World Federation of Advertisers

WFA Global Privacy Map

An overview of data protection & privacy regulation in key markets

Last updated: January 2019

WFA Global Privacy Map

In May 2018, the EU's General Data Protection Regulation (GDPR) required companies to make major changes to the way they collect and process consumer data.

Since then, new (and revised) privacy laws have been emerging in many countries across the world. Many of these laws are evidently inspired by GDPR, pointing to a trend towards a 'GDPR standard' emerging globally.

However, the picture is not that simple. Although some laws borrow heavily from GDPR, in many countries significant differences remain. The regulatory landscape is still fragmented: we are still far from seeing one global standard emerging across all markets.

This guide aims to identify some of the privacy trends emerging across a number of key markets for advertisers and how they compare to the 'GDPR standard'.

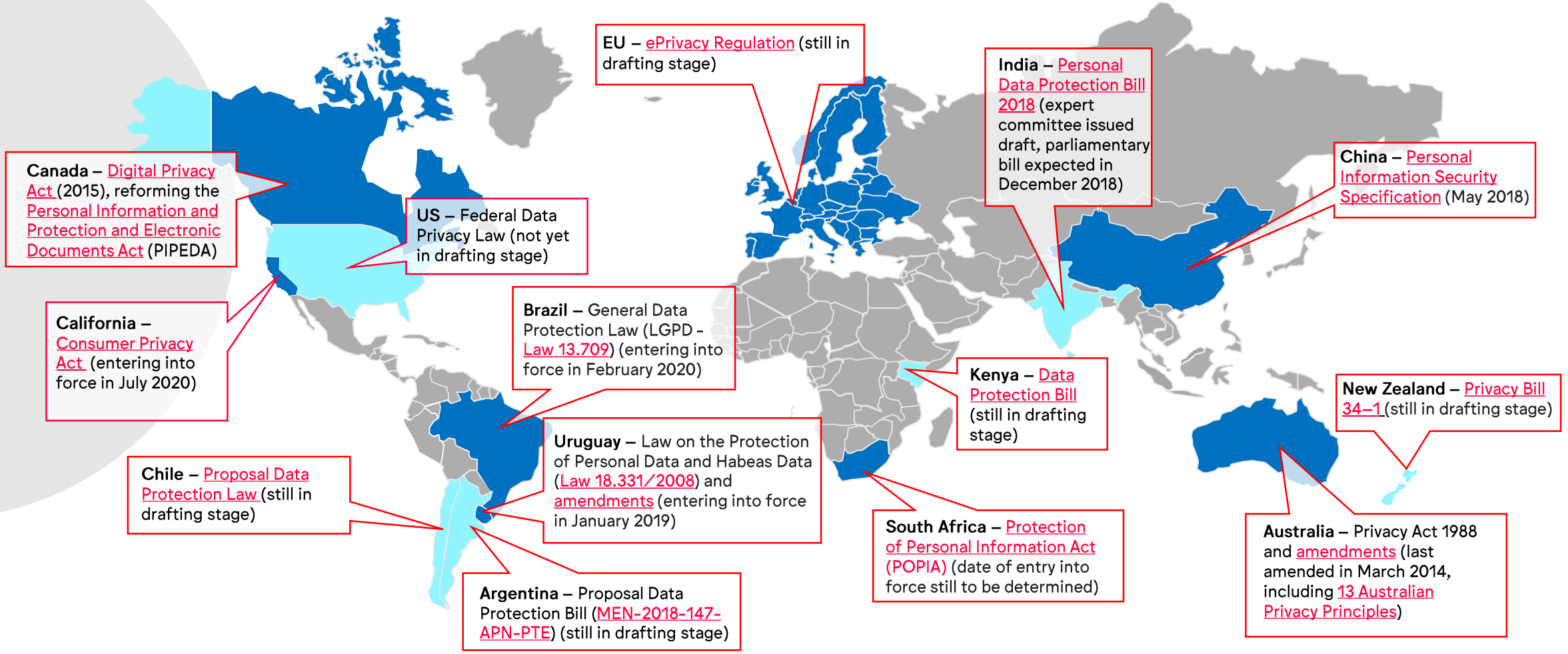
This is not designed to be an exhaustive list of all legislative developments in the world and it is intended to complement, rather than substitute or constitute legal advice. For more information or to find out about any country which is not represented on this map, please contact Catherine Armitage (c.armitage@wfanet.org).

WFA

Most recent legislative developments in key markets*

Regulation in place / due to come into force

Regulation under discussion



* Focus only on certain key markets for global advertisers – this is not an exhaustive list of all legislative developments in all countries in the world. For information about any country which is not represented on this map, please contact Catherine Armitage (c.armitage@wfanet.org)

The GDPR standard

Key provisions relevant to marketing

Territorial scope (Article 3):

Applies worldwide to all firms which offer goods or services to consumers in the EU or monitor the behaviour of people located in the EU.

Basis for processing (Article 6):

6 legal bases, applicable to all categories of data:

- Consent
- To fulfil contractual agreement/requirements
- To comply with a legal obligation
- To act in the vital interests of a data subject
- For the purposes of the legitimate interests of the controller or by a third party (provided data subject rights are not affected)
- If processing is in the public interest

Children's data (Article 8):

Parental consent is required to process the personal data of children under 16 years (though Member States are able to lower this age threshold to a minimum of 13 years).

Data breach notification (Article 33):

Must notify data breaches to DPA within 72 hours.

Right to erasure (Article 17):

Right to have personal data erased or rectified.

Sanctions (Articles 83, 84):

Fines up to €20m or 4% of global annual revenue (whichever is higher).

Data protection officer (Articles 37, 38, 39):

Must appoint DPO when regularly engaging in systematic monitoring or processing data on a large scale.

Data protection impact assessments (Article 35):

Must conduct impact assessments when there is a high privacy risk.

The spread of the GDPR standard

Laws which are heavily influenced* by GDPR

(Proposed) framework is similar to GDPR*

Canada – Digital Privacy Act (2015), reforming the Personal Information and Protection and Electronic Documents Act (PIPEDA)

US – Federal Data Privacy Law (not yet in drafting stage)

California – Consumer Privacy Act (entering into force in July 2020)

EU – ePrivacy Regulation (still in drafting stage)

India – Personal Data Protection Bill 2018 (expert committee issued draft, parliamentary bill expected in December 2018)

China – Personal Information Security Specification (May 2018)

Brazil – General Data Protection Law (LGPD - Law 13.709) (entering into force in August 2020)

Kenya – Data Protection Bill (still in drafting stage)

New Zealand – Privacy Bill 34–1 (still in drafting stage)

Uruguay – Law on the Protection of Personal Data and Habeas Data (Law 18.331/2008) and amendments (entering into force in January 2019)

Chile – Proposal Data Protection Law (still in drafting stage)

South Africa – Protection of Personal Information Act (POPIA) (date of entry into force still to be determined)

Australia – Privacy Act 1988 and amendments (last amended in March 2014, including 13 Australian Privacy Principles)

Argentina – Proposal Data Protection Bill (MEN-2018-147-APN-PTE) (still in drafting stage)

* Assessment based on 8 key areas of GDPR of relevance to marketing:

1) Extra territorial scope (Article 3)
2) Basis for processing (Article 6)
3) Children's data (Article 8)
4) Data breach notification (Article 33)
5) Right to erasure (Article 17)
6) Sanctions (Article 83, 84)
7) Data protection officer (Articles 37, 38, 39)
8) Impact assessments (Article 35)

WFA

Comparison with GDPR Framework

✓ Framework is similar* to GDPR

✗ Framework is not similar* to GDPR

	ARG		AUS	BRA		CAN	CHL		CHN	IND	KEN	NZL		ZAF	URY		USA	
	Current	Proposal	Current	Current	Future	Current	Current	Proposal	Current	Current	Proposal	Current	Proposal	Future	Current	Future	Current (Federal)	California (CCPA)
Extra-territorial scope	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓
Basis for processing	✓	✓	✓	✗	✓	✗	✗	✓	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗
Children's data	✗	✓	✗	✓	✓	✗	✓	✓	✓	✗	✓	✗	✗	✓	✗	✗	✓	✓
Data breach notification	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✓
Right to erasure	✗	✓	✗	✗	✓	✗	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✗	✓
Sanctions	✗	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Data protection officer	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗
Impact assessments	✗	✓	✗	✗	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗

*Assessment based on 8 key areas of GDPR of relevance to marketing:

1) Extra territorial scope (Article 3)
2) Basis for processing (Article 6)
3) Children's data (Article 8)
4) Data breach notification (Article 33)
5) Right to erasure (Article 17)
6) Sanctions (Article 83, 84)
7) Data protection officer (Articles 37, 38, 39)
8) Impact assessments (Article 35)

WFA

Argentina

	Current framework	GDPR-like?	Proposed framework (draft in discussion in Parliament)	GDPR-like?
Territorial scope	Applies only to the use of data of Argentinian residents by local entities.	✘	Applies worldwide to firms who conduct processing activities locally, collect and process data of Argentinian residents, or process data for purpose of providing goods or services to individuals located in Argentina, except where the law of the country where the data controller is located is more favourable to data protection.	✓
Legal bases for processing	Express and explicit consent; if data comes from publicly available sources; if necessary to fulfil legal or contractual obligations (but no 'legitimate interest'); if data is limited to certain basic information (name, ID, job and address).	✓	**Added:** If in the legitimate interest of the data controller or third party.	✓
Children's data	No parental consent required to process children's data.	✘	Parental consent is required to process the personal data of children under 13 years.	✓
Data breach notification	No provisions, although all data incidents must be recorded.	✘	Data breaches must be notified to DPA and data subjects within 72 hours if breach constitutes a significant risk to data subjects.	✓
Right to erasure	No provisions, although incomplete or partially or totally false data must be immediately amended or deleted.	✘	Right to be forgotten and right to rectification.	✓
Sanctions	Fines of up to ARG 5,000,000 (approx. €120,000).	✘	**Added:** Database can be temporarily or permanently shut down.	✘
Data protection officer	No specific provisions, but audits mandated by the government contain matters relating to data protection requiring a specific person to be designated.	✓	Organisations whose principal activity involves processing of sensitive data or who process personal data on a large scale must appoint a DPO.	✓
Impact assessments	No provisions.	✘	DPIAs must be conducted in situations where there is a high data privacy risk, such as when engaging in profiling or when processing sensitive data on a large scale.	✓
Notes:	DPO requirement is found in Disposition 3/2012.			

WFA

Australia

	Current framework	GDPR-like?
Territorial scope	Applies only to activities of organisations within Australia, to the activities of Australian organisations overseas, and to companies with a link to Australia (e.g. firms incorporated locally).	✘
Legal bases for processing	Explicit or implied consent (but must be informed); if secondary purpose of collection is related to primary purpose; if information is not sensitive; if necessary to fulfil legal obligations (but no 'legitimate interest'); direct marketing (non-sensitive data, includes opt-out).	✓
Children's data	No parental consent required to process children's data.	✘
Data breach notification	Data breaches must be notified when assessment shows individuals are at likely risk of serious harm.	✓
Right to erasure	No provision.	✘
Sanctions	Serious infractions can be subject to fines of up to AUD $2.3m (approx. €1.46m).	✓
Data protection officer	Guidance recommends appointment of DPO, but it is not an obligation.	✘
Impact assessments	No express requirement, but compliance with Privacy Principles may require impact assessments.	✘

Latest developments

- February 2018: **Data breach notification** became mandatory for all entities required to comply with the Privacy Act 1988.
- January 2017: Federal Court ruling narrowed down the definition of **'personal information'**: may not include data that only reveals identity if linked with other data (e.g. metadata).

Brazil

	Current framework	GDPR-like?	Future framework (entry into force Feb 2020)	GDPR-like?
Territorial scope	No specific provisions, though law in practice only applies to use of data of Brazilian residents by local entities.	✘	Applies worldwide to firms who conduct processing activities locally, collect and process data of Brazilian residents, or process data for purpose of providing goods or services to individuals located in Brazil.	✓
Legal bases for processing	Explicit consent required to process data that is personally identifiable.	✘	Consent and legitimate interest among 10 legal bases for collection, use and processing; broad definition of personal data and sensitive personal data.	✓
Children's data	Children under 18 years must be assisted to express consent; parental consent required for children under 16 years.	✓	No change vs previous framework.	✓
Data breach notification	No provisions.	✘	Data breaches must be notified within a reasonable timeframe.	✓
Right to erasure	No provisions.	✘	Right to erasure (15-day deadline).	✓
Sanctions	Fines of up to 10% of local gross profit.	✘	Fines increased to up to 2% of turnover in Brazil, max. R$50m (approx. €12m) per infraction.	✓
Data protection officer	No provisions.	✘	All data controllers must appoint DPO, although DPA will establish more specific norms and exceptions.	✓
Impact assessments	No provisions.	✘	Impact assessments may be mandatory in situations where there is a high data privacy risk, or at request of DPA. Additional guidance expected from DPA.	✓

Latest developments

- On 28 Dec. 2018: an Executive Decree established the **National Data Protection Authority (ANPD)** which holds similar power to the European DPAs. One particularity is that the ANPD will be advised by a permanent **National Council for the Protection of Personal Data and Privacy** composed of public and private stakeholders.

Canada

	Current framework	GDPR-like?
Territorial scope	Applies only to use of data of Canadian residents by local entities, although DPA may investigate compliance of foreign entities collecting and processing data of Canadian residents.	✘
Legal bases for processing	Express consent required for sensitive data; implied consent for non-sensitive data.	✘
Children's data	Framework does not differentiate between adults and children, but DPA guidance considers that use of data of children under 13 years requires parental consent.	✘
Data breach notification	Breaches resulting in risk of harm to individuals must be reported to DPA and data subjects.	✓
Right to erasure	Right to rectification.	✘
Sanctions	Breaches of notification and record keeping requirements may face fines of up to C$100,000 (approx. €65,000), although courts may award further damages to claimants.	✘
Data protection officer	Organisations must appoint an individual who is responsible and accountable for compliance with privacy framework.	✓
Impact assessments	No provisions, except in certain provincial health information protection acts.	✘

Latest developments

- November 2018: The revised **PIPEDA** came into force, enacting data breach notification requirements.
- October 2018: Canada's Privacy Commissioner asked its Federal Court to decide on whether the **right to be forgotten** applies in the country.
- March 2018: the DPA is considering policy reforms to offer more regulatory tools to protect personal information online.
  - Based on submissions received from a public consultation held in 2016, the DPA published in Jan 2018 a draft position on 'online reputation'. The document outlines proposed solutions from the regulator to balance the freedom of expression with the privacy interests of Canadian individuals.
  - Many submissions to the online consultation cited the **"right to be forgotten"** as a standard which should be followed by Canada.
  - The DPA position will be finalised and possibly revised based on the submissions to the public consultation.

WFA

Chile

	Current framework	GDPR-like?	Proposed framework (draft in discussion in Parliament)	GDPR-like?
Territorial scope	Applies only to use of data of Chilean residents by local entities.	✘	Applies only to use of data of Chilean residents by local entities.	✘
Legal bases for processing	Explicit and express consent required; if necessary to fulfil legal obligations; if data comes from publicly available sources; if data is only for exclusive internal use by private entities.	✘	Added: contractual obligations with data subject; legitimate interest of controller/third party (provided data subject rights are not affected).	✓
Children's data	Parental consent required for data of children under 18 years.	✓	Parental consent required for data of children under 14 years, and parental consent required for sensitive data of adolescents under 18 years.	✓
Data breach notification	No provisions.	✘	Must report data breaches to DPA, and serious breaches to data subjects as well, all within reasonable timeframe.	✓
Right to erasure	Right to modification or rectification, and cancellation or deletion.	✓	Right to be forgotten and rectification.	✓
Sanctions	Civil suits may result in fines of up to CLP 2,800,000 (approx. €3,500) if infringement of law involves financial data (up to CLP 550,000 if it doesn't), as well as damages	✘	Fines of up to CLP 236,500,000 (approx. €300,000).	✘
Data protection officer	No provision.	✘	Must appoint a data breach prevention officer.	✓
Impact assessments	No provision.	✘	No impact assessments required, but private and public entities must adopt breach prevention models and a compliance programme.	✘
Notes:	No DPA, enforcement is undertaken by courts.		Will establish DPA.	

WFA

China

	Current framework	GDPR -like?
Territorial scope	Applies only to use of data of Chinese residents by local entities, though comprehensive data localisation and transfer restrictions exist.	✘
Legal bases for processing	Explicit consent (though implicit consent is allowed for non-sensitive information); public interest; if necessary to fulfil contractual or legal obligations; and others. (NB No 'legitimate interest').	✓
Children's data	Parental consent required for children under 14 years.	✓
Data breach notification	Breaches must be promptly notified to DPA and data subjects.	✓
Right to erasure	Right to erasure, but only in event of breach of legal obligations or agreement with data subject.	✘
Sanctions	Fines of up to 10 times the amount of unlawful gains, or up to RMB 1,000,000 (approx. €125,000), up to 3 years imprisonment, and in extreme cases, business may be shut down.	✓
Data protection officer	DPO must be appointed if primary business is related to data processing with more than 200 employees, or if processing data of over 500,000 individuals.	✓
Impact assessments	Impact assessments are required when outsourcing data processing; transferring personal data (including to offshore parties); disclosing personal information to public.	✓

Latest developments

- June 2018: Chinese authorities published **a number of guidelines on the practical steps** organisations must take to comply with the new data protection, cybersecurity and technology regulations.
- June 2018: The third **draft of the proposed new e-commerce law** was debated at the top legislature. It **requires more explicit and layered consent options for targeted marketing.**
- May 2018: The Personal Information Security Specification took effect. Although the **standard is not binding**, there is consensus that Chinese and foreign firms will need to comply.
- A data trading framework is being drafted by government: includes recognition of **data as a type of intellectual property** that can be traded, including for marketing purposes.

WFA

India

	Current framework	GDPR-like?
Territorial scope	Applies only to use of data of Indian residents by local entities.	✘
Legal bases for processing	Written and explicit consent.	✘
Children's data	No parental consent required to process children's data.	✘
Data breach notification	Various cybersecurity incidents must be reported to DPA.	✓
Right to erasure	No provisions.	✘
Sanctions	Fines of up to INR 500,000 (approx. €6,000) for disclosure of personal information in breach of lawful contract or without consent.	✘
Data protection officer	A 'grievance officer' must be appointed to address discrepancies or grievances of data subjects within one month of reception.	✓
Impact assessments	Entities processing sensitive personal data must have security practices independently audited once a year, or when significantly upgrading systems.	✘

Latest developments

- July 2018: An expert committee submitted a report on data protection together with a suggested draft data protection bill, which underwent a public consultation. The draft issued by the committee includes a number of provisions which are similar to GDPR including:
  - **Extra-territorial scope.**
  - More **legal bases for processing,** including legal obligations and legitimate interest.
  - **Parental consent** required for children under 18 years.
  - **Data breach notification** requirements.
  - **Right to be forgotten** and correction.
  - **Fines** of up to INR 150m (approx. €1.8m) or 4% of the organisation's global revenue.
  - **Data protection officer** requirements.
  - **Data protection impact assessment** requirements.
- Reports suggest the Government might introduce a bill in Parliament by December 2018.

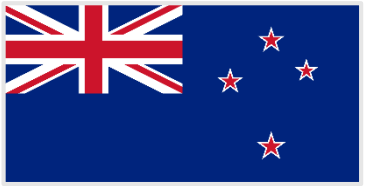
Kenya

	Proposed framework	GDPR-like?
Territorial scope	Applies only to use of data of Kenyan residents by local entities.	✘
Legal bases for processing	Specific and informed consent; if data comes from a publicly available source; if necessary to fulfil contractual or legal obligations; if in the legitimate interest of the data controller or third party; public interest.	✓
Children's data	Parental consent required for children under 18 years. Data controllers are forbidden from profiling, tracking, or monitoring children, and from directing targeted advertising towards children.	✓
Data breach notification	Breaches must be promptly notified to DPA and data subjects.	✓
Right to erasure	Right to erasure and right to rectification.	✓
Sanctions	Fines of up to KES 5,000,000 (approx. €43,000).	✘
Data protection officer	Must appoint a DPO when regularly engaging in systematic monitoring or processing data on a large scale.	✓
Impact assessments	Entities must conduct a DPIA when data processing is likely to result in a high risk to data subjects.	✓

Latest developments

- August 2018: Kenya's Ministry of Information, Communication and Technology issued a draft Data Protection Bill for comment. If approved, this bill would be the first time Kenya has had a framework on data protection. The period allocated for comments ended on September 19th 2018.

New Zealand



For more information on developments in New Zealand, please contact Lindsay Mouat (Lindsay@anza.co.nz) at the Association of New Zealand Advertisers.

	Current framework	GDPR-like?	Future framework (draft in discussion in Parliament)	GDPR-like?
Territorial scope	Applies only to use of data of residents of New Zealand by local entities.	✘	Certain "Information Privacy Principles", including those relating to the right to correction, apply to data of residents held overseas.	✘
Legal bases for processing	Informed consent (no provisions on how consent should be gathered); if data comes from a publicly available source; if necessary to fulfil a legal obligation; if data is processed in way which will not identify the data subject concerned; if compliant with the 12 "Information Privacy Principles" set out by the law.	✘	No changes vs previous framework.	✘
Children's data	No parental consent required to process children's data.	✘	No changes vs previous framework.	✘
Data breach notification	No mandatory provisions, although guidelines describe instances in which voluntary notification should be made to DPA and data subjects affected.	✘	Breaches that pose a risk of harm to data subjects must be notified to DPA and data subjects.	✓
Right to erasure	Right to correction (which can involve deletion). Additionally, data subjects may apply for take-down orders issued by courts.	✓	No changes vs previous framework.	✓
Sanctions	Fines of up to NZ$ 2,000 (approx. €1,200).	✘	Fines of up to NZ$ 10,000 (approx. €6,000).	✘
Data protection officer	Every private and public entity must appoint a DPO.	✓	No changes vs previous framework.	✓
Impact assessments	No mandatory provisions.	✘	No mandatory provisions.	✘
Notes:	The DPA is not able to impose fines or issue formal rulings, only opinions, which can be referred to the Human Rights Review Tribunal, whose rulings are legally binding.		DPA would be able to issue compliance orders and fines independently.	

WFA

South Africa

	Future framework (date of entry into force still to be determined)	GDPR-like?
Territorial scope	Applies only to use of data of South African residents by local entities.	✗
Legal bases for processing	Express and specific consent; if necessary to fulfil contractual or legal obligations; if in legitimate interest of data subject, data controller or third party.	✓
Children's data	Consent of legally competent person required for children under 18 years, unless: if necessary to fulfil legal obligations; for research purposes; if data has been made publicly available with consent of legally competent person.	✓
Data breach notification	Breaches must be notified to DPA and data subjects within reasonable timeframe.	✓
Right to erasure	Right to deletion and correction.	✓
Sanctions	Fines of up to ZAR 10,000,000 (approx. €685,000)	✗
Data protection officer	The head of a company is its DPO by default, although the role can be delegated.	✓
Impact assessments	No provisions.	✗

Latest developments

- December 2018: POPIA has still not been published in the official Government Gazette, so it remains unclear when the law will enter into force.
- April 2018: The DPA indicated that one of the key components of the incoming POPIA is **aligning** South Africa's privacy laws **with international standards**, and that it will follow the lead of the EU and UK on protecting personal data.
- September 2016: the national assembly approved the appointment of the members of the DPA, the Information Regulator.
- April 2014: some sections of POPIA entered into force via Decree. These include its definitions, the parts detailing the establishment of the DPA, and the parts allowing the government and the DPA to draft POPIA regulations.

WFA

Uruguay

	Current framework	GDPR-like?	Future framework (Entry into force Jan 2019)	GDPR-like?
Territorial scope	Applies only to use of data of Uruguayan residents by local entities.	✘	Applies worldwide to firms which provide goods and services in Uruguay, process data of Uruguayan residents, and if processing facilities are located within Uruguay.	✓
Legal bases for processing	Express and explicit consent; if data comes from a publicly available source; if data is limited to address, telephone number, ID number, nationality, or tax number; if necessary to fulfil a legal or contractual obligation.	✓	No changes vs previous framework.	✓
Children's data	No parental consent required to process children's data.	✘	No changes vs previous framework.	✘
Data breach notification	Data breaches should be reported to the affected data subjects.	✘	Data breaches must be notified immediately to DPA.	✓
Right to erasure	Right to deletion and rectification.	✓	No changes vs previous framework.	✓
Sanctions	Fines of up to UYU 200,000 (approx. €54,000).	✘	No changes vs previous framework.	✘
Data protection officer	No provisions.	✘	Firms processing sensitive data or processing data on a large scale must appoint a DPO.	✓
Impact assessments	No provisions.	✘	Firms must undertake DPIAs, but it's not clear what specific instances require them.	✓

WFA

US: California

	Future framework (entry into force July 2020)	GDPR-like?
Territorial scope	Applies worldwide to for-profit entities doing business in California and which use data of Californian residents.	✓
Legal bases for processing	Right to opt out of businesses selling residents' personal information.	✗
Children's data	'Opt in' consent is required for residents between 13 and 16 years. Parental consent is required for children under 13 years.	✓
Data breach notification	Breaches affecting more than 500 residents must be reported to state Attorney-General.	✓
Right to erasure	Right to erasure (with some exemptions).	✓
Sanctions	Allows lawsuits whereby affected residents can individually recover up to $750 per incident (approx. €665), or actual damages.	✗
Data protection officer	No provisions.	✗
Impact assessments	No provisions.	✗
Notes:	Data breach notification is governed by the Californian Data Breach Notification Law, rather than the CCPA.	

Latest developments

- September 2018: amendments pushed back the date the California Attorney General will promulgate the regulation from January 2020 to **July 1, 2020.** The California Attorney General's recommendation that the CCPA's limited private right of action be expanded was rejected, and language was added to clarify the limits of consumer lawsuits.

WFA

US: Federal

	Current framework	GDPR-like?
Territorial scope	Applies only to use of data of United States residents by local entities.	✘
Legal bases for processing	No general provisions, although FTC guidelines require express consent for sensitive personal data. GLB Act and HIPPA have sector-specific requirements.	✘
Children's data	Parental consent required for children under 13 years.	✓
Data breach notification	No country-wide provisions, although 47 states have requirements.	✘
Right to erasure	No provisions.	✘
Sanctions	Fines vary with regards to violations of sectoral privacy provisions; civil suits have resulted in compensation going as high as $18.5m (approx. €16.4m).	✘
Data protection officer	Only certain entities handling health data must appoint a DPO.	✘
Impact assessments	No provisions.	✘
Notes:	Federal framework includes FTC Act (applies to most firms in US), GLB Act (financial institutions), and HIPAA (health insurance and healthcare providers).	

Latest developments

- October 2018: Senator Ron Wyden is drafting a new federal data privacy bill, and has released a discussion draft.
- September 2018: The US Department of Commerce launched a **public consultation** on a proposed approach to consumer data privacy. The consultation saw several firms propose model frameworks, including Google, the Information Technology Council (ITI) and Intel.

EU

Additional privacy law in development in the EU

- Following the entry into force of the GDPR in May 2018, policymakers in Brussels are proposing revisions to specific rules designed to regulate online tracking (*ePrivacy Regulation*).
- Consent required for online tracking (e.g. placing cookies on a website); proposal moves the consent request to software level upon installation; may end-up mandating that these settings must be set to no tracking by default.
- No other legal bases available for online tracking (e.g. legitimate interest).
- Potential prohibition on requiring consent for online tracking in order to access an online service or website.
- Introduction of fines and definitions in line with GDPR.
- **Status**: earliest possible entry into force - mid 2020. Delays likely as the legislative process is moving slowly; could be as late as 2021/2022.

Link: WFA's position paper on the proposed ePrivacy Regulation

Want to stay up to date on global privacy developments?

WFA's Digital Governance Exchange (DGX) network brings together a broad range of functions (privacy, compliance, digital governance, legal, digital marketing, media..) to identify practical solutions to data challenges and share insights and experiences with each other in relation to developing and implementing good data policies and practices.

Being part of the DGX network means:

- Receiving regular updates on global policy developments e.g. privacy regulation around the world.
- Attending DGX meetings to share best practice & experiences with other WFA members on issues such as privacy, data management and data transparency.
- Guides & briefings on important issues e.g. WFA's global privacy map.
- Access to WFA webinars and remote forums on relevant topics.

To join the DGX network, email c.armitage@wfanet.org

Meetings in 2019:
California (Feb 7), London (Mar 7, Nov 14), Lisbon (Mar 27), Singapore (June 13), New York (Sept 5)

World Federation of Advertisers
London, Brussels, Singapore

wfanet.org
info@wfanet.org
+32 2 502 57 40

twitter @wfamarketers
youtube.com/wfamarketers

linkedin.com/company/wfa