World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Privacy at the core of audit, compliance and cyber law: The Nebraska data privacy act: a new era for state privacy laws

Chidinma Mercy Ekwuruke * and Lisa Mckee

Department of Cybersecurity, Bellevue University, Nebraska, USA.

World Journal of Advanced Engineering Technology and Sciences, 2026, 19(02), 275-285

Publication history: Received on 15 April 2026; revised on 22 May 2026; accepted on 25 May 2026

Article DOI: https://doi.org/10.30574/wjaets.2026.19.2.0278

Abstract

The COVID-19 pandemic accelerated digital transformation across organizations, exposing significant weaknesses in traditional audit, compliance, and data governance frameworks. The rapid shift to remote and hybrid work environments expanded cybersecurity risks as sensitive data moved through decentralized networks, cloud platforms, and third-party systems. These changes highlighted the need for adaptive, privacy-centered compliance models capable of addressing evolving technological and regulatory challenges. In response, governments increasingly reframed privacy as both a legal obligation and a strategic asset, leading to the expansion of state-level data protection laws in the United States. The Nebraska Data Privacy Act (NDPA), effective January 1, 2025, represents a key development in this evolving privacy landscape. This paper examines privacy as the foundation of modern audit, compliance, and cyber law, using the NDPA as a case study. It analyzes the Act's implications for organizations, its alignment with broader privacy frameworks, and its role in advancing proactive, risk-based data governance in an increasingly digital environment.

Keywords: Data Privacy; Cybersecurity; Audit and Compliance; Nebraska Data Privacy Act (NDPA); Privacy-by-Design; Remote Work Security; State-Level Privacy Laws; Data Governance; Regulatory Compliance; Consumer Data Rights

1. Introduction

The rapid digital transformation accelerated by the COVID-19 pandemic fundamentally reshaped how organizations manage data, conduct audits, and ensure regulatory compliance. As businesses transitioned to remote and hybrid work environments, traditional audit and compliance frameworks—largely designed for centralized, on-site operations—proved insufficient. Employees increasingly accessed sensitive personal, financial, and health data through cloud platforms, home networks, and third-party systems, significantly expanding the cybersecurity threat surface. These changes exposed vulnerabilities in legacy governance models and highlighted the urgent need for privacy-centered, technology-enabled compliance strategies. At the same time, public concern over personal data protection intensified as organizations adopted artificial intelligence, big data analytics, and interconnected digital services. High- profile data incidents and enforcement challenges demonstrated that existing regulatory mechanisms often lag behind technological innovation. Consequently, privacy has evolved from a narrow legal requirement into a strategic organizational asset, essential for maintaining trust, accountability, and legal legitimacy. Modern compliance frameworks now emphasize privacy-by-design, continuous risk assessment, and proactive data governance rather than reactive, rule-based enforcement. In the United States, the absence of a comprehensive federal privacy statute has led to the rise of state-level data protection laws. The Nebraska Data Privacy Act (NDPA), effective January 1, 2025, reflects this post-pandemic regulatory shift by strengthening consumer data rights while balancing practical business obligations. By positioning privacy at the core of audit, compliance, and cyber law, the NDPA illustrates how adaptive governance frameworks can address emerging digital risks. This paper examines the NDPA as a case study to explore the evolving role of privacy in

* Corresponding author: Chidinma Mercy Ekwuruke.

modern audit and compliance systems within an increasingly complex cybersecurity landscape.

1.1. Privacy at the core of audit, compliance, and cyber law

The global COVID-19 (Coronavirus Disease) pandemic served as a catalyst that dramatically exposed the fragility of traditional audit and compliance systems. As organizations scrambled to dapt to fully remote or hybrid work environments, legacy procedures reliant on in-person oversight and centralized control quickly became obsolete. Suddenly, very sensitive data can be stolen by hackers through unsecured home networks, and management decisions forced the audit team to operate virtually, relying on cloud-based systems, video conferencing, and digital tools to conduct assessments. The unplanned transformation revealed a pressing need for more flexible, privacy-centric compliance approaches to address technological shifts and new threat landscapes. Nebraska's 2025 Data Privacy Act (NDPA) came into the picture illustrating how state governments are rethinking privacy governance in light of these global challenges, positioning privacy not as a compliance burden but as a strategic asset (Nebraska Legislature, 2024). Also, looking forward from regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR) and California's Privacy Rights Act (CPRA), a pattern emerges: privacy resilience depends not on the rigidity of rules but on the adaptability of systems (Castka & Searcy, 2021). The shift marks a critical evolution in cybersecurity, where success hinges on proactive data governance, cross-functional coordination, and the seamless integration of privacy-by-design principles. As digital ecosystems expand and threats become more complex, only those organizations that embrace agile and predictive compliance models will maintain trust and legal viability in the post-pandemic world. One prominent case example illustrating consequences of weak data governance is the LinkedIn scraping incident in 2024, where attackers compiled profiles of over 700 million users using publicly accessible data and repackaged it without consent, triggering global debates over privacy, platform responsibility, and compliance failures (O'Shea, 2024). Regulatory bodies like the U.S. Department of Health and Human Services and the European Data Protection Board responded by updating compliance expectations. However, enforcement struggled to keep pace with the speed of technological change (U.S. Department of Health & Human Services, 2024). The crisis illuminated a global truth: traditional audit and compliance systems are no longer sufficient in a world marked by rapid transformation, AI-driven data mining, and unpredictable disruptions.

1.2. **What is privacy?**

Privacy represents an individual's right to control the collection, use, and dissemination of their data, making it not only a legal concept but also a matter of ethics and trust (European Commission, 2022). With the proliferation of artificial intelligence, big data analytics, and interconnected cloud services, organizations are collecting and processing data on a scale never seen before. The exponential growth has fueled public concern about misuse, unauthorized access, surveillance, and the commodification of personal information. Policymakers worldwide have introduced stringent privacy laws to curb abuse and safeguard digital rights. However, compliance with these regulations cannot rest solely on policies; it requires robust enforcement mechanisms such as cybersecurity audits and internal risk assessments. Audits are functions structured to evaluate an organization's practices, helping verify the systems are secure and aligned with regulatory frameworks. At the same time, compliance ensures ongoing adherence to laws and standards like HIPAA, PCI DSS, or GDPR (U.S. Department of Health & Human Services, 2024). Audit and compliance frameworks form the backbone of responsible data governance, particularly in a climate of accelerating cyber threats and evolving digital infrastructures, causing a significant shift in how organizations operate, especially in how they handle privacy, audits, and compliance. With the move to remote work, cybersecurity and privacy became top concerns. Employees are now be able to access sensitive data such as medical records, payment information, and customer profiles from the comfort of their home networks, which are not always secure.

2. Remote work and the associated security challenges

The global transition to remote work, accelerated by the COVID-19 pandemic, revealed systemic deficiencies within traditional cybersecurity and compliance infrastructures. Legacy systems, often reliant on perimeter-based defenses, struggled to support decentralized operations. In response, organizations adopted advanced security measures such as Virtual Private Networks (VPNs), Multi- Factor Authentication (MFA), endpoint detection and response (EDR), and encrypted cloud-based servicesto ensure secure communication and data exchange across remote environments. The controls aligned with the regulatory mandates of frameworks including the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and the Payment Card Industry Data Security Standard (PCI DSS), each of which emphasizes strict controls over personal, health, and financial information (U.S. Department of Health & Human Services, 2024; PCI Security Standards Council, 2022). Information Security Management Systems (ISMS), such as those governed by ISO and IEC (ISO/IEC 27001, 2013), also gained renewed prominence, particularly as independent certification became a symbol of trustworthy cyber hygiene and regulatory

alignment. In addition, the increased attack surface prompted the widespread implementation of zero-trust architectures, mandating continuous verification of access permissions regardless of user location or network origin. Security Information and Event Management (SIEM) systems, identity governance platforms, and behavior analytics tools further reinforced compliance postures in the remote operational context. In response to pandemic-related disruptions, regulatory authorities enacted flexible yet principled guidance to sustain compliance expectations. The U.S. Department of Health and Human Services temporarily suspended certain HIPAA penalties related to telehealth technology usage, provided that core privacy protections remained in effect (Department of Human Health Service, 2024). Simultaneously, auditing processes underwent digital reinvention. Traditional on-site inspections were replaced with remote audit tools, including secure document portals, real-time video walkthroughs, smart glasses, and unmanned aerial systems (UAS), which enabled auditors to verify compliance while maintaining health protocols. These adaptations preserved audit integrity and revealed opportunities for cost savings and increased audit frequency. Internal policies also evolved rapidly. Remote access policies were updated to reflect new user behavior patterns, while endpoint security, encrypted data transfer channels, and strict identity verification protocols became essential security elements. Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs) were conducted with increased frequency to evaluate risks stemming from remote processing and storage of sensitive data. Post-pandemic shifts in data protection philosophy have reshaped the compliance landscape permanently. The widespread implementation of privacy-by-design and privacy-by-default principles signaled a cultural and operational shift in how organizations handle regulatory risk, requiring privacy considerations at the inception of every process and technology deployment. The convergence of artificial intelligence (AI) and machine learning (ML) with audit methodologies enabled real-time anomaly detection, risk prediction, and automated compliance reporting, contributing to proactive governance models. Privacy legislation in the United States continues to evolve, with landmark statutes such as the California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), and the recently introduced Nebraska Data Privacy Act (NDPA) expanding consumer rights over personal data and obligating businesses to meet stringent transparency and accountability standards (California State Legislature, 2021; Nebraska Legislature, 2024). Organizational responses have included the implementation of continuous compliance monitoring systems, hybrid audit models combining physical and virtual assessments, and enterprise-wide risk assessment frameworks. These measures reflect a growing recognition that cybersecurity, privacy, and legal compliance are inseparably linked in an increasingly digital, regulated, and high-risk operational environment.

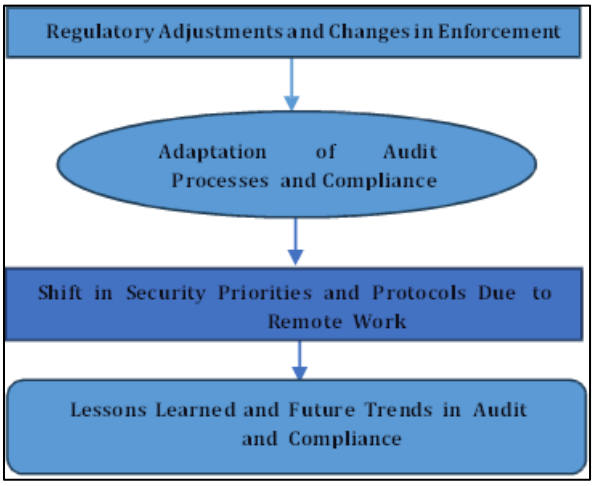

Figure 1 Flowchart: Evolution of Security Challenges & Compliance in the Pandemic Era.

As teams began working from home, organizations had to strengthen their security posture quickly. Tools like Virtual Private Networks (VPNs), multi-factor authentication (MFA), and encrypted cloud storage became essential. Privacy compliance frameworks such as HIPAA pushed businesses to adapt fast to protect personal data, even outside the office. In 2000, Bruce Schneier said, "Security is a process, not a product," and the pandemic 20 years later showed how true that was. During the COVID-19 pandemic, the Mayo Clinic implemented rapid deployment of VPNs and endpoint encryption to allow healthcare professionals to access Electronic Health Records (EHRs) remotely without violating HIPAA requirements (Furst, J. 2022).

3. Features of security challenges

3.1. Regulatory Adjustments and Changes in Enforcement

Regulators also responded. Some enforcement agencies showed flexibility, recognizing the difficulty of maintaining standard compliance routines. However, the expectations for protecting consumer privacy did not disappear. The pandemic compelled regulatory agencies to reconsider traditional enforcement approaches to compliance. Many agencies demonstrated flexibility, understanding that strict adherence to standard procedures was not always feasible. For example, the U.S. Department of Health and Human Services (HHS) temporarily relaxed enforcement of some HIPAA rules, enabling healthcare providers to quickly adopt telehealth solutions using non-traditional platforms. The flexibility allowed vital healthcare services to continue while maintaining a reasonable level of privacy protection. Despite such accommodations, regulators made it clear that the obligation to protect sensitive consumer data, especially in healthcare, finance, and education, remained non-negotiable. At the same time, frameworks such as HIPAA continued to hold organizations accountable for data privacy, often increasing scrutiny as remote work raised new risks. Healthcare organizations, for instance, faced heightened expectations to secure electronic patient records accessed remotely. Financial institutions were required to maintain strict controls over remote transaction systems to prevent fraud. Educational institutions had to ensure that digital learning platforms complied with student privacy laws. The shifting regulatory landscape thus created a dynamic tension between pragmatic enforcement flexibility and steadfast data protection mandates.

3.2. Adaptation of Audit Processes and Compliance Strategies

According to (Castka & Searcy, 2021), the change was more than a workaround. It marked the beginning of a new audit paradigm. Auditors began using drones, smart glasses, and wearable cameras to inspect hard- to-reach or high-risk locations. Companies realized that many parts of the audit process could be safely and effectively done online. In-person audits became impractical under pandemic restrictions, prompting organizations to innovate their compliance verification methods. Remote auditing tools such as Zoom and Microsoft Teams became central to conducting interviews, reviewing documentation, and evaluating compliance remotely. The digital pivot not only maintained audit schedules but also allowed greater flexibility and reduced travel costs. Companies such as Ernest & Young (EY) and PwC quickly adopted virtual audits, developing secure methods to handle sensitive audit evidence online and uphold confidentiality standards. Beyond video conferencing, organizations integrated emerging technologies like drones, smart glasses, and wearable cameras to enhance audit capabilities. For example, industrial firms used drones to remotely inspect infrastructure, avoiding the need to send auditors into hazardous environments. Smart glasses allowed on-site personnel to stream real-time video to auditors, enabling remote observation and immediate feedback.

3.3. Shift in Security Priorities and Protocols Due to Remote Work

With remote work becoming a long-term model for many organizations, privacy policies must be rewritten. Security teams prioritized access control, identity management, and endpoint protection to prevent unauthorized access to private data. Regular privacy risk assessments became more critical than ever to ensure sensitive data wasn't being mishandled. The rapid shift to remote work forced organizations to fundamentally rethink their security protocols and privacy policies. Existing guidelines designed for on- premises environments were often inadequate for protecting data accessed from home networks and personal devices. Consequently, many companies rewrote privacy policies to explicitly address risks related to remote access, BYOD (Bring Your Own Device), and data handling outside corporate firewalls. These updates included clear expectations for employees regarding device security, data storage, and secure communication practices. Security teams also placed heightened emphasis on access control and identity management. Multi-factor authentication (MFA) became widely mandated to mitigate credential theft risks, while Zero Trust models gained traction, ensuring no user or device was automatically trusted regardless of location. Endpoint protection strategies were reinforced with tools that provide continuous monitoring and threat detection for devices outside traditional security perimeters. For instance, companies like Microsoft deployed enhanced endpoint detection and response (EDR) platforms to safeguard remote employees, while financial institutions adjusted risk assessments to account for new remote vulnerabilities (Microsoft, 2023).

3.4. Lessons Learned and Future Trends in Audit and Compliance

The pandemic taught us that audit and compliance practices must be flexible, technology-driven, and privacy-focused. The future of auditing is now shaped by real-time monitoring, AI-driven analytics, and digital twins, virtual replicas of systems or processes that can be used for predictive auditing. Organizations that invest in privacy-first technologies and digital audit tools are better prepared to meet evolving compliance challenges in a post-pandemic world. The pandemic underscored the importance of flexibility, technology adoption, and privacy-centric approaches in audit and compliance

functions. Organizations learned that rigid, periodic audits were insufficient in a fast-changing environment and that continuous, technology-enabled monitoring was essential. The realization prompted many companies to invest in AI-driven analytics, and real-time data feeds to identify risks proactively and maintain ongoing compliance assurance rather than episodic reviews. Looking ahead, emerging technologies like digital twin's virtual replicas of physical systems promise to revolutionize auditing by enabling predictive analysis and scenario testing without disrupting operations. AI tools will further enhance auditors' ability to analyze complex data streams and detect anomalies. Organizations that embed privacy-first principles into their compliance frameworks and embrace these innovations will be better positioned to navigate evolving regulatory landscapes and security challenges in the post-pandemic world. The future of auditing is digital, dynamic, and deeply integrated with organizational risk management.

4. The privacy, audit, and compliance: comparison between countries and cities

4.1. Developing Countries vs. the USA

Privacy, audit, and compliance frameworks differ greatly between developing countries and the United States, primarily due to resource disparities, regulatory maturity, and technological infrastructure. In the United States, there is a growing emphasis on privacy

rights, backed by federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA), by state regulations such as, California Consumer Privacy Act (CCPA) and the, New York Privacy Act (The New York State Senate, 2019), and by global regulations and frameworks such as the, Payment Card Industry Data Security Standard (PCI DSS), European Union GDPR, and Brazil LGPD. These laws mandate strict audit trails, technical safeguards, and compliance programs enforced by regulatory bodies like the Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC).

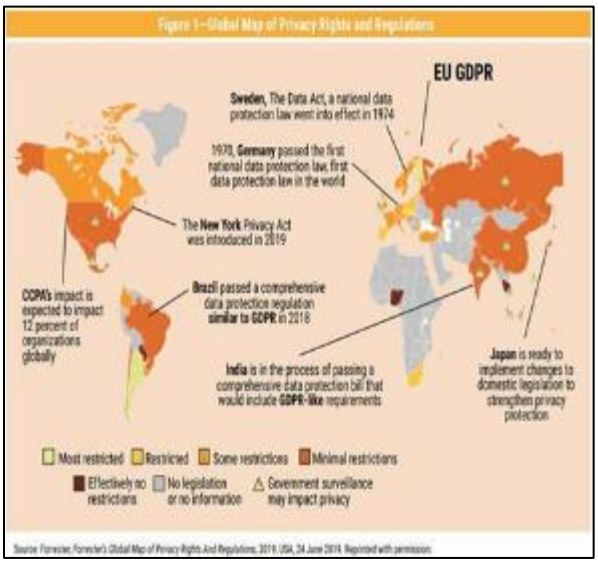

Figure 2 Forrester's Global Map (2019)

This section compares the constating audit and compliance capabilities between, developing nations, how they often struggle with enforcing privacy and compliance regulations. While many have adopted data protection laws modeled after the EU's General Data Protection Regulation (GDPR), implementation remains inconsistent due to limited funding, lack of trained professionals, and weak institutional oversight. Bada and Sasse (2015) state that "in many low-income countries, cybersecurity is often seen as a secondary priority to other socio-economic challenges." As a result, audits are often infrequent, and breaches go unreported or unpunished, creating a fragile privacy environment. The rapid digitization of services exacerbates these challenges without corresponding investment in secure infrastructure.

Despite these gaps, some developing countries are making significant strides through partnerships with international organizations, cybersecurity capacity- building programs, and regional privacy frameworks. For example, African countries like Kenya and Nigeria are developing national cybersecurity strategies that align with global best practices, although enforcement and auditing mechanisms are still evolving. In comparison, the U.S. continues to lead in compliance auditing sophistication and the institutionalization of privacy as a governance issue.

5. The Privacy, Audit, and Compliance in the USA and Nebraska

In the United States, privacy and compliance enforcement varies significantly by state. While Federal regulations tend to be sector-specific (HIPAA, GLBA, FERPA) and while they form the backbone of national privacy governance, state-level laws like the California Consumer Privacy Act (CCPA) and the Colorado Privacy Act (CPA) have introduced broader consumer protections. These state regulations provide residents with specific rights over personal data, mandate data processing disclosures, and require businesses to implement robust compliance mechanisms. Nebraska has joined the movement by enacting the Nebraska Data Privacy Act, codified in Neb. Rev. Stat. §§ 87-1101 to 87-1130, effective January 1, 2025. Under the legislation, the Nebraska Attorney General protects residents' personal data rights and provides resources to educate businesses and consumers about their rights and responsibilities. The Act applies to any business or organization that;

- Conducts business in Nebraska or offers products/services to Nebraskans
- Processes or sells personal data.
- Thirdly, it is not considered a small business under the federal Small Business Act as of January 1, 2024 (Nebraska Legislature, 2024).

The law defines personal data as any information reasonably linkable to an identifiable individual, including pseudonymous data, when combined with other identifying information. Sensitive data, such as biometric, racial, or geolocation, is subject to stricter protections. Businesses functioning as data controllers or data processors have defined roles and obligations regarding collecting, using, modifying, storing, and deleting personal data. The Act also clearly outlines exceptions regarding specific businesses, types of information, and data usage scenarios (Neb. Rev. Stat.§§ 87-1103 to 87-1106).

The significant mark development for privacy compliance in Nebraska reflects the broader national and international trend toward empowering individuals with more control over their personal information. Organizations operating in Nebraska must adjust their audit processes, privacy policies, and compliance mechanisms accordingly. Unlike California, Nebraska's approach is more recent and reactive, but its inclusion of consumer rights and business accountability illustrates a strong step forward in privacy governance.

5.1. Nebraska's Approach to Data Privacy and Compliance

In 2024, Nebraska enacted the Nebraska Data Privacy Act (NDPA) to be enacted by January 1, 2025, a legislative milestone that aligns the state with a growing national trend of state-level data privacy laws. Codified as Neb. Rev. Stat. §§ 87-1101 to 87- 1130, the statute places Nebraska among the states taking proactive steps to regulate the collection, processing, and storage of personal data. The law mirrors foundational principles from global and national data protection frameworks, notably the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR), while also introducing state-specific nuances to fit Nebraska's regulatory environment (Nebraska Legislature, 2024). After observing legislative trends in states like California and Colorado, Nebraska passed the Nebraska Data Privacy Act, which became effective in January 2025. A local insurance company, BlueCross BlueShield of Nebraska, reported updating its audit practices in 2024 to align with the anticipated regulations (Blue Cross Blue Shield Nebraska, 2024).

5.2. Scope and Applicability of the NDPA

The NDPA applies to businesses that meet the following criteria:

- Conduct business in Nebraska or target services/products at Nebraska residents,
- Process or sell the personal data of at least 25,000 Nebraska consumers and
- Do not qualify as a "small business" under the U.S. Small Business Administration standards.
- Conducts Business in Nebraska or Offers Products/Services to Nebraska Residents

The Nebraska Data Privacy Act (NDPA) applies to any business that directly engages with Nebraska residents, regardless of the company's physical location. The organizations with physical locations within the state, such as retail outlets, service centers, or corporate offices. However, the scope extends beyond physical presence to include digital commerce and services. Businesses offering products through online platforms or digital services like streaming content, cloud-based applications, or mobile apps must ensure compliance if these are accessible to Nebraskans. For example, an e-commerce company headquartered in Texas that routinely ships products to Omaha or Lincoln residents is subject to the NDPA. Similarly, a subscription-based music streaming service based in California with Nebraska

customers must uphold the data privacy rights mandated by the law. The criterion ensures that any business leveraging Nebraska's consumer base is held accountable for protecting personal data, thus extending consumer rights uniformly across physical and digital marketplaces.

5.3. Processes or Sells the Personal Data of Consumers.

The second condition centers around the handling of personal data belonging to Nebraska consumers. The NDPA broadly defines "personal data" as any information that can identify or be linked to an individual, such as names, email addresses, geolocation, IP addresses, browsing behavior, and biometric data. Companies involved in collecting, analyzing, or selling the type of information, whether directly or through third-party partnerships, fall under the law's jurisdiction. Crucially, the term "selling" includes any exchange of personal data for monetary or other valuable consideration, meaning even non- traditional monetization models (like behavioral advertising) may qualify. For instance, a mobile game app that tracks user interactions and sells anonymized data to advertisers must comply with NDPA mandates. Likewise, a newsletter company that shares subscriber lists with marketing affiliates is engaged in personal data processing.

5.4. Is Not Considered a "Small Business" Under the U.S. Small Business Act

The NDPA incorporates an exemption for entities classified as "small businesses" under the U.S. Small Business Administration (SBA) standards, which vary by industry but generally consider employee headcount and annual revenue. For example, a retail company with fewer than 500 employees or annual revenue below $7.5 million would typically be exempt from NDPA compliance. The exemption aims to reduce the regulatory burden on startups and smaller enterprises with limited resources. However, the exemption is not absolute; small businesses are still required to comply if they deal with sensitive personal data, including health records, biometric data, precise geolocation, or data from children under 13. A small health-tech startup collecting patient vitals or a mobile app aimed at children that tracks usage patterns would still be bound by NDPA provisions. The tiered approach strikes a balance between consumer protection and economic feasibility, allowing flexibility for small businesses while maintaining safeguards for the most vulnerable types of personal data.

6. Consumer Rights and Business Obligations

The NDPA empowers Nebraska residents with several fundamental rights over their personal data, including:

Right to access: The Nebraska Data Privacy Act grants individuals the authority to obtain a comprehensive summary of personal data held by a covered business. It includes both the categories of information collected (e.g., contact details, purchase history, or browser activity) and specific data points associated with the individual. For instance, if a user has made purchases on an e-commerce website, the individual may request a report showing order history, saved addresses, and stored payment preferences. The streaming platform must disclose viewing history and user preferences upon request, and the right ensures transparency by allowing individuals to understand how personal data is being used and stored (Bruce Wray, 2024).

Right to deletion: Individuals have the legal ability to request the erasure of personal information collected by an organization unless specific exceptions apply, such as the need to retain data for legal compliance, transaction completion, or system security. For example, a customer who previously registered for a newsletter may request that all related data, including email addresses, preferences, and interaction logs, be deleted from marketing databases. However, if a financial transaction is still pending or subject to audit requirements, certain information may be retained temporarily. The provision empowers users to control digital footprints and minimize long-term data exposure (Thompson Hine LLP, 2024).

Right to correction: The NDPA allows individuals to demand the rectification of inaccurate or outdated personal data maintained by a business. For example, if a service provider has stored an incorrect birth date or misspelled last name in a user profile, a correction request can be submitted to update the record. Accurate information not only benefits the individual but also ensures data integrity within the organization's systems, reducing operational errors and improving customer experience. The right isparticularly relevant in healthcare, finance, and education sectors where incorrect data may lead to service denials or compliance violations (LB1074, 2024).

Right to opt-out: The right to opt-out allows individuals to restrict the transfer of personal data to third parties, especially for purposes such as targeted advertising or analytics. It includes any transaction where personal information is exchanged for monetary value or other benefits. For instance, a user of a fitness-tracking app may choose to prohibit the sharing of activity data with external advertising platforms. Similarly, an online bookstore customer may opt out of

data being shared with recommendation engines or marketing affiliates. Organizations must provide a clear and accessible mechanism, such as a "Do Not Sell or Share My Data" link on a homepage, to enable the opt-out function (LB1074, 2024).

The rights echo provisions found in other state laws, especially the CCPA and the Virginia Consumer Data Protection Act (VCDPA, 2023). However, Nebraska's approach emphasizes transparency and education, mandating that businesses provide clear privacy notices and invest in public awareness campaigns (Nebraska Legislature, 2024).

6.1. Enforcement and Compliance Mechanisms

The Nebraska Attorney General is tasked with enforcing the NDPA. There is no private right of action, which means that individuals cannot sue companies directly under the law. Instead, the Attorney General may bring civil enforcement actions against companies for non-compliance, with penalties reaching up to $7,500 per violation. To comply, businesses must implement data protection measures such as:

- Privacy impact assessments (PIAs) for new data processing activities,
- Data minimization practices,
- Secure data storage and access controls and vendor management protocols, especially for third-party data processors.

Furthermore, companies functioning as data controllers (entities that determine the purpose and means of data processing) or data processors (entities that process data on behalf of a controller) as assigned.

6.2. Comparing Nebraska to Other U.S. States

Nebraska's data privacy legislation, the Nebraska Data Privacy Act (NDPA), positions the state as an emerging participant in the broader national conversation about consumer data rights, yet it differs significantly from trailblazing states like California and Virginia. While California has set the gold standard in state-level privacy reform through the California Consumer Privacy Act (CCPA) and its amendment, the California Privacy Rights Act (CPRA), Nebraska's approach is more measured and reactive. California established a dedicated enforcement authority, the California Privacy Protection Agency (CPPA), granting it independent power to audit businesses, issue fines, and conduct rulemaking (California State Legislature, 2021). In contrast, Nebraska's law is enforced solely by the state Attorney General, which may limit enforcement bandwidth and responsiveness. Moreover, Nebraska explicitly exempts certain entities, such as small businesses and nonprofits, from compliance requirements, while California's broad definitions and indirect compliance expectations may still impact those sectors through supply chain or vendor relationships. These structural differences reflect not just policy philosophy but also capacity. California's mature regulatory infrastructure allows it to adopt a more proactive and aggressive privacy posture. Unlike California, which has led the nation in privacy reform with the CCPA and the California Privacy Rights Act (CPRA), Nebraska's law is relatively new and reactive. California includes a dedicated enforcement agency, the California Privacy Protection Agency, whereas Nebraska relies solely on its Attorney General. Nebraska's law is also less aggressive in scope, excluding entities like small businesses and nonprofits that California's law may still influence through indirect compliance pressures (California State Legislature, 2021). However, Nebraska's legislation is notable for being consumer-friendly and business- accessible, aiming for clarity and practical enforceability rather than regulatory burden. It represents a middle ground between minimalist laws, such as Utah's, and more comprehensive frameworks, like California's. Despite these differences, Nebraska's NDPA is notable for its pragmatic orientation. It avoids overburdening local businesses while still advancing consumer rights through clearly defined opt-out provisions, data access rights, and correction mechanisms. Nebraska's model appears intentionally business-accessible, with simpler compliance expectations and a narrower scope of applicability traits that resemble more minimalist privacy laws like Utah's Consumer Privacy Act, which focuses on balancing consumer protection witheconomic development. However, Nebraska's law is arguably more robust than Utah's, offering a middle path that supports privacy innovation without overwhelming emerging enterprises (Utah Legislature, 2022). The legislative strategy may be especially important in states with fewer resources to support expansive oversight infrastructures. As more states adopt similar laws, Nebraska's moderate but evolving framework could become a template for states seeking a functional balance between protecting personal data and maintaining a favorable business climate. In the absence of a federal privacy statute, the patchwork of state laws underscores the importance of interoperability and policy harmonization across jurisdictions (Brookings Institution, 2023).

6.3. Implications for Organizations in Nebraska

Businesses operating in Nebraska are now required to take a comprehensive and proactive approach to data privacy management in order to comply with the Nebraska Data Privacy Act (NDPA). The begins with a thorough evaluation of

the entire data lifecycle, from collection and storage to sharing and disposal. Organizations must update privacy policies to clearly reflect how personal information is used, processed, and protected. These policies must not only comply with the NDPA but also be easily accessible and understandable to consumers. Training programs should be implemented to ensure that all employees— particularly those handling consumer data understand privacy rights, data handling protocols, and their responsibilities under the law. Channels must be established to handle consumer requests, including those for data access, correction, deletion, and opting out of data sales or sharing. The often involves building or upgrading customer service portals, revising consent mechanisms, and enhancing data subject access request workflows.

Moreover, internal audits have become a critical tool in ensuring NDPA compliance. Regular audits allow organizations to identify weaknesses in data governance practices, verify that third-party vendors and contractors also meet NDPA requirements, and ensure that records of processing activities are maintained and up to date. Organizations must evaluate vendor contracts to confirm that data sharing aligns with the law's provisions and that appropriate safeguards are in place to prevent unauthorized access or misuse. The implementation of the NDPA is also reflective of a broader trend toward decentralized privacy regulation in the United States, where states increasingly take charge of protecting consumer data rights. However, the patchwork of state-level laws is creating a complex compliance environment for businesses operating across multiple jurisdictions. Asa result, there is mounting pressure for federal lawmakers to pass a unified national privacy framework that would establish consistent protections and simplify regulatory obligations nationwide. Until such legislation is passed, organizations must remain agile, continuously adapting to evolving privacy expectations across the country while maintaining strong compliance programs at the state level.

7. Pre-covid vs. Post-covid compliance: a privacy and audit perspective

The global shift caused by COVID-19 reshaped organizational approaches to cybersecurity, compliance, and data privacy. Pre-pandemic, many compliance frameworks and audits were structured around in-person work environments with centralized IT infrastructure. Privacy enforcement was often localized and focused on sector-specific rules like HIPAA, an example is the episode featuring cybersecurity leader Dr. Ann Cavoukian discussing how organizations are implementing Privacy by Design frameworks across industries, especially post- pandemic (Taylor, 2023).

However, the pandemic forced the rapid adoption of remote work, exposing gaps in existing compliance frameworks and amplifying the importance of data protection. Organizations were suddenly vulnerable to phishing attacks, ransomware, and fraud, particularly targeting remote workers using unsecured networks and personal devices. The shift drove a surge in privacy concerns and regulatory pressures. As a result, compliance frameworks evolved to prioritize remote audit capabilities, proactive data protection strategies, and heightened awareness around digital threats (U.S. Department of Health & Human Services, 2024).

The increased dependence on virtual platforms prompted regulators and businesses to revise security protocols, often blending flexibility with resilience. Post-COVID, there is a stronger emphasis on real-time monitoring, digital audit tools, privacy-by-design, and cross-border data governance. The changes represent a paradigm shift that favors agility, transparency, and a user-focused approach to compliance and privacy (U.S. Senate Committee on Commerce, Science, and Transportation, 2019)

Table 1 Pre-COVID vs. Post-COVID Compliance, Privacy, and Audit

Aspect	Pre-COVID	Post-COVID
Compliance Frameworks	In-person audits; static controls; sector-specific rules	Remote audits; dynamic controls; privacy-by- design emphasized
Security Protocols	Perimeter-focused (office firewalls, onsite access)	Endpoint-focused (VPNs, MFA, cloud access, device monitoring)
Privacy Concerns	Focused on HIPAA, FERPA, COPPA, DPPA, GLBA, FCRA, DPPA, BIPA in traditional settings	Expanded to cover remote work, home networks, surveillance risks, and mobile privacy tools
Audit Methods	Onsite document review and physical access verification	Virtual assessments, cloud-based logs, screen sharing, AI-driven compliance tracking

Cyber Threat Landscape	Mostly contained to known threat vectors	Phishing, ransomware, fake apps, and impersonation attacks surged by over 600% during the pandemic
Regulatory Response	Standard enforcement cycles and audits	Temporary leniency; more guidance; accelerated privacy law reform (e.g., CCPA/CPRA updates)
Employee Role in Compliance	Often limited to policy training	Central to defense strategy; trained for phishing, data handling, and secure access from home
Use of Technology	Selective digital transformation	Full digital transformation; increased cloud adoption, monitoring, and remote work capabilities
Data Governance Priorities	Compliance-focused	Risk-based, agile, and transparency-driven privacy and data governance

8. Conclusion

In conclusion, the Nebraska Data Privacy Act (NDPA) reflects the broader post-pandemic shift towards strategic, privacy-centered compliance frameworks that balance consumer right with business feasibility. The NDPA takes a middle-ground approach, excluding small businesses from compliance, focusing on clarity, and limiting enforcement to the state Attorney General. It makes it more approachable for organizations operating in or targeting Nebraska residents, provided they process the personal data of 25,000 or more consumers and do not qualify as "small businesses" under the U.S. Small Business Administration (SBA). The Act grants key rights such as access, correction, deletion, and opt-out from data sales. These consumer rights require organizations to revise privacy policies, train staff, and implement transparent data governance processes. Compliance efforts should include conducting internal audits, reviewing third-party contracts, and developing mechanisms for fulfilling consumer requests efficiently (ISACA, 2020). This include updating privacy policies, training staff on data protection practices, and establishing processes to respond to consumer data requests. By integrating these frameworks into their operations, organizations can not only meet the NDPA's obligations but also build trust with consumers and stakeholders.

To make the NDPA truly impactful, Nebraska must invest in community education, digital outreach and perhaps even integrate privacy awareness into school curricula and public service campaigns. Promoting the law through local media, social platforms, and community partnerships can help ensure that both consumers and business owners understand its significance. With greater visibility, the NDPA can evolve from law into a living standard of practice, encouraging ethical behavior and a culture that values privacy. Looking to the future, the NDPA's alignment with frameworks from NIST regulation offers a scalable compliance roadmap for compliance and accountability. NIST's Privacy Framework and Cybersecurity Framework explain proactive risk identification, data lifecycle management, and privacy engineering principles echoed in the NDPA's business obligations. The growing patchwork of state-level laws is likely to push federal lawmakers toward unified national privacy regulation, a move increasingly supported by privacy advocates and industry leaders alike. In doing so, Nebraska not only strengthens local accountability but also contributes to shaping a national standard in the evolving landscape of U.S data privacy law.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Blue Cross Blue Shield Nebraska. (2024). Draft for discussion purposes only. Subject to review and submission for approval. https://www.nebraskablue.com/-

[2] /media/Files/NebraskaBlueDotCom/About- Us/Compliance-and-Ethics/Annual_Meeting_Members_Goodlife_Partner s_Draft_Minutes.pdf?utm_source=chatgpt.com

[3] Brookings. (2013, July 19). Privacy, technology, and national security: An overview of intelligence collection. https://www.brookings.edu/events/privacy- technology-and-national-security-an-overview-of- intelligence-collection/

[4] Bruce Wray. (2024). CSF.

[5] https://www.nebraskacert.org/CSF/CSF-Aug2024.pdf

[6] California State Legislature. (2021). California Privacy Rights Act (CPRA). https://oag.ca.gov/privacy/ccpa

[7] Castka, P., & Searcy, C. (2021). Audits and COVID-19: A paradigm shift in the making. Business Horizons, 66(1), 5–11. https://pmc.ncbi.nlm.nih.gov/articles/PMC9532210/#

[8] :~:text=The%20COVID%2D19%20pandemic%20rap idly,person%2C%20on%2Dsite%20audits.

[9] European Commission. (2022). General Data Protection Regulation (GDPR) compliance guidelines.https://www.trade.gov/market- intelligence/eu-general-data-protection-regulation- gdpr

[10] Forrester. (2019). The 2019 Forrester global map of privacy rights and regulations. https://www.forrester.com/blogs/its-here-the-2019- forrester-global-map-of-privacy-rights-and- regulations/

[11] Furst, J. (2022, February 28). Mayo Clinic's 2021 achievements affirm 'Bold. Forward.' strategic vision, staff dedication. https://newsnetwork.mayoclinic.org/discussion/mayo

[12] -clinics-2021-achievements-affirm-bold-forward- strategic-vision-staff-dedication/

[13] ISO/IEC 27001. (2013). Information technology- Security techniques-Information security management system-Requirement. https://itref.ir/uploads/editor/42890b.pdf

[14] Microsoft. (2023). Audit policy recommendations. https://learn.microsoft.com/en- us/windows-server/identity/ad-ds/plan/security-best- practices/audit-policy-recommendations

[15] Nebraska Legislature. (2024). Nebraska Data Privacy Act, Neb. Rev. Stat. §§ 87-1101 to 87-1130. https://protectthegoodlife.nebraska.gov/data-privacy- homepage. https://listings.pcisecuritystandards.org/documents/P CI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r1.pdf

[16] Taylor. (2023). Privacy by design in the real world [Audio podcast episode]. https://www.google.com/gasearch?q=privacy%20by

[17] %20design%20in%20the%20real%20world%20%5B audio%20podcast%20episode%5D.&source=sh/x/gs/m2/5#fpstate=ive&vld=cid:ad9c2487,vid:rSUPTIz9E ZI,st:0

[18] The New York State Senate. (2019). Bills and Laws. https://www.nysenate.gov/legislation

[19] O'Shea. (2012). The LinkedIn incident. https://darknetdiaries.com/transcript/86/

[20] PCI Security Standards Council. (2022). PCI DSS v4.0 summary of changes.

[21] Thompson Hine LLP. (2024). The data protection guidebook 2024. https://www.thompsonhine.com/insights/the-data- protection-guidebook-2024/

[22] US Department of Health and Human Services. (2024). HIPAA for professionals. https://www.hhs.gov/hipaa/for-professionals/index.html

[23] Utah State Legislature. (2022). S.B. 227 Consumer Privacy Act

[24] https://le.utah.gov/~2022/bills/static/SB0227.html

[25] VCDPA. (2023). Attorney General of Virginia. https://www.oag.state.va.us/consumer- protection/files/tips-and-info/Virginia-Consumer- Data-Protection-Act-Summary-2-2-23.pdf