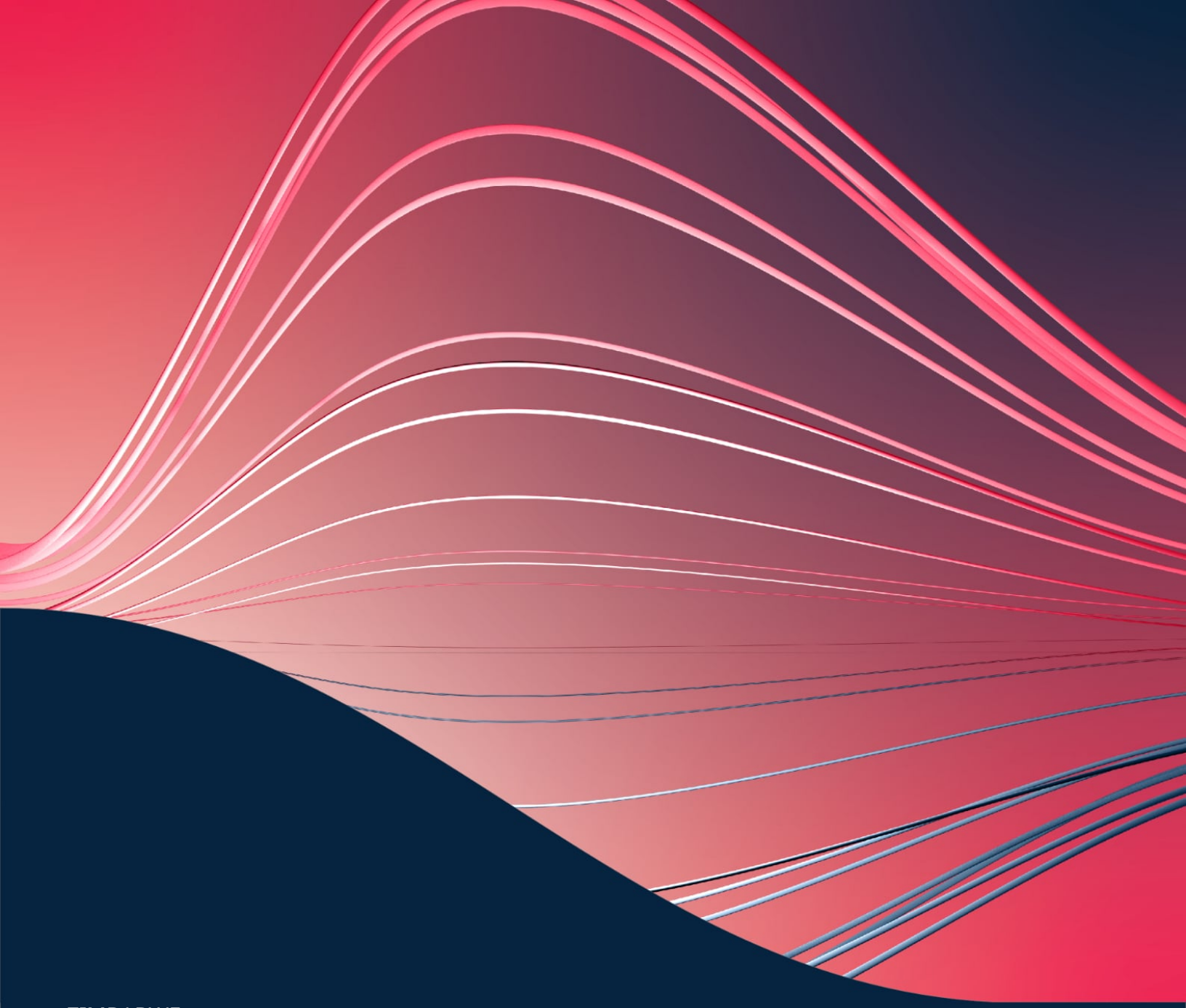


ZIMBABWE

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.

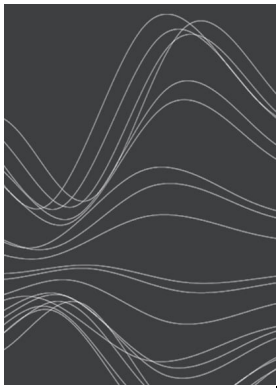
Africa key contact

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

Americas key contact

Andrew Serwin
Partner
andrew.serwin@us.dlapiper.com
Full bio

Asia Pacific key contact



Carolyn Bigg
Partner
carolyn.bigg@dlapiper.com
Full bio

Europe key contacts

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

Ewa Kurowska-Tober
Partner
ewa.kurowska-tober@dlapiper.com
Full bio

John Magee
Partner
john.magee@dlapiper.com
Full bio

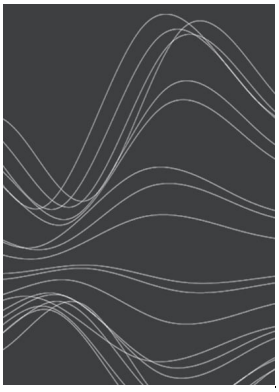
Middle East key contact

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

Editors

James Clark
Partner
james.clark@dlapiper.com
Full bio

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



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

Zimbabwe

LAST MODIFIED 27 JANUARY 2025

Data protection laws

- Cyber and Data Protection Act [Chapter 12:07] (the "**Act**"); and
- Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations, 2024 (the "**Regulations**").

Definitions

Definition of personal data

According to the Act, "personal information" means information relating to a data subject, and includes:

- the person's name, address or telephone number;
- the person's race, national or ethnic origin, colour, religious or political beliefs or associations;
- the person's age, sex, sexual orientation, marital status or family status;
- an identifying number, symbol or other particulars assigned to that person;
- fingerprints, blood type or inheritable characteristics;
- information about a person's health care history, including a physical or mental disability;
- information about educational, financial, criminal or employment history;
- opinions expressed about an identifiable person;
- the individual's personal views or opinions, except if they are about someone else; and
- personal correspondence pertaining to home and family life.

Definition of sensitive personal data

According to the Act, "sensitive data" refers to:

- information or any opinion about an individual which reveals or contains the following—
- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sex life;
- criminal educational, financial or employment history;
- gender, age, marital status or family status;
- health information about an individual;
- genetic information about an individual; or
- any information which may be considered presenting a major risk to the rights of the data subject.

Definition of personal life data

There is no definition of "Personal Life Data" in the Act or the Regulations.

Definition of biometric personal data

According to section 2 of the Regulations, "biometric data" means physiological characteristics which are related to a data subject and include but are not limited to the following:

- Fingerprints;
- Palm veins;
- Face recognition.

Definition of publicly available personal data

There is no definition of "Publicly Available Personal Data" in the Act or in the Regulations.

National data protection authority

The Data Protection Authority, also referred to as the "Authority," is the Postal and Telecommunications Regulatory Authority of Zimbabwe (the "**Authority**"). It was established by the Postal and Telecommunications Act [Chapter 12:05] and designated as the Data Protection Authority by the Act.

Registration

Section 3 of the Regulations state that anyone who processes personal information to decide the means, purpose, or outcome of processing, to decide what or whose data to collect, or to obtain commercial gain from processing data, must apply for a license with the Data Protection Authority.

The exemptions are data controllers who process personal data for the following purposes are exempt from licensing, but must register with the Authority:

- Law enforcement;
- Journalistic, historical, or archival purposes The Authority maintains a register of all licensed and registered data controllers.

Data protection officers

Data Protection Officers Data controllers are required to appoint a data protection officer ("**DPO**") and notify the Authority in writing using Form DP2. The Authority must also be notified of any changes to the DPO's contact information, dismissal, or resignation. DPOs must have the following qualifications:

- Skill, qualifications, or experience in data science, data analytics, information security systems, information systems audit, law, audit, or any other relevant qualification;
- Knowledge of national data protection laws and practices;
- Understanding of the data controller's business operations and processing activities;
- Certification through a course approved by the Authority DPOs have the following duties:
  - Monitoring compliance with the Act, the Regulations, and organizational data protection policies;
  - Managing internal data protection activities;
  - Raising awareness of data protection;
  - Training staff on data protection;
  - Conducting internal data protection compliance audits;
  - Dealing with requests from the Authority and data subjects;
  - Advising employees on their data protection obligations;
  - Advising on and monitoring data protection impact assessments;
  - Working with the Authority; and
  - Acting as the contact point for data subjects.

Collection and processing

Characteristics for processing publicly available personal data

This is not addressed by the Act or the Regulations.

Characteristics for processing sensitive personal data

According to section 11 of the Act, written consent from the data subject is required to process sensitive data. This consent can be withdrawn at any time without explanation and free of charge.

The Minister responsible for the Cyber Security and Monitoring Centre may give directions on processing sensitive data related to national security or state interests.

Several exceptions to the written consent requirement are outlined in the Act, including:

- Processing necessary to carry out the controller's obligations and rights in employment law;
- Processing necessary to protect the vital interests of the data subject or another person when the data subject is incapable of giving consent;
- Processing carried out by a foundation, association, or other non-profit for political, philosophical, religious, health-insurance, or trade-union purposes, provided the processing relates only to members or those with regular contact and the data is not disclosed to third parties without consent;
- Processing necessary to comply with national security laws;
- Processing necessary for the establishment, exercise, or defence of legal claims;
- Processing of data made public by the data subject;
- Processing necessary for scientific research, with conditions specified by the Authority;
- Processing authorized by law for reasons of substantial public interest.

Characteristics for processing personal data of persons with incapacity or limited capacity and minors under the age of 16

The processing of children’s data is subject to the provisions of section 26 of the Act, which addresses the representation of data subjects who are children. Characteristics for processing personal data of persons with incapacity or limited capacity and minors under the age of 16.

Where the data subject is a child, their rights may be exercised by their parents or legal guardian.

Data subjects who are physically, mentally, or legally incapable of exercising their rights may exercise them through a parent, guardian, or as provided by law or a court.

When processing children's information, data controllers must:

- Obtain consent from the child's parent or legal guardian;

- Make reasonable efforts to verify that consent is given or authorized by the parent or legal guardian;
- Adhere to all data processing principles;
- Conduct regular data protection impact assessments to identify and mitigate privacy risks to children;
- Ensure data protection by design and data protection by default;
- Avoid subjecting children's data to automated decision making that affects their rights.

Characteristics for processing biometric personal data

According to section 12 of the Act, Processing genetic, biometric, and health data is prohibited unless the data subject gives written consent.

The written consent requirement for genetic, biometric, and health data can be withdrawn at any time without explanation and free of charge.

Several exceptions to the written consent requirement for genetic, biometric, and health data are outlined in the Act, including:

- Processing necessary to carry out the controller's obligations and rights in employment law;
- Processing necessary to comply with national security laws;
- Processing necessary for the promotion and protection of public health;
- Processing required by law for reasons of substantial public interest;
- Processing necessary to protect the vital interests of the data subject or another person when the data subject is incapable of giving consent;
- Processing necessary for the prevention of imminent danger or the mitigation of a criminal offense;
- Processing of data made public by the data subject;
- Processing necessary for the establishment, exercise, or defence of legal rights;
- Processing required for scientific research;
- Processing necessary for preventative medicine, medical diagnosis, the provision of care or treatment, or the management of healthcare services;
- Health-related data may only be processed under the responsibility of a healthcare professional unless the data subject provides written consent or the processing is necessary for the prevention of imminent danger or the mitigation of a criminal offense.

Processing of personal data by an authorized person assigned by the processor of data

According to section 17 of the Act, only persons acting under the authority of the controller, as well as the processor themselves may process data as instructed by the controller.

Blocking or destruction of personal data

This is not addressed by the Act or the Regulations.

Transfer

According to section 28 of the Act, data controllers may not transfer personal information to a third party in a foreign country unless an adequate level of protection is ensured. This adequacy is assessed based on the circumstances surrounding the transfer, including the nature of the data, the purpose and duration of processing, the recipient, the recipient country's data protection laws, and professional rules and security measures.

Data controllers must notify the Authority of any intention to transfer or share data outside of Zimbabwe.

Security

Section 13 of the Act states that Data controllers are responsible for processing personal information lawfully, fairly, and transparently, and for taking all necessary measures to comply with the Act and Regulations.

Data controllers must take appropriate technical and organizational measures to protect personal data from negligent or unauthorized destruction, loss, alteration, access, or processing.

Security measures must ensure an appropriate level of security considering technological development, implementation costs, the nature of the data, and potential risks to the data subject.

The Authority may issue information security standards for processing activities.

Data controllers must appoint data processors who provide sufficient guarantees regarding technical and organizational security measures and must enter into a written contract or legal instrument with the processor ensuring security measures are maintained.

Data controllers must take all appropriate technical and organizational measures to safeguard data security, integrity, and confidentiality, ensuring an appropriate level of security.

Technical and organizational security measures include:

- Conducting risk assessments;
- Developing and implementing organizational policies;

- Implementing appropriate physical and technical measures for all data phases;
- Data controllers and processors may implement additional security measures depending on the circumstances and risks associated with the processing.

Breach notification

Data controllers must report data breaches to the Authority within 24 hours of becoming aware of a breach affecting the data they or their processor handles.

If a breach poses a high risk to individuals' rights and freedoms, the data controller must inform the affected data subjects within 72 hours.

Enforcement

The Data Protection Authority is responsible for enforcing the Act and Regulations. The Authority has the following functions:

- Regulating personal information processing by establishing conditions for lawful processing;
- Promoting and enforcing fair data processing;
- Issuing opinions on privacy protection matters;
- Submitting administrative acts that violate privacy protection principles to the courts;
- Advising the Minister on privacy and access to information;
- Conducting inquiries or investigations;
- Receiving and investigating complaints;
- Conducting research and advising the Minister on international best practices;
- Facilitating cross-border cooperation in privacy law enforcement.

Electronic marketing

This is not addressed by the Act or the Regulations. However, obtaining user consent through appropriate disclaimers is recommended.

Online privacy

There is no regulation on cookies and location data. However, it is advisable to obtain user consent, such as through appropriate disclaimers.

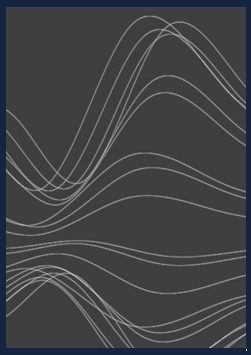
Data protection lawyers

Farai Nyabereka
Partner
Manokore Attorneys
farai.nyabereka@ma.dlapiperafrica.com
View bio

Steve Chikengezha
Senior Associate
Manokore Attorneys
steve.chikengezha@ma.dlapiperafrica.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