Global Privacy & Data Protection eBook

A Snapshot of Select Countries

BDO

We embarked on a global dialogue to uncover what's on the horizon for Privacy & Data Protection in 2025. We challenged our regional leaders to spotlight emerging trends, share their insights on privacy, and contribute thought-provoking commentary to articles worth your attention. Here's what we discovered!

As we enter 2025, global privacy and data protection are being reshaped by key trends. Data sovereignty is on the rise, with countries asserting control over data within their borders, leading to localised regulations that challenge multinational organisations. Ethical considerations in data processing are gaining attention, especially with the proliferation of AI and machine learning, prompting calls for regulations that ensure fairness and transparency.

Privacy by design is becoming more prominent, advocating for the integration of privacy into technology development from the start. This proactive approach helps protect personal information and mitigate risks. Decentralised technologies like blockchain and cryptocurrency offer both opportunities and challenges, requiring nuanced regulatory frameworks to address their complexities.

In marketing technology, there is a push for ethical handling of consumer data, with regulations demanding clear consent and robust protection measures to curb invasive practices. Cross-border data transfers remain crucial, with mechanisms like Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) ensuring secure exchanges while maintaining privacy standards.

In our interconnected world, privacy is a fundamental right that demands rigorous protection and harmonisation. As we navigate the digital age, striving for comprehensive privacy protections is essential to uphold individual rights and foster trust. Through international cooperation and adaptive policymaking, we can ensure privacy is safeguarded for all, transcending geographical boundaries.

> *A unified approach to data protection is essential for fostering trust and ensuring the rights of individuals are respected on a global scale." Alternatively, "In a globalised world, privacy is not just a privilege but a fundamental right that demands rigorous protection and harmonisation across nations.*

KAREN SCHULER
Global Privacy & Data Protection Leader
kschuler@bdo.com

BDO USA

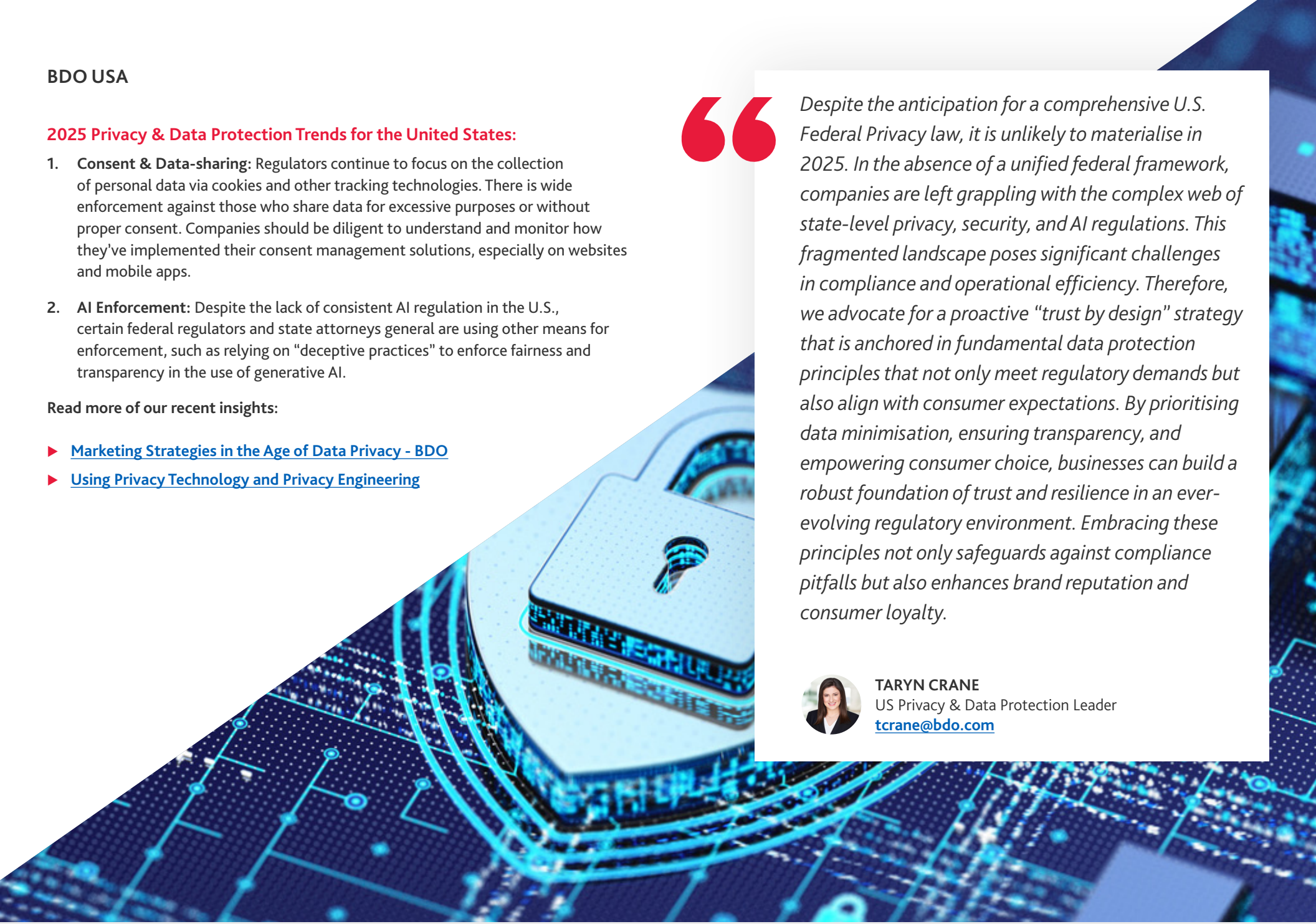
2025 Privacy & Data Protection Trends for the United States:

1. **Consent & Data-sharing:** Regulators continue to focus on the collection of personal data via cookies and other tracking technologies. There is wide enforcement against those who share data for excessive purposes or without proper consent. Companies should be diligent to understand and monitor how they've implemented their consent management solutions, especially on websites and mobile apps.

2. **AI Enforcement:** Despite the lack of consistent AI regulation in the U.S., certain federal regulators and state attorneys general are using other means for enforcement, such as relying on "deceptive practices" to enforce fairness and transparency in the use of generative AI.

Read more of our recent insights:

- Marketing Strategies in the Age of Data Privacy - BDO
- Using Privacy Technology and Privacy Engineering



Despite the anticipation for a comprehensive U.S. Federal Privacy law, it is unlikely to materialise in 2025. In the absence of a unified federal framework, companies are left grappling with the complex web of state-level privacy, security, and AI regulations. This fragmented landscape poses significant challenges in compliance and operational efficiency. Therefore, we advocate for a proactive "trust by design" strategy that is anchored in fundamental data protection principles that not only meet regulatory demands but also align with consumer expectations. By prioritising data minimisation, ensuring transparency, and empowering consumer choice, businesses can build a robust foundation of trust and resilience in an ever-evolving regulatory environment. Embracing these principles not only safeguards against compliance pitfalls but also enhances brand reputation and consumer loyalty.

TARYN CRANE
US Privacy & Data Protection Leader
tcrane@bdo.com

BDO UK

2025 Privacy & Data Protection Trends for the UK:

1. **Changing UK Data Protection Regulation:** The UK government has reintroduced data protection regulation with the "Data Use and Access Bill," currently under parliamentary review. If passed, it will require organisations processing personal data in the UK to comply with new requirements. Although it resembles the existing UK GDPR, organisations will need to review and adapt once it's enacted.
2. **UK Artificial Intelligence Regulation:** While the EU AI Act emerged in 2024, the UK cannot adopt it due to jurisdictional differences. The UK is developing its own AI regulatory framework, which will evolve with technological advancements and eventually open for public consultation. The focus will be on AI governance and ethical use, with developments expected in 2025 and beyond.
3. **Accountability in Data Protection Compliance:** UK organisations must demonstrate accountability in data protection. Many lack effective data privacy governance structures, which hinders compliance. Organisations need to improve their strategies, despite challenges like limited resources and expertise, as accountability is a key focus for UK regulators.

Read more of our recent insights:

- Data Privacy update - BDO
- Data Protection Update – ICO Priorities moving forward - BDO

In a more digitally focused world with the ever-growing emergence of AI, data protection rightly continues to be a significant risk to organisations in how they are using data, but also to the individuals whose data is being used in seeking assurances that their rights and freedoms are not being compromised. As a result of this, the regulatory landscape is becoming more complex on a global scale, and it is vital that organisations are staying informed of requirements and have fully embedded risk management practices in place to support with safeguarding their reputation and to help build trust with their partners and customers.

CHRISTOPHER BEVERIDGE
UK Head of Privacy & Data Protection
christopher.beveridge@bdo.co.uk

2025 Privacy & Data Protection Trends for Spain:

1. **Increase in the AEPD's sanctioning activity:** In 2023, the AEPD imposed 367 sanctions, with a total amount close to €30 million, representing an increase of 44% over the previous year.
2. **Increase in the number of complaints filed with the AEPD:** In 2023, 21,590 complaints were filed, an increase of 43% over 2022, reflecting greater awareness and concern for data protection among citizens and companies.
3. **Focus on artificial intelligence and privacy:** The AEPD has published guidelines and documents analyzing data processing in AI systems, emphasizing the need for ethical and auditable AI. It is also committed to the importance of transparency in artificial intelligence systems, publishing guidelines on how to guarantee this principle in the development and use of such technologies.
4. **Adaptation of organizations to new privacy paradigms:** Companies in Spain are working to adapt their risk management models to the challenges posed by AI, seeking to mitigate potential privacy impacts.
5. **Proactivity in digital compliance in risk management:** The crucial role of digital compliance for organizations to mitigate risks and define effective privacy and data protection strategies is recognized. In 2024, the AEPD had a proactive approach by releasing guidelines on biometric systems, addictive data patterns, and cookie usage, ensuring robust GDPR risk compliance across Spain.
6. **Development of regulatory sandboxes:** Controlled testing environments for the safe and responsible development of AI, known as sandboxes, are being promoted with the aim of fostering innovation while ensuring data protection and legal certainty.
7. **Companies preparing for the EU Artificial Intelligence Law:** Although the European AI law will come into force in 2026, Spanish authorities and companies are already working to adapt to its requirements, recognizing the importance of 'Digital Trust' and data protection in the use of emerging technologies.
8. **Focus on privacy and cybersecurity**: Digital law trends in Spain for 2024 highlight the digital economy, artificial intelligence, cybersecurity and data protection as key areas, underlining the need for companies to adapt to these areas to ensure regulatory compliance and user trust.

> *Currently, Spanish competent authorities are actively involved in overseeing the use of cybersecurity and artificial intelligence, ensuring that compliance with new key regulations such as the EU AI Act, DORA, and NIS2 upholds the fundamental principles of privacy, by stepping up enforcement through strict penalties to ensure that companies properly safeguard user information.*

SOFÍA ANIDO
Senior Lawyer
Digital Law
BDO Legal Spain
sofia.anido@bdo.es

View the recordings:

- EU Data Act – Exploring the Impact – A Trilogue of Webinars

General Information on the EU Data Act Webinars:

BDO Legal was pleased to present an insightful webinar series focused on the EU Data Act, organised by our international Tech & Data working group. These sessions explored the Act's implications for manufacturers, B2B dynamics, data access rights, and the evolving business models in this new data-driven landscape.

- The series commenced on **June 25** with **Matthias Niebuhr** from BDO Legal in Germany, who provided the critical obligations regarding the sharing of IoT data.
- The second webinar, held on **September 12**, featured **Micha Groeneveld** from BDO Legal Netherlands, who discussed regulations surrounding cloud switching.
- The final session took place on **November 14**, led by **Pieter Goovaerts** who examined unfair terms, model contracts, and standard clauses.

BDO Legal Spain moderated all sessions, ensuring a cohesive and engaging experience.

2025 Privacy & Data Protection Trends for the Netherlands:

In 2025, privacy and data protection in the Netherlands will face intensified scrutiny from authorities and collective actions. Key developments include:

1. **Stricter Cookie Policy Enforcement:** The Dutch Data Protection Authority (AP) is enhancing its oversight, exemplified by a €600,000 fine on Kruidvat for tracking cookies. Companies must find GDPR-compliant methods for data collection, especially as Google considers phasing out third-party cookies.
2. **AI Challenges**: Managing personal data in AI applications remains complex. The AP, along with other bodies like the Digital Infrastructure Inspectorate and the Netherlands Institute for Human Rights, will oversee AI compliance, leading to diverse regulatory approaches.
3. **Online Platform Regulation:** The Authority for Consumers and Markets (ACM) will expand its role, using tools like the Digital Services Act (DSA) to tackle issues such as fake reviews and geoblocking.
4. **Increase in GDPR Fines:** A rise in GDPR fines is anticipated, with recent penalties including €91 million for Meta and €290 million for Uber. GDPR compliance is crucial for businesses.
5. **Cyber Resilience Importance:** Cybercrime remains a major concern, with new European legislation like NIS2 and the Cyber Resilience Act adding layers to existing GDPR requirements. Companies must navigate multiple regulations, demanding increased attention and resources.

With growing consumer concerns about online privacy, regulatory bodies are intensifying their focus on compliance, particularly regarding online platforms, consumer rights, and AI, alongside stricter enforcement and heavier penalties.

Read the full insight:

- ESG: Technologie, data en privacy - BDO

The future of data protection in the EU is stricter enforcement, bigger penalties, and a greater focus on consumer privacy and AI. Compliance is no longer optional - it's essential for businesses to avoid serious consequences.

MICHA GROENEVELD
Lawyer
Tech & Data
BDO Legal Netherlands
micha.groeneveld@bdo.nl

BDO LEGAL GERMANY

Thoughts on 2025 Predictions:

BDO AG – A&A SERVICES: IT & CONTROLS ASSURANCE

Read the full insight:

- Data Protection & Data Security

BDO ROMANIA

Read the full insight:

- Website Privacy Notice and Cookies Policy - BDO

'From data protection to data use – we must navigate this paradigm shift.'

For the EU, this shift is central to the new Commission's agenda. Previously, the EU introduced extensive data legislation. While the AI Act focuses on risks, many laws aim to build a European Data Economy.

New acts like the EU Data Act, European Health Data Space Regulation, and draft Financial Data Access Regulation (FiDA) challenge GDPR's data minimization principle, promoting innovative data use. This is further supported by new cybersecurity laws such as NIS2, the Cyber Resilience Act, and DORA.

For companies, this feels overwhelming, presenting a 'have your cake and eat it too' dilemma, as new laws demand data availability while keeping GDPR intact.

The challenge for 2025 and beyond is to make this work for both the EU and businesses.

MATTHIAS NIEBUHR
Lawyer
Tech & Data
BDO Legal Germany
matthias.niebuhr@bdo.de

Data Protection Practices in Sub-Saharan Africa: Emerging Trends and Expectations for 2025

By 2024, 36 out of 55 African countries have enacted data protection laws. According to Data Protection Africa, Ethiopia, Namibia, and Malawi have draft laws under consideration. In North Africa, five countries (excluding Libya) have enacted such laws, while in sub-Saharan Africa, 30 out of 49 countries have done so. Countries are increasingly recognising the importance of data protection laws for attracting foreign investments and fostering global collaboration.

The number of data protection laws in Africa is expected to rise in 2025, with more countries likely to adopt legal frameworks through regulations or parliamentary enactments. A Data Protection Summit held in Uganda from December 2-5, 2024, focused on "Data Protection Compliance: A Catalyst for Africa's Digital Transformation." Key topics included balancing business needs with regulatory compliance and addressing privacy enforcement challenges.

Summit highlights emphasized:

- Developing localised data protection frameworks
- Investing in cybersecurity infrastructure
- Creating public awareness programs
- Establishing independent data protection authorities

The African Union is working to harmonise data protection approaches, promoting consistent regulatory standards, cross-border cooperation, and knowledge sharing.

The 2025 outlook for sub-Saharan Africa's data protection landscape includes:

- Increased regulatory sophistication
- Greater alignment with global standards
- Enhanced technological capabilities
- Emphasis on digital rights

Sub-Saharan Africa is advancing in developing robust data protection practices, with continued investment in legal frameworks, technology, and public awareness as essential for protecting digital rights and fostering trust in the digital ecosystem.

> *As organisations expand their digital reach globally, robust privacy practices are essential to ensuring the protection of data subjects and avoid non-compliance with data protection regulations across jurisdictions.*
>
> *In our increasingly interconnected digital world, collaborative efforts among nations are essential to protect personal information and enhance cyber safety.*

AKEEM OKUNOLA
Information Systems Auditor/Data Privacy Specialist

Malawi's Data Protection Act 2024 sets a new standard for data protection in the country. As organizations adapt to the new regulatory framework, we can expect to see increased investment in cybersecurity, improved data protection practices, and a growing awareness of the importance of data protection among individuals and businesses alike.

KUDAKWASHE CHIMA
BDO Malawi Audit Director
kchima@bdo.co.mw

2025 Privacy & Data Protection Trends for the DRC:

With a mobile telephony penetration rate reaching 59.1% and mobile Internet adoption limited to 31.5% at the end of 2023, the Democratic Republic of Congo (DRC) exemplifies a promising yet unevenly distributed digital transformation. These figures, sourced from ARPTC data, highlight not only the potential of a rapidly growing tech market but also the challenges of limited access for much of the population.

In this context, the implementation of the Code Numérique (Digital Code), a reference framework for data governance, marks a significant legislative milestone. However, its practical application remains hindered by inadequate infrastructure, limited awareness of privacy issues, and nascent levels of compliance. Without overcoming these obstacles, the emergence of a competitive and inclusive digital ecosystem risks being stifled.

In 2025, three major data privacy trends are expected to shape the landscape in the DRC:

1. Strengthened Legal and Regulatory Compliance

The adoption of the Code Numérique represents a major step forward for personal data governance in the DRC, establishing clear rules for the collection, processing, storage, and use of such data. Article 183 defines personal data categories, encompassing sensitive information such as identification, professional, banking, and biometric data—an indication of a comprehensive approach. The legislation also mandates prior declarations and, in some cases, specific authorisations (Articles 186-187) for high-risk processing activities, such as those involving genetic or biometric data or international transfers.

In response, local companies are progressively aligning their policies with the Code Numérique, often drawing inspiration from international standards like the GDPR. Compliance audits are increasingly common, ensuring adherence to obligations related to managing sensitive data. Efforts are also underway to align practices with specific provisions of the Code, such as securing data processing (Article 188) and ensuring subcontractor accountability.

However, effective implementation remains a significant challenge. Weak infrastructure and limited awareness slow the practical application of regulations. Moreover, both public and private entities need improved coordination to meet declaration and authorisation requirements for processing personal data.

> *Regarding the top three trends in privacy and data protection for 2025 specific to our country, the Democratic Republic of Congo (DRC), we propose to provide commentary on the **Digital Code of the DRC**, which represents a cornerstone of our evolving regulatory landscape. Additionally, we could highlight global trends such as the emphasis on **data sovereignty, privacy by design, and the challenges posed by decentralised technologies**, which are also highly relevant in our context.*

JOSUÉ MINSIME
BDO DRC IT Manager
josue.minsime@bdo-ea.com

2. Increased Awareness of Personal Data Protection

The culture of data privacy in the DRC is still in its infancy but is steadily gaining ground:

- Awareness campaigns aim to educate businesses and the public on key aspects, including consent, data rectification, and deletion.
- There is a marked rise in demand for specialized training for IT and legal teams, reflecting the growing importance of data protection in the Congolese digital landscape.

While these initiatives are promising, sustained coordination among stakeholders is essential to achieve lasting results.

3. Management of Cross-Border Data Transfers and Data Sovereignty

The Code Numérique imposes stringent restrictions on data transfers abroad. Article 201 stipulates that, whenever possible, personal data must be stored and/or hosted within the DRC. Exceptions do exist, allowing transfers to third countries or international organisations under strict security and data protection conditions, as approved by the Data Protection Authority.

This focus on limiting cross-border transfers underscores the country's push for digital sovereignty, translating into two key measures:

- The establishment of local data centres, such as Raxio Data Centre and OADC Texaf Digital-Kinshasa, offering modern solutions to mitigate risks associated with international transfers.
- The adoption of standard contractual clauses and specific agreements to align local practices with international standards while adhering to Congolese laws.
- Nonetheless, challenges persist in ensuring that local infrastructure meets growing connectivity and security needs while maintaining compliance with global standards.

A Rapidly Evolving Data Privacy Landscape

The trajectory of data privacy in the DRC is accelerating, guided by the Code Numérique and global trends. Strengthened compliance, heightened awareness, and the management of cross-border data transfers are emerging as key priorities for 2025. However, achieving true data sovereignty remains a significant challenge.

Modern infrastructure, such as Tier III-certified data centers like Raxio and OADC Texaf, represents a critical leap forward, but continued support is required to maximize their impact.

To navigate this evolving landscape effectively, businesses in the DRC must:

- Bolster internal capabilities through regular audits and tools aligned with the Code Numérique.
- Train and sensitise their teams to cultivate a robust data privacy culture.
- Leverage local solutions, such as national data centres, while forging strategic partnerships to ensure compliance with international standards.

> *By combining these efforts, businesses can not only meet legal obligations but also strengthen stakeholder trust, contributing to a secure, sovereign, and inclusive digital ecosystem in the DRC.*

BLAISE MBATSHI
BDO DRC Managing Partner
blaise.mbatshi@bdo-ea.com

BDO GHANA

2025 Privacy & Data Protection Trends for Ghana:

On issues of data privacy and sovereignty in Ghana, the growing emphasis is on data sovereignty, ethical considerations in data processing, and the importance of privacy by design due to the increasing reliance on technology and digital platforms.

As global attention on data governance intensifies, Ghana's approach aims broader conversation on data protection and privacy rights. It underscores the need for robust data protection frameworks to safeguard personal information in an increasingly digital world. The integration of privacy by design principles in new technologies as a best practice, ensuring that data protection is considered at every stage of technological development.

> *Embracing privacy is not just a choice, it's a responsibility.*

EMILE VORGBE
BDO Ghana Head of Audit
Emile.Vorgbe@bdo.com.gh

BDO BOTSWANA

2025 Privacy & Data Protection Trends for Botswana:

- **Implementing data protection frameworks** – Most entities are still grappling with improving their processes to accommodate increased data subject rights and adherence to lawful basis requirements.
- **Cross border transfer** – Where data is being transferred and or hosted is a topical issue with an inclination or expectation for data to be hosted locally. Stricter security measures are expected for cross border transfer.
- **Artificial intelligence and Machine learning considerations** – Due to associated ethical issues, there is an increased requirement to consider data subject rights to avoid infringing on the right to privacy.

> *Botswana Data Protection Law was originally assented in 2018 and effective 2021 granting consumers more control over their personal data. While the ACT has seen several extensions over the years, we expect that with recent updates in 2024, entities have no choice but to employ data protection frameworks with considerations for cross border transfer, cybersecurity, artificial intelligence considerations, data retention and destruction to ensure compliance and minimise regulatory fines and reputational risk. Banking on data subjects not exercising their rights under the law should not be a risk mitigation response.*

PHILIP LOMBARD
CEO
plombard@bdo.bw

BDO ZAMBIA

The Zambia Data Protection Act 2021 established a framework for safeguarding personal data and ensuring responsible handling by organisations. With its focus on transparency, accountability, and individuals' rights, the Act has become a cornerstone of Zambia's digital transformation. Organisations must now prioritise compliance by addressing areas such as data security, cross-border data sharing, and retention policies. As enforcement gains momentum, non-compliance poses significant risks, including regulatory penalties and reputational harm. The Act underscores that respecting data rights is not just a legal obligation but a critical driver of trust in Zambia's growing digital economy.

2025 Privacy & Data Protection Trends for Zambia:

- **Enhanced Regulatory Compliance and Enforcement:** The Zambia Data Protection Act 2021 has set a strong foundation for data privacy, and we anticipate stricter enforcement and compliance measures in 2025. Organisations will need to adopt more rigorous data protection frameworks to meet the evolving regulatory requirements. This includes ensuring transparency in data processing, obtaining explicit consent from data subjects, and implementing robust data security measures to avoid hefty fines and reputational damage.
- **Integration of Advanced Technologies:** The adoption of advanced technologies such as Artificial Intelligence (AI) and Privacy-Enhancing Technologies (PETs) will be crucial. AI can help in automating data protection processes and enhancing threat detection, while PETs like homomorphic encryption and federated learning will enable secure data processing without compromising privacy. These technologies will play a significant role in safeguarding personal data and ensuring compliance with privacy laws.
- **Focus on Cross-Border Data Transfers and Cybersecurity:** With the increasing globalisation of businesses, cross-border data transfers will become more prevalent. Ensuring the security of data during these transfers will be a critical focus area. Organisations will need to implement stringent cybersecurity measures to protect data from breaches and unauthorised access. This includes adopting zero-trust architectures and blockchain technologies forsecure transactions.

BDO SINGAPORE

Read the full insight:

- Data Security & Privacy in ESG - BDO

BDO INDONESIA

Read more of our recent insights:

- Navigating the Personal Data Protection Act (UU PDP)
- BDO Legal Talk: Alumni Association of the Faculty of Law, University Padjadjaran, discussing the Personal Data Protection Law

> *Personal Data Protection Law marks a pivotal shift in Indonesia's digital landscape, where safeguarding personal data is no longer an option but a necessity. By embracing this law, businesses can turn compliance into a strategic advantage—building trust, fostering innovation, and positioning themselves as leaders in a privacy-conscious world.*

EMAN ACHMAD
Legal Services Managing Partner
Head of BDO Legal Indonesia
eman.achmad@bdo.co.id

2025 Privacy & Data Protection Trends for Australia:

1. **Privacy-Enhancing Technologies (PETs):** Innovations such as data masking, differential privacy, and homomorphic encryption will gain traction. These technologies enable secure data processing without exposing sensitive information, supporting compliance with privacy laws and enhancing data security.
2. **Consumer Awareness and Demand for Control:** Australians are becoming more vigilant about their digital footprints, leading to higher expectations for plain-language privacy policies, simplified consent processes, and clear communication about data usage.
3. **Cloud Privacy and Security:** The growing reliance on cloud platforms will drive the adoption of stricter access controls, encryption, and data localisation measures. Organisations will need to ensure compliance with both domestic and international privacy standards.

Read more of our recent insights:

- A Guide to Privacy Practices for Businesses - BDO
- The Australian Government's Digital ID System: Enhancing Security and Privacy - BDO

Australia is currently in a privacy era where there is a shift towards prioritising privacy rights, in the digital era. Along side privacy reform we have seen AI and cyber security legislation that supports this shift.

Notably Attorney-General Mark Dreyfus, stated during the discussion of the Privacy and Other Legislation Amendment Bill 2024: "[These reforms] begin the work of bringing Australia's privacy protection framework into the digital age [and] re-affirm the Government's view that entities have a responsibility to protect Australians' personal information and not treat it merely as a commercial asset.

GEORGE CHOUEIFATE
Advisory and Cyber Security Senior Manager
George.Choueifate@bdo.com.au

It is an exciting time of change here in Australia. Significant change to support legislative amendments will be underway in 2025.

JULIE KILNER
Digital Director
julie.kilner@bdo.com.au

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.