Fuller, L. R., Gauntlett, D., Oehlers, P. F., & Frankel, M. (2026). The Effect of Data and Privacy Rights on Small Business. *Small Business Institute Journal*, *22*(1), 1–6.
https://doi.org/10.53703/001c.159537

Articles

The Effect of Data and Privacy Rights on Small Business

Lori R. Fuller, PhD, BS[1], Daniel Gauntlett, MBA, BS[1], Peter F. Oehlers, DBA, MBA, BS[1], Matt Frankel, DPA, MBA, BS[1]

[1] Accounting, West Chester University

Keywords: data privacy, data security, risk management, privacy regulation

https://doi.org/10.53703/001c.159537

Small Business Institute Journal

Vol. 22, Issue 1, 2026

Data privacy and data security are areas in risk management that small businesses must plan for in the ever-increasing technologically driven business environment. This paper explores the existing landscape of data privacy concerns, identity theft issues facing businesses, and changing data privacy legislation. Furthermore, recommendations and solutions related to a data privacy audit are discussed to ensure businesses are prepared to comply with legislation and mitigate risk.

Introduction

A business's ability to provide adequate security over customer data and manage the rights over that data has become increasingly important in recent years. This becomes especially impactful to companies doing business with European entities due to the General Data Protection Regulation (GDPR) which became law in 2018 and significantly increased the number of protections afforded to user data. In addition, attempts to manipulate social media along with hacking attempts into government, corporate, and individual systems are happening with greater regularity. Thus, the majority of data included in business and informational transactions are in danger of being stolen, bought, and sold.

Data privacy has become a critical issue as all online transactions involve data transfer and storage. Companies request and collect information on their customers and potential customers on visits to websites, purchases, and information requests. Accentuated by business breaches, customer confidence in the ability for organizations to protect their information is potentially irreparable when breaches occur (Gable, 2014). Another problem is the cost of data breach to the small business. An astonishing 60% of small businesses close their doors within six months of a data breach (Trak, 2019). Because of these concerns, entities turn to auditors to provide assurance that their information is being protected.

Data are one of the most valuable assets an organization has and maintaining, managing, and protecting it is becoming a larger challenge. CPA firms go through a variety of procedures to check for existence of assets and that policies and procedures are being followed in addition to examining the access and basic security of the computer system. For smaller businesses, an inquiry to senior management regarding the risks to the business is often the primary method of analyzing data risks.

Although the inquiries do get a basic overview of policies, smaller firms do not have the staff or capabilities to examine data privacy for customers and other stakeholders who have their information with the CPA client. Having a specific audit program, defined as a series of procedures for auditors to follow, will help ensure organizations reduce their risk of data breach. These policies and procedures need to be grounded in Generally Accepted Auditing Standards (GAAS, 2025) and the AICPA Interpretations and then will be extrapolated to the specifics of data privacy rights. As the audit program is developed, CPA firms will be able to perform specific tests to verify that internal controls, policies and procedures are in place to ensure that data privacy rights are being protected.

Creating organizational norms or best practices is critical in managing data privacy and the greatest concern is that the best practice is not enforced (Sloan & Warner, 2015). In addition, due to the rise of big data, data that is so voluminous that only until recently does technology exist to analyze it, will make privacy rights even more critical as regulators such as the Federal Trade Commission focus on limiting data collection and data retention rather than creating standards to measure the effectiveness of the protection. As more organizations begin to use big data for data analytics and business intelligence, the ability is created to completely examine characteristics and events among many co-existing data points. The AICPA has released a Service Organization Controls (SOC) for cybersecurity (*2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022) (2017 TSC)*, 2023). As part of this framework, organization management documents its cybersecurity risk practices, asserts whether their practices were effective, and has their assertions audited and reported on by a CPA firm. Most organizations are not willing to spend money unless there is a greater benefit (usually monetary). Since organizations are not required to be proactive and are not willing to spend resources until negative events happen, there is a strong possibility that firms may take advantage of this cybersecurity review only after a major breach has occurred – when it is often too late. However, by providing a straightforward series of steps that focus specifically on data privacy, organizations will be able

to incorporate these rules into their audit and mitigate negative future consequences of ineffective data security practices.

Even if data are not reviewed for data privacy, organizations will want to analyze big data as businesses are looking for new opportunities to derive value and create competitive advantage from their data. Accounting uses big data in auditing clients, analyzing fraud, determining trends in sales, examining an organization's general ledger, and managing inventory. The growth of this interest is creating demand from many employers. One concern is the management and storage of data to maintain privacy of individuals after the use of data has ended. As organizations accumulate data from AI interactions, that data should be anonymized if it is used and rules should be established for storage and retention. Through the increased use and storage of data, businesses now have an increasing number of issues to manage including minimizing identity theft, protection privacy rights, and creating sufficient policies to ensure these protections are in place.

Identity Theft

Identity theft occurs when personally identifiable information is taken with the intent for use in fraud (Oehlers & Li, 2008). This occurs when information is shared over the internet or via wireless device. In 2022, the Federal Trade Commission reported that consumers lost nearly $8.8 billion to fraud, which was an increase of 30% from the previous year (FTC, 2023). Investment scams were the largest category, while imposter scams and online shopping scams were next. Over 2.4 million consumer-reported fraud, with a likely higher number since not all victims reported to the FTC (FTC, 2023).

Identity theft can be a big risk to customers and businesses alike. Customers often spend countless hours repairing their credit and monitoring their personal information. Businesses can suffer reputation losses and often additional costs for credit monitoring services for those customers affected by the breach as well as lost sales. These events often create additional expenditures in technology and system improvements related to strengthening the computer system to minimize future hacking threats.

Data Privacy

Our interconnected world provides businesses with significant opportunities as well as significant challenges. The European Union (EU) has new data protection rules that provide greater protection for customer and employee data than in the past and have become the premier standards globally. Twenty of the United States have signed Privacy Legislation laws that have been enacted (Kibby, 2025) (California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia).

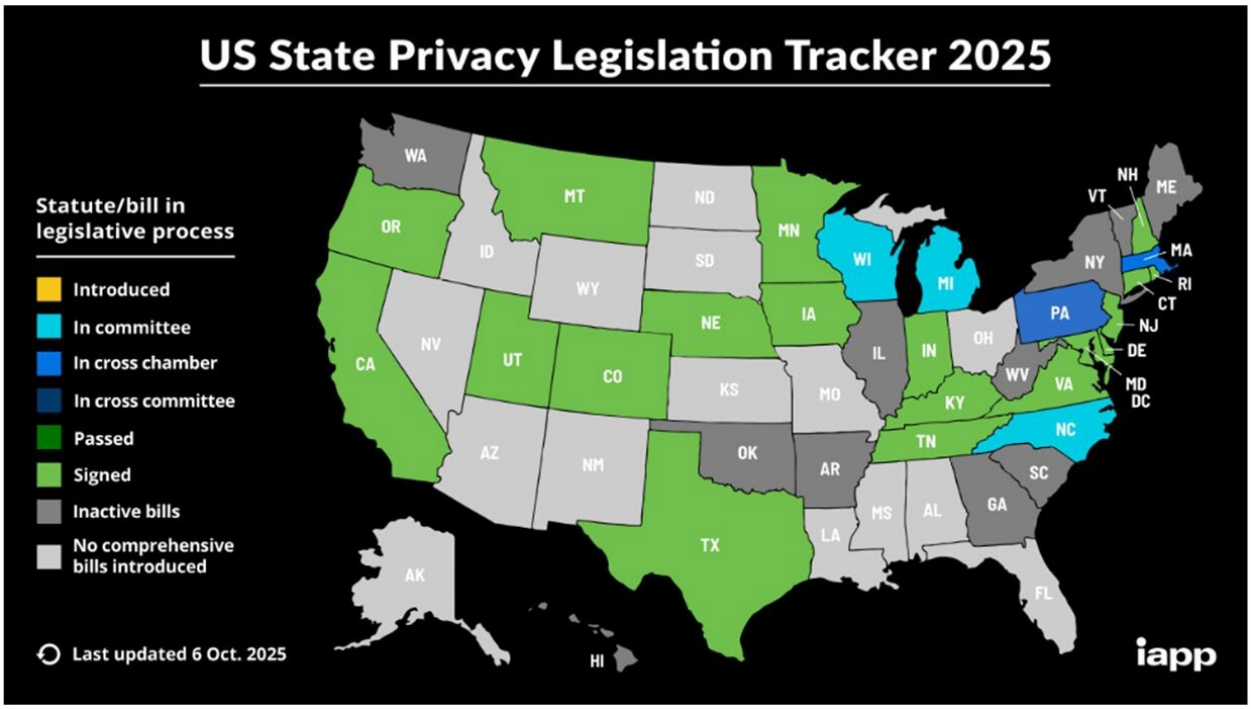
As more states adopt laws with a variety of specific requirements, organizations of all sizes will have to manage a general data policy that can cover a broad category of state rules, as well as the GDPR regulations if business is done with EU customers. Further, the policy must consider the specifics for each state that the organization performs significant business. With many states adopting individual rules, the federal government might take on the responsibility of creating standardized federal regulations to create an enforceable standard set of rules.

The European Commission reports that the EU accounts for approximately 14% of exports worldwide, with the US being the largest trading partner for exports in 2022 (*International Trade in Goods*, 2024). As US tariffs are implemented, EU imports and exports could change. The EU rules apply equally to all entities that transact with the EU – there are no exemptions for size. Entities that have operations in the EU are subject to these rules, including both companies that sell products in the EU and monitor EU site visitor's data (Lambert, 2018). Therefore, subject organizations have new data breach rules to follow and significant fines that can be levied by the EU as a result of noncompliance. A recent example of this is the 290 million euro fine levied against Uber in 2024 for improper storage of European Uber driver data on U.S. servers (*Dutch SA Imposes a Fine of 290 Million Euro on Uber Because of Transfers of Drivers' Data to the US*, 2024). No business is exempt based on size. Any businesses that interact with third party processes, cloud storage, and other outsourcing companies are subject to EU fines if improper data security policies are in place.

US-only based companies still must follow significant, but segmented rules that look at some aspects of personal data, health data, and financial data. US rules often take a historic look at data protection that enact after a hack or breach occurs. The consequences of this approach can be more expensive and, for smaller businesses, devastating. Although it comes with potential ethical issues, AI can be used to help small businesses to determine customer location, track amounts of customers in each state and other group dynamics that could be an issue (Catherine et al., 2025). With AI capabilities ever-changing, data privacy and security needs, rules, and impacts will require continuous consultation and examination and review of the ethical issues those changes create (Gupta et al., 2025). EU data protection rules suggest that all organizations (including small businesses) design controls into the system rather than reacting to events. By creating, monitoring and updating procedures to protect data, organizations have a better chance to mitigate risks from hacking and data breach. While it is important for each business to consider implementing each of these rules if you are under the individual state threshold, you may be exempt from following all the required rules but may consider adopting them as best practices. Check with your individual state laws on privacy to determine where those thresholds are.

US Privacy Legislation

Following the implementation of EU's GDPR legislation, several states have adopted privacy rights legislation. As of June 2022, eleven states have privacy laws in place where residents of those states have a basic right to know about



Map of U.S. State Privacy Legislation as of 10/06/2025 taken from iapp.org/resources/article/us-state-privacy-legislation-tracker/ on 10/13/2025

the consumer information collected about them, delete information collected, the ability to opt out of data collection, and consumer protection rights (*State Laws Related to Digital Privacy*, 2022). As of October 2025, three states, Wisconsin, Michigan, and North Carolina have legislation in committee related to individual privacy rights (Kibby, 2025).

In addition, organizations would be required to limit the collection of personal data. Because of the variety of state laws and a lack of federal legislation, small businesses must deal with multiple jurisdictions if they conduct commerce in more than their domiciled location. If the small business transacts internationally, they must also follow the GDPR regulation, as well as any country that has their own set of specific privacy regulations.

Small businesses may choose to follow the GDPR guidelines which have the highest standards in data privacy globally (at this time) and will effectively lay a foundation for implementation for all other state and country regulations. Some recommendations for creating a data privacy policy include:

1. Risk based approach – rules should be based less on organization size but rather tailored to fit the respective business risk
2. Standardized enforcement rules – how are rules enforced within and between the states?
3. Data collection should be transparent – what items are collected and what is the purpose of the data collected?
4. The right to know when your data has been hacked
5. A right to have one's name deleted from data files – e.g. a right to be forgotten
6. Easy access to one's own data

All accounting firms that audit must follow accounting and audit standards. The framework to review this technology and data privacy is Control Objectives for Information and related Technology or COBIT (2018). COBIT is a framework for governance and management of information technology. COBIT defines the components to build and sustain a governance system: processes, organizational structures, policies and procedures, information flows, cultures, and behaviors, as well as skills and infrastructure. As one of the important governance responsibilities, a discussion of risk and risk assessment should occur. The significance of not having a data privacy policy and not being aware of the patchwork of states that have laws and potential fines is not an available defense. Board of directors or senior executives with the organization (owners, senior managers) should have regular reviews of organization policy and review the policy with the auditors and audit committee.

To verify that a company is maintaining a COBIT compliant framework and to determine compliance with any relevant data privacy regulatory policies, businesses are encouraged to undergo regular Data Privacy audits. The audit is customized to center around organization-specific data security and IT objectives to aid in audit efficiency and to ensure that the audit is serving a functional purpose to proactively save the organization from future financial hardships (Whitener, 2012). As it takes 287 days on average to identify a data breach with the average time to contain a breach taking 80 days (NCDIT, 2022), consistent monitoring of the businesses data security framework is integral to mitigate risk.

What Should You Expect of Your Auditors?

When analyzing information systems auditors have a checklist of the tasks to perform – otherwise known as an audit program. The Data Privacy Audit should follow specific privacy audit criteria (standards). A privacy audit does not evaluate your financial statements. Upon completion of those tasks, an opinion of the business's data privacy policies and procedures will be issued.

Questions for Auditors

1. Are they familiar with and have they performed privacy audits?
2. Are they knowledgeable about IT?
3. Do they conduct a privacy impact assessment?
4. Do they have an "in-house" expert or access to an expert?
5. Are they familiar with the General Data Protection Regulation (GDPR)?
6. What risks do they consider?
7. Will they make recommendations to improve the current system and are they included in the audit?
8. Is our company required to have a data privacy policy?
9. How do my stakeholders (vendors, suppliers, customers, employees, government agencies) impact our privacy?
10. How do we find out if they are protecting their data?

After the Data Privacy Audit, other audits are available to make sure the system is secure. These audits include a penetration test, where the firm tries to penetrate the system's controls, and a general systems audit, which covers the entire system of software, hardware, data, policies, and controls. These audits will help prepare you for the rules enacted by the European Union.

What Steps Can Businesses Take?

Prevention

1. Secure personal data.
2. Assess the risk for damage of personal data loss to the organization and individuals. The organization needs to measure the likelihood of occurrence and severity of loss and/or damage to the individual.
3. Identify best practices to mitigate risk: professional organizations, trade groups, consultants, and peer organizations may have tools in place that can minimize "reinventing the wheel".
4. Proper use of encryption: data transmitted over the internet should be encrypted with browser encryption of at least 256-bit encryption. A lock icon appears when data is encrypted.
5. Identity and Access Management (IAM): IAM is comprised of four elements:
   i. A directory of the personal data the system uses to define individual users;
   ii. A set of tools for adding, modifying, or deleting that data;
   iii. A system that regulates user access; and
   iv. An auditing and reporting system.
   The purpose is to regulate user access. One of the primary functions of IAM is having the system use passwords to identify who is entering the system, but a strong password may not be sufficient so many organizations incorporate biometrics, and artificial intelligence as well as multi-factor authentication.
6. Regular updates for anti-virus and malware.
7. Measures to prevent unauthorized data access, alteration, disclosure, destruction, and processing.
8. Managing employee separation to mitigate the risk of internal fraud or dependency risks.
9. Train employees to protect against social engineering.

What should an organization do when a breach occurs?

1. Assess the extent and magnitude of the breach: determine what accounts have been affected and who needs to be informed.
2. Inform the appropriate corporate officer and any applicable regulatory authority, such as PrivacyRights.org
3. Communicate the breach to the affected individuals, members of IT, the impacted departments, and senior corporate officials.
4. Determine what can be done to not have a second similar breach.

Recommendations[1]

1. Regular privacy audits by either internal or external (CPA) parties
2. Penetration tests (by external parties)
3. Update software
4. Be aware you are the front line for your supply chain (Target & HVAC example)
5. Assume no one has good controls – everyone is at risk. Hackers are constantly trying to break defenses.
6. Remotely wipe laptop data/software if it is stolen
7. Train employees to protect customer data by not making it visible – including not displaying it on computer monitors or leaving data unattended on a workspace.
8. Train employees to be familiar with the EU's GDPR. Regular updates will be required.

1 The cost of compliance will always be an issue for a small business. Currently, estimating the costs of these audits are beyond the scope of this paper and would be difficult for the authors to provide meaningful amounts.

Online and other instruction on state-level privacy laws can be found by searching through resources like the National Conference of State Legislatures (NCSL), IAPP Privacy Legislation Tracker, and legal websites that provide overviews, guides, and alerts

9. Create and update a written privacy policy
10. Password-protect all workstations and laptops. Passwords should be changed regularly.
11. New rules and legislation for data privacy may come from congressional hearings and the FTC given recent events.
12. Report any data breaches to PrivacyRights.org
13. For participants in your supply chain, request SOC-1 and SOC-2 reports, which analyze the effectiveness of their controls and how it would impact your organization.

Looking into the future

As data privacy regulations are still emerging and being evaluated in the U.S. and globally, there are many changes that might soon be making their way into upcoming legislation. As the EU led internationally with its comprehensive GDPR regulations, future expectations of the EU and UK are the focus of regulation targeting the use of AI, increased data regulation of the financial services industry, and defined data subject rights.

From the U.S. standpoint, an increasing number of states are expected to pass their own data privacy laws in upcoming years joining the nineteen existing states with policies currently enacted. While still in its infancy, the need for a federal policy has been promoted with the historic American Privacy Rights Act being drafted and put up for discussion in the summer of 2024 (Energy and Commerce, 2024). Therefore, with change on the horizon, it is in every business's best interest to review its own data privacy and security policies, formally evaluate those policies via IT audits, and establish best practices which promote data integrity and security.

Along with staying informed on regulatory changes directly related to data privacy reform, small businesses should maintain awareness for future policies proposed regarding AI's role in data security. Future research should explore the increased, and possibly outsized, risks of AI and consumer data security as well as the need to update internal controls surrounding AI implementation. As the paradigm continues to shift towards AI usage in business, a new breed of controls must be designed to take advantage of all digital, mechanical, and management processes available to ensure that only authorized applications and employees can access data to ensure effective data privacy rights. Future legislation on AI will affect data rights and continue to change the landscape of data privacy.

Submitted: June 29, 2025 MDT. Accepted: December 17, 2025 MDT. Published: April 07, 2026 MDT.

References

2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022) (2017 TSC). (2023). AICPA. https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022

Anatomy of a Data Breach: What Are They and What to Do When You Spot One? (2022). North Carolina Department of Information Technology. https://it.nc.gov/blog/2022/10/11/anatomy-data-breach-what-are-they-and-what-do-when-you-spot-one

Catherine, S., Suresh, N. V., Mangaiyarkarasi, T., & Jenefa, L. (2025). Unveiling the enigma of shadow: Ethical difficulties in the field of AI. In *Navigating data science: Unleashing the creative potential of Artificial Intelligence* (pp. 57–67). Emerald Publishing Limited.

COBIT 2019 Framework: Introduction & Methodology. (2018). ISACA. https://www.isaca.org/resources/cobit

Dutch SA imposes a fine of 290 million euro on Uber because of transfers of drivers' data to the US. (2024). European Data Protection Board. https://www.edpb.europa.eu/news/news/2024/dutch-sa-imposes-fine-290-million-euro-uber-because-transfers-drivers-data-us_en

Gable, J. (2014). Principles for Protecting Information Privacy. *Information Management*, *48*(5), 38–42. https://www.proquest.com/openview/396aa8884be00648f4f8cacca5de57a5/1?cbl=47365&pq-origsite=gscholar

Gupta, A., Amarnani, M., Soanki, S., & Kishore, J. (2025). AI and data privacy in business. In *2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT)* (pp. 109–114). IEEE. https://doi.org/10.1109/CE2CT64011.2025.10939576

International trade in goods. (2024). Eurostat. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=International_trade_in_goods

Kibby, C. (2025). *US State Privacy Legislation Tracker*. IAPP. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

Lambert, P. (2018). *Understanding the New European Data Protection Rules*. CRC Press. https://doi.org/10.1201/9781138069848-31

New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022. (2023). Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022

Oehlers, P., & Li, H. (2008). Identity Theft Issues in China. *Issues in Innovation*, *2*(1), 28–37. https://research.ebsco.com/c/qkxrjx/viewer/pdf/5io5xizyxz

Sloan, R., & Warner, R. (2015). The Harm in Merely Knowing: Privacy, Complicity, Surveillance, and the Self. *The Journal of Internet Law*, *19*(3). https://download.ssrn.com/16/01/26/ssrn_id2722676_code364457.pdf

State Laws Related to Digital Privacy. (2022). NCSL. https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy

Trak, C. (2019). Data Security. *Cybercrime Magazine*. https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

Whitener, M. (2012). Conducting a Privacy Audit. *The Corporate Counselor*, *27*(3).