SINT MAARTEN

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.

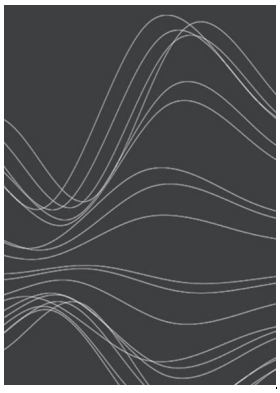
Africa key contact

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

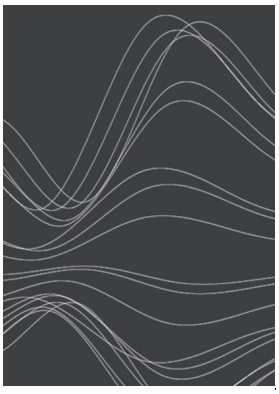
John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

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

Sint Maarten

LAST MODIFIED 10 FEBRUARY 2025

Data protection laws

- National ordinance personal data protection *(Landsverordening bescherming persoonsgegevens*, National Gazette 2010, Consolidated text no. 2) "(National Ordinance Personal Data Protection");
- General Data Protection Regulation (the "GDPR") – a regulation of the European Union which became effective on May 25, 2018 – may have implications for a data controller / data processor as the extra-territorial reach of the GDPR is not only relevant to businesses established in the European Union but also to international businesses established in Sint Maarten which offer goods or services to individuals in the European Union or monitor their behaviour in the European Union.

Definitions

Definition of Personal Data

National Ordinance Personal Data Protection

According to the Explanatory Memorandum on the National Ordinance Personal Data Protection the term personal data has a broad meaning. This does not only concern data that can identify a person, but concerns any data that can be associated with a particular person; it is foreseeable that under certain circumstances data can be traced to one person through systematic comparison and lengthy investigations. Personal identifiable confidential data is therefore not only limited to home address, email address, telephone number, membership number and/or identity number.

GDPR

Personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of Sensitive Personal Data

National Ordinance Personal Data Protection

A person's religion or belief, race, political views, health, sexual life as well as personal data concerning membership of a trade union.

GDPR

Data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

National data protection authority

National Ordinance Personal Data Protection

The Personal Data Protection Committee as referred to in article 42 of the National Ordinance Personal Data Protection.

GDPR

An independent public authority established by a Member state pursuant to article 51 of the GDPR (Article 4(21), GDPR). The authority is responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the EU.

Registration

National Ordinance Personal Data Protection

No registration required.

GDPR

Article 30 GDPR requires companies to keep an internal electronic registry, which contains the information of all personal data processing activities carried out by the company.

Data protection officers

National Ordinance Personal Data Protection

Pursuant to article 13 of the National Ordinance Personal Data Protection the responsible party shall execute appropriate technical and organizational measures to secure personal data against loss or any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking account of the technical state of the art and the costs of execution, in view of the risks associated with that processing and the nature of the data to be protected. The measures shall be aimed partly at preventing unnecessary gathering and further processing of personal data.

Besides the measures above, the National Ordinance Personal Data Protection does not contain any clauses on any type of registration, filings of documents to any public agency or having a mandatory data protection officer in place.

GDPR

The appointment of a data protection officer under the GDPR is only mandatory in three situations:

- When the organisation is a public authority or body;
- If the core activities require regular and systematic monitoring of data subjects on a large scale; or
- If the core activities involve large scale processing of special categories of personal data and data relating to criminal convictions.

Collection and processing

National Ordinance Personal Data Protection

Collection: a natural or legal person, public authority, agency or other body which who has control over a person registration.

Processor: a natural or legal person, public authority, agency or other body which who owns all or part of the has equipment in his possession, with which a personal registration of which he is not the holder.

GDPR

Collection: a natural or legal person, public authority, agency or other body that collect personal data and use it for certain purposes, like a website that markets to users based on their online behaviour.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority.

Transfer

National Ordinance Personal Data Protection

Contains no clauses.

GDPR

The GDPR restricts transfers of personal data outside the European Economic Area, or the protection of the GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.

Security

National Ordinance Personal Data Protection

Pursuant to article 13 of the National Ordinance Personal Data Protection the responsible party shall execute appropriate technical and organizational measures to secure personal data against loss or any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking account of the technical state of the art and the costs of execution, in view of the risks associated with that processing and the nature of the data to be protected. The measures shall be aimed partly at preventing unnecessary gathering and further processing of personal data.

GDPR

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (article 32 GDPR).

Breach notification

National Ordinance Personal Data Protection

Contains no specific clauses.

GDPR

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with article 55 GDPR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Enforcement

National Ordinance Personal Data Protection

Pursuant to article 60 the responsible party who acts in contravention of the provisions of the National Ordinance Personal Data Protection may be penalized by the Sint Maarten committee of data protection with a financial penalty in the minimum amount of Naf. 1,000 (USD 571.43) maximum amount of Naf. 500,000.00 (USD. 277,777.78).

GDPR

The GDPR holds a variety of potential penalties for businesses.

For example, article 77 of GDPR states that:

"Every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of

the alleged infringement if the data subject considers that the processing of personal data relating him or her infringes this Regulation."

Additionally, article 79 of the Regulation states that *"such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence."*

Penalties

Compensation to Data Subjects. One penalty that may be imposed is compensation to, as stated in article 82 of the Regulation, *"Any person who has suffered material or non-material damage as a result of an infringement of this Regulation"* for the damage they' ve suffered.

Fines

Article 83 of GDPR specifies a number of different fines that may vary based on the nature of the infraction, its severity, and the level of cooperation that "data processors" (i.e. you) provide to the "supervisory authority." Less severe infringements may incur administrative fines of up to 10,000,000 Euros or 2% of your total worldwide annual turnover for the preceding year (whichever is greater), while more severe infractions may double these fines (20,000,000 or 4% annual turnover).

Individual Member States of the EU may have additional fines and penalties that may be applied as well. However, these additional penalties are not specifically listed in the text of the Regulation since they're up to the individual EU nations to set—the only guidelines in article 84 of GDPR are that *"Such penalties shall be effective, proportionate and dissuasive"* and that *"Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018."*

Electronic marketing

National Ordinance Personal Data Protection

N/A.

GDPR

Under article 22 GDPR organizations cannot send marketing emails without active, specific consent.

Companies can only send email marketing to individuals if:

- The individual has specifically consented.
- They are an existing customer who previously bought a similar service or product and were given a simple way to opt out.

Online privacy

National Ordinance Personal Data Protection

Contains no specific clauses.

GDPR

Cookies, insofar as they are used to identify users, qualify as personal data and are therefore subject to the GDPR. Companies do have a right to process their users' data as long as they receive consent or if they have a legitimate interest.

Location data, the GDPR will apply if the data collector collects the location data from the device and if it can be used to identify a person.

If the data is anonymized such that it cannot be linked to a person, then the GDPR will not apply. However, if the location data is processed with other data related to a user, the device or the user's behavior, or is used in a manner to single out individuals from others, then it will be "personal data" and fall within the scope of the GDPR even if traditional identifiers such as name, address etc. are not known.

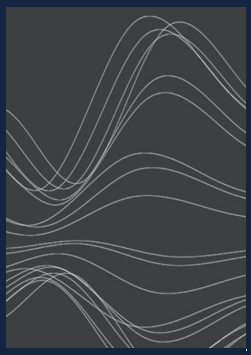
Data protection lawyers

Maarten Willems
Associate Partner
Attorney
HBN Law & Tax
maarten.willems@hbnlawtax.com
View bio

Misha Bemer
Partner
HBN Law & Tax
misha.bemer@hbnlawtax.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