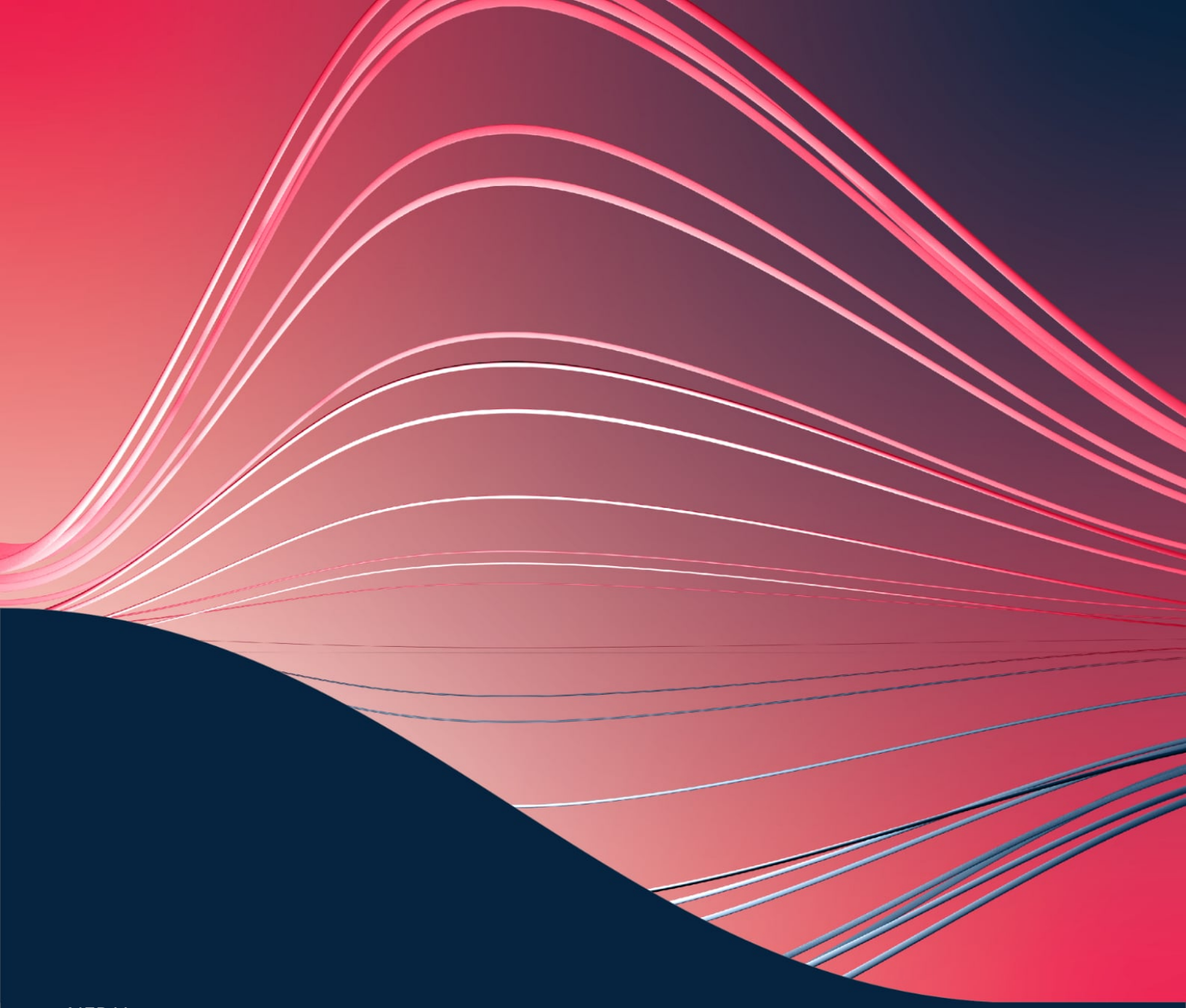


NEPAL

Data Protection Laws of the World

DLA PIPER

Introduction

Welcome to the 2025 edition of DLA Piper's Data Protection Laws of the World Handbook. Since the launch of our first edition in 2012, this comprehensive guide has been a trusted resource for navigating the complex landscape of privacy and data protection laws worldwide. Now in its fourteenth edition, the Handbook has grown to provide an extensive overview of key privacy and data protection regulations across more than 160 jurisdictions. As we step into 2025, the global landscape of data protection and privacy law continues to evolve at an unprecedented pace. With new legislation emerging in jurisdictions around the world, businesses face a growing need to stay informed and agile in adapting to these changes. This year promises to bring new developments and challenges, making the Handbook an invaluable tool for staying ahead in this ever-changing field.

Europe

Established data protection laws in Europe continue to evolve through active regulatory guidance and enforcement action. In the United Kingdom, the UK government has proposed reforms to data protection and e-privacy laws through the new Data (Use and Access) Bill ("**DUAB**"). The DUAB follows the previous government's unsuccessful attempts to reform these laws post-Brexit, which led to the abandonment of the Data Protection and Digital Information (No.2) Bill ("**DPDI Bill**"), in the run-up to the general election. Although the DUAB comes with some bold statements from the government that it will *"unlock the power of data to grow the economy and improve people's lives"*, the proposals represent incremental reform, rather than radical change.

United States

In the United States, legislation on the federal and in particular state level continues to evolve at a rapid pace. Currently, the US has fourteen states with comprehensive data privacy laws in effect and six state laws will take effect in 2025 and early 2026. Additionally, at the federal level, the new administration has signaled a shift in enforcement priorities concerning data privacy. Notably, there is a renewed focus on the regulation of artificial intelligence (AI), with an emphasis on steering away from regulation and promoting innovation. This includes the revocation of previous executive orders related to AI and the implementation of new directives to guide AI development and use.

In the realm of children's privacy, many of the new administration's supporters in Congress have indicated a desire to make the protection of children on social media a top priority, and new leadership at the Federal Trade Commission (FTC) appears aligned on this goal, albeit with a willingness to take another look at the recently adopted amendments to the Children's Online Privacy Protection Act (COPPA) Rule. Health data

privacy remains a critical concern, with a handful of states following Washington state's lead in enhancing or adopting health data privacy laws. On the international data transfer front, Executive Order (E.O.) 14117 " Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" as supplemented by the DOJ's final Rule will impact companies transferring data into certain jurisdictions, such as China, Iran and Russia. Another area of focus for companies with an EU presence will be the Trump administration's approach to the Privacy and Civil Liberties Oversight Board, as it is a critical pillar of the EU/UK/Swiss-US Data Privacy Framework.

Asia, the Middle East, and Africa

Nowhere is the data protection landscape changing faster – and more fundamentally – than in Asia, with new laws in India, Indonesia, Australia and Saudi Arabia, as well continued new data laws and regulations in China and Vietnam. The ever-evolving data laws, as well as the trend towards regulating broader data categories (beyond personal data), in these regions continue to raise compliance challenges for multi-national businesses.

Emerging trends in data governance

Unlocking data, regulating the relentless advance of AI, creating fairer digital markets and safeguarding critical infrastructure against the ever growing cyber threat, continue to impact and overlap with the world of data protection and privacy. Perhaps most notably, the EU have introduced a raft of new laws forming part of its ambitious digital decade, which will bring huge change to businesses operating within the EU. With the rapid adoption of artificial intelligence enabled solutions and functionality, data protection supervisory authorities have been closely scrutinising the operation of AI technologies and their alignment with privacy and data protection laws. For businesses, this highlights the need to integrate date protection compliance into the core design and functionality of their AI systems. In the midst of this, the privacy community found itself at the centre of an emerging debate about the concept of 'AI governance'. This is not a surprising development – AI systems are creatures of data and the principle-based framework for the lawful use of personal data that sits at the heart of data protection law offers a strong starting point for considering how to approach the safe and ethical use of AI. As AI technologies advance, so will regulatory expectations. It is expected that regulatory scrutiny and activity will continue to escalate and accelerate in tandem with the increase in integration of powerful AI models into existing services to enrich data. Whilst privacy professionals cannot tackle the AI challenge alone, expect them to continue to be on the front lines throughout 2025 and beyond.

Disclaimer

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.

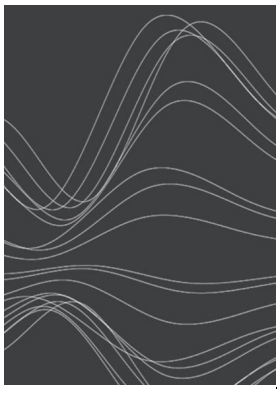
Africa key contact

Monique Jefferson
Director
monique.jefferson@dlapiper.com
Full bio

Americas key contact

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

Asia Pacific key contact



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

Europe key contacts

Andrew Dyson
Partner
andrew.dyson@dlapiper.com
Full bio

Ewa Kurowska-Tober
Partner
Head of Intellectual Property and Technology, Poland
ewa.kurowska-tober@dlapiper.com
Full bio

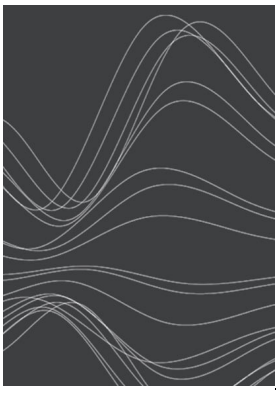
John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Middle East key contact

Rami Zayat
Partner
rami.zayat@dlapiper.com
Full bio

Editors

Kate Lucente
Partner
kate.lucente@us.dlapiper.com
Full bio



Lea Lurquin
Associate
lea.lurquin@us.dlapiper.com
Full bio

Nepal

LAST MODIFIED 20 JANUARY 2025

Data protection laws

1. Individual Privacy Act, 2018 (2075) ("**Privacy Act**")
2. Individual Privacy Regulation, 2020 (2077) ("**Privacy Regulation**")
3. National Penal Code, 2017 (2074) ("**Penal Code**")
4. Advertisement Act, 2019 (2076) ("**Advertisement Act**")
5. Advertisement Regulation, 2020 (2076) ("**Advertisement Regulation**")
6. National Broadcasting Regulation 1995 (2052) ("**National Broadcasting Regulation**")

Definitions

Definition of Personal Data

Privacy Act defines "Personal information" as the following information related to any person:

- his or her caste, ethnicity, birth, origin, religion, color or marital status;
- his or her education or academic qualification;
- his or her address, telephone or address of electronic letter (email);
- his or her passport, citizenship certificate, national identity card number, driving license, voter identity card or details of identity card issued by a public body;
- a letter sent or received by him or her to or from anybody mentioning personal information;
- his or her thumb impressions, fingerprints, retina of eye, blood group or other biometric information;
- his or her criminal background or description of the sentence imposed on him or her for a criminal offence or service of the sentence;
- matter as to what opinion or view has been expressed by a person who gives professional or expert opinion, in the process of any decision.

Definition of Sensitive Personal Data

Privacy Act has listed following information as the “sensitive information”:

- his or her caste, ethnicity or origin;
- political affiliation;
- religious faith or belief;
- physical or mental health or condition;
- dexual orientation or event relating to sexual life;
- fetails relating to property.

National data protection authority

Not applicable.

Registration

Not applicable.

Data protection officers

Not applicable.

Collection and processing

Collection

The collection of data by any public body or body corporate is allowed with the consent of the concerned person. In addition to this, the Privacy Act provides an exclusive provision in the context of the collection of data. It provides that no one except the official authorized under law or the person permitted by such official shall collect, store, protect, analyze, process or publish the personal information of any person. Officer authorized under the law means those officials who have been authorized by other laws to collect the information such as investigating authority, collection of prescribed information by the civil service officer.

Processing

Privacy Act prohibits to process the sensitive information. However, the sensitive information can also be processed in following circumstances:

- in the course of alleviation of disease, public health protection, disease identification, health treatment, management of health institution and providing health service by the health worker, without insulting or letting the concerned person feel inferior;

- if the concerned person has published the information himself or herself.

The revised Draft Information Technology and Cyber Security Bill, 2024 ("**IT Bill**"), which is yet to be passed and made into law by the Parliament, has also added provisions relating to privacy (Section 80). It states that personal details collected from an individual in an information technology system shall not be used, disseminated, or exchanged for any purposes other than the disclosed purpose without the consent of the data subject. It also stipulates that personal information collected and stored for a specific purpose shall be destroyed, with assurance to the data subject, within 30 days after fulfillment of that purpose. The applicable punishment for violation of this provision will result in fine of up to NPR 5,00,000 or three years of imprisonment or both.

Transfer

The 11th amendment to National Broadcasting Regulation which has been effective from 3rd March 2022, has mandated Over the Top ("**OTT**") service providers to store their customer data within servers in Nepal. Such requirements only extend to OTT service providers and the regulation has defined OTT as "*the service of delivering any program according to the consumer's demand through the internet and without the use of cable or satellite television, and the term also refers to media streaming services on other platforms via the internet*." However, the National Broadcasting Regulation is silent on the methods / procedure / requirements for the transfer of such data outside Nepal.

Furthermore, the Information Technology Bill, 2019 (2075) (which is currently tabled in the parliament of Nepal), if implemented in its current form, then the prescribed data held by governmental, public, financial, and health-related authorities would be prohibited for export outside Nepal. Also, Bill to amend Record Protection Act 1989 (2046) would further prohibit to export records of national importance outside Nepal.

Security

The collected data should only be used for the purpose for which such data have been collected. Further, the Privacy Act obligates the public body which has the collected information, to make appropriate arrangements for the protection of collected information.

Breach notification

Certain offenses under the Privacy Act, and all offenses under the IT Bill and the Social Media Bill are state-party offenses listed under Schedule-1 of the National Criminal Procedure Code, 2017 ("**NCP**"). Pursuant to Section 4 of the NCP, anyone aware of a Schedule-1 offense must file a First Information Report (FIR) which may be submitted in written, verbal, or electronic form and should include any available evidence, with the prescribed format under Schedule-5 of the NCP. The obligation to notify a breach is also mandated by Section 96 of the National Penal Code, 2017 which states that a person under the legal duty to provide information regarding an offence when aware that such an offense has been committed, shall provide the concerned authority with such information.

Enforcement

As aforementioned, the prevailing laws have not designated Data Protection Authority. Nonetheless, the Privacy Act and Criminal Code provide a complaint mechanism.

Complaint of the offense under the Privacy Act is processed either by filling a plaint at the concerned district court by the concerned person or filling FIR at the relevant police office. In relation to the latter one, the concerned police office through the government office would file a charge sheet in the concerned district court. Such procedure of directly filing a complaint at the concerned district court or police office is determined based on the nature of the offense. In relation to an offense under the Criminal Code, the FIR process as aforementioned is adopted.

Electronic marketing

The matters related to marketing are regulated by the Advertisement Act and Advertisement Regulation. The definition as provided under the Advertisement Act also includes inter alia advertisement done through electronic medium, online or social media.

Advertisement-oriented SMS or Email cannot be sent to any person without obtaining the said concerned person's consent.

Online privacy

Every person has the right to privacy in terms of data available in electronic means. Such data cannot be used or share such data without the consent of the concerned person. In relation to the cookies and location data, there is no exclusive provision for it. However, if a data subject's personal information or location data is collected using cookies or otherwise, the concerned entity must adhere to the Privacy Act and further such information must be used for the same purpose as it was collected for.

The Directives for Managing the Use of Social Networks, 2023 ("**Social Network Directives**"), prohibits users from breaching personal privacy, including editing, publishing, or broadcasting private photographs and videos without permission, except for content of a public nature. Violation of the Social Media Directives may lead to penalties under the Electronic Transactions Act, 2008, including a fine of up to NPR 50,000, imprisonment for up to six months, or both, depending on the severity of the offense.

The Social Media (Use and Regulation) Management Bill, 2024 ("**Social Media Bill**") has received approval from the council of ministers and may either be introduced via ordinance or be tabled in the Parliament. Section 16 of the Social Media Bill mandates social media platforms to adopt necessary security measures to safeguard privacy of users' personal information and ensure that such information is not publicly disclosed or used for any other purpose. Any social media platform acting in contravention to this requirement may be subject to a fine of up to NPR 10,00,000.

Section 42 of the Social Media Bill prohibits use of social media to breach a person's privacy, including privacy of life, family, residence, property, documents, data, correspondence, or information. A person committing an offense under this section

shall be referred to the concerned authority for further investigation and punishment in accordance with the prevailing law.

Data protection lawyers

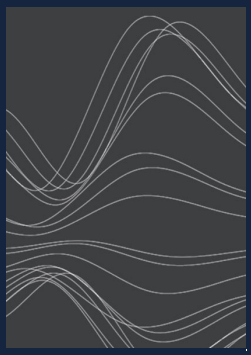
Anup Raj Upreti
Managing Partner
Pioneer Law Associates
anup@pioneerlaw.com
View bio

Suman Siwakoti
Senior Associate
Pioneer Law Associates
suman@pioneerlaw.com
View bio

Sujan Shrestha
Associate
Pioneer Law Associates
sujan.shrestha@pioneerlaw.com
View bio

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com