to conduct a data protection impact assessment (DPIA). A DPIA helps ensure that the data is accessible, its integrity is protected from attacks and its availability is assured.

Data protection policies have no set structure and no specific template. That could be a blessing for businesses because every organization is different and adheres to its own specific goals. Still, companies operating in the same region are governed by the same regulations and fundamental obligations to protect a customer's personal information. The following components are essential in building a data protection policy that satisfies regulatory compliance requirements and meets business goals:

- Specify a reason for establishing a data protection policy relating to issues that meet strategic business goals.
- Be aware of the prevailing regulations and legislation that affect how organizations collect, store and use data in different environments.
- Understand the types of data the business possesses, the sensitivity of each data source and how the data is retained, managed and used.
- Define the concepts or terms, offer a high-level overview, outline the overall processes and summarize stakeholder roles.
- Consider recruiting professionals well-versed in data protection planning and policy creation in similar industries.
- Review the policy annually or when changes to laws and regulations warrant adjustments to keep the policy relevant and compliant.

In this guide:



Basic data protection policy example

Data protection policies can be as individual as the organizations that use them but can still follow a basic template. Varied examples can be found on the internet and emphasize other major regulatory environments such as the GDPR in the European Union.

Introduction

- Provide details such as the business name, location and contact details of anyone involved in creating the policy, such as a data protection officer.
- Denote revisions or track versions of the policy.

Policy summary and purpose

- Summarize the purpose of the policy, the business reasons for creating this policy and the goals of the policy.

Policy scope

- Summarize the individuals impacted or affected by the policy, such as officers, employees, customers and suppliers that provide any information to the business.
- Summarize all individuals that must be governed by the policy, such as employees, consultants or suppliers that access or use the data.

Policy details

- Outline in general terms where data comes from, what kinds of data are included and how permission or knowledge of the data collection is obtained.
- Summarize any goals for the data, such as accuracy, timeliness, adherence to prevailing laws or regulations, limitations or purposes of processing, and intentions for protection and security.
- Summarize any limits or prohibitions to data and its use, such as limitations on retention periods, transfer limitations or usage restrictions.
- Summarize how data collection and use impacts or involves its sources. For example, inform people when their data is collected, how it's used, who has access, how errors or omissions are handled and how requests for data changes are handled.

Policy actions

This section is the heart of the policy, summarizing the high-level data protection goals or practices that the enterprise intends to implement.

- Define how data is handled and protected.
- Create transparent data collection methods.
- Monitor and restrict access to data.
- Provide employee training for data privacy and security.
- Establish a secure IT infrastructure.
- Implement a clear and effective process for reporting and remediating data breaches.

Policy enforcement

- This section outlines the details of policy enforcement and consequential disciplinary actions that might include employment termination and potential legal action.

DATA PROTECTION TRENDS AND EXPECTATIONS

Businesses, consumers and regulators are continuously adjusting to the complex, ever-changing data protection and privacy environment. Expect several of the following trends to affect the way businesses collect, process, govern, secure and distribute personal and sensitive information:

- AI and its double-edged sword will dominate the landscape in providing enterprises with new and improved methods to safeguard data, while empowering cybercriminals to steal and compromise proprietary information.
- Businesses will continue to play catch-up with almost daily advancements in generative AI's capabilities.
- The cost of data privacy protection will increase amid expanding business investments in tools and techniques as well as legal and technical expertise.
- As data protection and privacy laws proliferate nationally and regionally, businesses will seek greater regulatory clarity and guidance, especially concerning the implications of AI.
- Just as the GDPR has affected the way businesses and consumers view personal data, its provisions could influence the development and deployment of AI in several ways.
- Tech-savvy consumers supported by more abundant and stricter data protection and privacy regulations will seek greater control over their personal information.
- Congress' discussion draft of a long-awaited bipartisan U.S. national data protection bill, if passed, might overshadow state protection laws, creating more

confusion or providing more cohesiveness in protecting the data privacy rights of consumers.

- Society's view of data ownership and control is continuing to evolve and "privacy by default" could become the norm.
- Businesses will heighten their focus on digital safety and ethics and build a culture around data values.
- The sale of personal data, whether volunteered or stolen, is big business and will lead to an economy unto itself on the back of personal data.

Ron Karjian is an industry editor and writer at TechTarget covering business analytics, artificial intelligence, data management, security and enterprise applications.

Stephen J. Bigelow, Paul Crocetti, Stacey Peterson and Kim Hefner contributed to this article.

CONTINUED READING

- **AI and GDPR: How is AI being regulated?**
- **How to conduct a data privacy audit, step by step**
- **Best data protection software platforms of today**