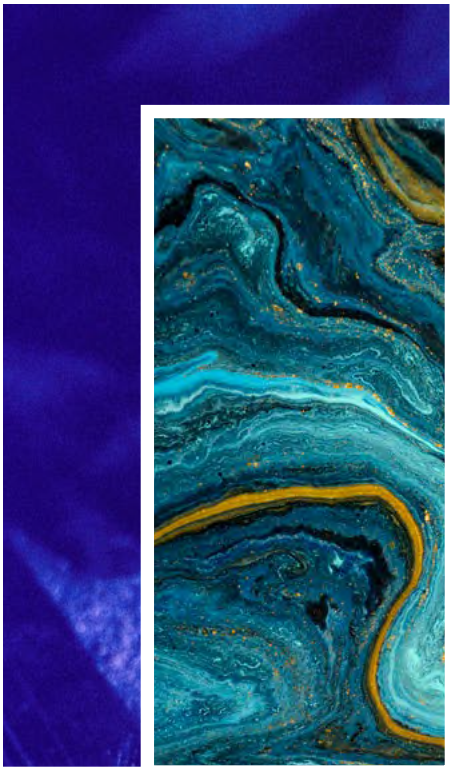
ESOMAR

GLOBAL LEGAL UPDATES

This document provides a global overview with a regional angle of privacy laws that have been adopted or proposed in the past two years. Originally prepared for ESOMAR's Legal Affairs Committee as part of their monitoring activities, it's now been released for the wider ESOMAR community. We hope that you will find this document useful and we would very much welcome any feedback you may have.

22 October 2019

Table of Content



USA

California

While the California Consumer Privacy Act (CCPA) will enter into force on 1 January 2020, there is already a new ballot initiative to adapt the law. The project is led by the same advocacy group which was the driving force behind CCPA. If it obtains sufficient signatures, the California Privacy Rights and Enforcement Act of 2020 (CPREA), will appear on the November 2020 California ballot.

It aims to significantly amend the CCPA, introducing several new consumer rights and obligations for business.

- New notice requirements: the existing disclosure requirements are being expanded, with companies also having to inform consumers about retention periods, the types of sensitive data collected, and the specific purposes. Furthermore, it requires disclosure of the "logic" behind automated profiling practices that may have a significant adverse impact on consumers.

- Expanded consent requirements: while under CCPA consumers have a right to opt-out from having their personal information sold, CPREA would introduce heightened protections for "sensitive" personal information (PI), prohibiting businesses from selling sensitive PI unless a consumer has provided opt-in consent. It furthermore would introduce a right to opt-out from the use of PI for marketing or advertising purposes.

- Service providers: The CPREA would mandate that businesses include specific data protection obligations in contracts with (i) third parties to whom businesses sell PI and (ii) service providers or contractors to whom businesses disclose PI.

- CPREA would implement the principles of data minimisation, data accuracy, and the safeguarding of personal information. It would further introduce the right to correct personal information, requiring business to take "commercially reasonable efforts" to correct the inaccurate PI.

- Where currently the enforcement sits with the Californian Attorney-General, CPREA would introduce a new agency, the California Privacy Protection Agency, to administer and enforce the new law.

COPPA

The FTC has started the process to update its guidelines that implement the Children's Online Privacy Protection Act. In particular, the FTC is looking for feedback on definitions, notice and parental consent requirements, and exceptions to verifiable parental consent.

Federal privacy bill

While there is still a push to adopt a Federal Privacy Bill, the progress seems to have slowed down. Congress organised a series of hearings with experts from both industry and advocacy groups, however this has not yet resulted in a proposal that can obtain sufficient support in both Chambers. Nevertheless, the general consensus seems to be that a federal law will be adopted in the near future.

Other state laws

Awaiting a federal law, several states have introduced their own privacy bills, adding to the complexity. At the moment, no less than 15 states have introduced legislation, of which California, Nevada and Maine have been signed to law. A full overview of these laws can be found at the IAPP website.

AFRICA

Tunisia

In March 2018, a Bill was introduced to amend the 2004 Law on the Protection of Personal Data. The goal of the draft is to become more in line with the GDPR, so as to create more business opportunities with Europe. It provides more independence to the National Personal Data Authority and gives it more power, namely: being able to issue financial and judiciary sanctions, being able to issue recommendations regarding the protection of personal data, and a consultative power in this domain. The draft also limits custodial sentences to dangerous crimes threatening public security and national defence. Under the Bill, the transfer of personal data to a third party cannot be done without the consent of the data subject.

Algeria

The 2018 Algerian law on the Protection of Individuals in the Processing of Personal Data contains provisions which cover most topics expected to be found in a data privacy law: data subject's consent requirements regarding data processing, the right to modification and erasure, and children's data protection. Furthermore, the new Law requires that all personal data processing operations first be subject to a declaration to the national authority. This same authority (Autorité National de Protection des Données à Caractère Personnel) is allowed to deliver administrative sanctions in case of a breach. The sanctions regarding processing one's sensible data are very strict: it can involve not only a monetary fine, but also two to five years imprisonment. Finally, it may be interesting to know that researchers can contact a data subject without consent through automated dialling, e-mail or similar technology.

Egypt

A brand-new Data Protection law was passed in June 2019. It will protect personal data for Egyptians and EU citizens based in Egypt. It applies to all firms dealing with personal data. The law includes a consent clause, as with most Data Protection laws, both for the collection, processing and disclosure of one's data but also for the transfer, storage and preservation of said data. It also provides a definition for sensitive data: data relating to physical/mental health, financial, political, and religious data. Any transfer or sharing of personal data to a foreign country must first obtain a license from the newly created Personal Data Protection Centre.

Kenya

There are currently two separate draft Data Protection Bills currently under consideration in Kenya; one submitted to the Kenyan Parliament, and another to the Senate. Not much is known about the status of these bills at this moment in time. The voting on the Bill presented to the Senate was delayed as of July 2019. The two Bills seem to be clashing on clauses that have remained unnamed. Due to the lack of information on this topic, the main element to take out of Kenya's current legislation state regarding Data Privacy is that it is on its way to develop regulations regarding the topic, and on its way to adopting international standards.

Zambia

In June 2018, the Zambian Cabinet approved the introduction of a Data Protection Bill to Parliament. It applies to both private and public bodies, and has an extraterritorial scope, meaning that this Bill would apply to a personal data controller using processing means located in Zambia (except if the data is

merely in transit through Zambia). It provides for the establishment of an independent Administrative Authority, which will have oversight and control of the law. It will not be able to sanction on breaches themselves, but will have the power to conduct inquiries, and submit complaints to the courts regarding any breach of the Act. The Bill also contains provisions on requirements regarding the quality of data, the adequacy of the data, accuracy, and anonymization. Interestingly, the processing of non-sensitive personal data is permitted without consent of the data subject, whereas processing sensitive data requires written consent. Information as to when this Bill is expected to pass is unclear.

Zimbabwe

Laws on Data Protection and on Freedom to Access Information are expected to come in the near future, as the Minister of Information, Publicity, and Broadcasting Services has announced in February of this year that the current Access to Information and Protection of Privacy Act would be repealed to welcome new laws on the topic. The information regarding these laws is, currently, quite scarce.

ASIA PACIFIC

Bhutan

Bhutan's "Information, Communications and Media Act" came into force in 2018. The Act gives Bhutan a minimal data privacy law, but its coverage regarding privacy does remain extremely limited. The law covers almost all uses of electronic information and enables for the creation of an Infocomm and Media Authority, a partly independent body with limited authority. Under the Act, it is able to investigate and resolve complaints. The Act also covers offences and compensation in such cases.

India

The Indian Personal Data Bill was introduced following a landmark ruling on privacy by the Indian Supreme Court, which declared that privacy is an intrinsic part of Article 21 of the Constitution, which protects life and personal liberty. Among other things, the Indian Bill would allow for the creation of an independent regulatory body and heavy penalties in cases of violation. Furthermore, it would apply to both private and government entities in India. Finally, it introduces a data localization requirement, where data will have to be stored on servers located within the country and provide clarifications on the topic of data ownership. Considering the size of the Indian market research industry, this is an important bill to look out for.

Indonesia

The Indonesian Personal Data Protection Bill draws a lot of its features from the GDPR. It widens the scope of sensitive information to include location data from phones and political views and introduces obligations for data controllers and processors. The Bill does not provide for a general data protection authority, but rather each ministry would remain in charge of data protection matters for its own sector.

Kazakhstan

The Kazakh law was updated to add a localization requirement: data operators now have to store personal data on the territory of the Kazakh Republic, although it is not clear to whom this rule applies. Regardless, no further restrictions on cross-border transfer of personal data are introduced.

New-Zealand

In New-Zealand, a bill amending the 1993 Privacy Act was introduced in March 2018 and as this is being written, it is undergoing a second reading in Parliament. It is predicted to be passed in 2019/2020. One of the main changes is to give the Act an extraterritorial scope. The bill will provide for the Act to apply to overseas agencies doing business in New Zealand, and also to an individual "not ordinarily resident in New Zealand, who is present in New Zealand, in relation to any action they take, and information they collect, while in New Zealand, regardless of where the information is held or where the relevant individual is located".

South Korea

As for South Korea, a bill was introduced in 2018 and is currently under review to amend the 2011 Personal Information Protection Act (PIPA), the original goal of which was to expand on other Acts related to the topic. This bill was part of a series of reforms amending not only the PIPA but also the Network Act, the Location Information Act and the Credit Information Act thus creating a single law covering data protection and privacy. The bill introduces the concept of "pseudonymized data", expands on the permissible purposes for personal data processing, and permits for the combination of data sets. Furthermore, it provides more enforcement powers for the Personal Information Protection Committee.

Kyrgyzstan

Kyrgyzstan's 2017 amendment to the Law on Personal Information provided a needed and important legislation related to electronic commerce and was drafted with a view to a better protection for data subjects and enhances security measures related to the protection of data stored electronically. Furthermore, data holders will now have to account for third-party transfers and register these transfers with the relevant state authorities. The bill also includes the creation of a supervisory authority, although not much information has been given as to when and how this authority is expected to emerge.

Thailand

The Thai Personal Data Protection Act was just approved earlier this year by the Government and was passed into law. It has been given one transitional year for companies and organizations processing personal data to take the necessary measures to become compliant. The law has extraterritorial applicability, covers all personal data and allows both for penalties and for lawsuits in case of a personal data breach. It also gives the right for people to request access to their personal information, and in the case where the data-controller is not complying to the Act, for their data to be deleted, destroyed or anonymized.

Pakistan

The Pakistan Data Protection Bill has been drafted to provide individuals with rights similar to those in the GDPR, i.e. consent giving, security requirements, right of access, correction and erasure of one's personal data, etc. It provides for the creation of an enforcement body, the National Commission for Personal Data Protection, which will be able to receive and decide complaints from individuals, as well as support data processors and controllers in complying with the Act.

LATAM

Cayman Islands

In 2017, a new comprehensive data protection law was adopted which will come into force by September 2019. The new law takes many aspects from internationally recognised principles, such as requiring data minimisation and purpose limitation. It grants individuals the rights to access the data that an organisation is processing, and to request that any inaccurate data is corrected or deleted. The Office of the Ombudsman will be made responsible to enforce the law.

Brazil

One of the major new data protection laws is Brazil's General Data Protection Law. The law draws heavily on the EU's GDPR, with similar requirements for data exports limited by adequacy requirements of the destination, data protection impact assessments, data protection officers, data breach notifications to the DPA and the data subject, and limits on automated processing.

It also includes well-known rights, including the right to access, rectify and delete data; the right to be informed about data processing; and the right to data portability. The law will be enforced by a the newly established Data Protection Authority and administrative fines can be given of up to 2% of a company's previous year's revenue in Brazil.

Panama

In October 2018, the Panamanian Parliament passed the Data Protection Law, and will take effect in 2021, i.e. two years after publication in the Official Gazette. With this law, Panama follows the regional trend of adopting comprehensive data protection legislation. The law makes the National Authority for Transparency and Access to Information responsible for its enforcement, which can hand out sanctions between US$1,000 and US$10,000. It provides for similar rights to individuals as most modern privacy laws, i.e. access, rectification, cancellation, objection and portability.

St Kitts & Nevis

The Data Protection Act 2018 was enacted on May 4, 2018. The Act is largely derived from the Organization of Eastern Caribbean States (OECS) model, drawing upon EU sources as well as the OECD. It covers both the public sector and the private sector in respect to commercial transactions and goes beyond minimal principles by including requirements in relation to sensitive data, and limits on data retention. The Information Commissioner is empowered to issue enforcement notices. Data subjects can take civil actions to seek compensation for breaches of the Act, and there are a range of criminal penalties.

Uruguay

Uruguay was one of the first countries in LATAM to adopt a comprehensive data protection law. In order to ensure its legal framework remains compatible with the new GDPR, so it can continue to enjoy the EU's adequacy decision, it has updated its privacy law. The updated legislation strengthens the extra-territorial scope, data breach notification, accountability (requiring controllers to implement other GDPR elements), and data protection officers.

MIDDLE EAST

Iran

A Draft Act on Personal Data Protection and Safeguarding was introduced to the Iranian Parliament in September 2018 and is currently awaiting review. The Draft Act is intended to apply to "Iranian citizens (individuals and corporations), public or private, whether their private data is being processed inside or outside Iran, and to foreign citizens (individuals and corporations), public or private, only if their data is processed by Iranian processors and controllers". Furthermore, it proposes the creation of a Data Protection Commission in charge of enforcing the Act. However, there remains in the Draft Act a number of unclear points, such as its territorial scope, which is not covered in any provisions. Hopefully, more clarifications on the Draft Act will be provided in the future.

Bahrain

In Bahrain, the Data Protection Law (DPL) was implemented on April 1st 2019, which applies to the private sector. The law has an extraterritorial scope, meaning that it applies to persons processing personal data using means available in Bahrain (such as appointed local representatives), and provides for a Personal Data Protection Authority, which has the power to investigate breaches of the DPL. A feature of the law worth noting is that it provides for criminal penalties for violations of certain provisions of the legislation, such as processing sensitive personal data or transferring personal data outside of Bahrain without complying with the relevant requirements as listed in the DPL, such as (among other things) the receiving countries having equivalent data protection laws or receiving a transfer authorization from the Personal Data Protection Authority.

Lebanon

Law No. 81 Relating to Electronic Transactions and Personal Data was introduced in October 2018, adding Lebanon to the ever-growing group of countries with a general data protection law. The Act took a big step in the direction of stronger personal data protection by regulating all collection, processing, or use of personal data, both through digital means and otherwise (as opposed to data protection being regulated only for certain industries and only to a certain extent). The Law provides a set of conditions that need to be met before one is able to collect, process and use personal data, as well as a list of exceptions to these conditions.

Israel

In February 2018, the Israeli government approved an amendment to its 1981 Privacy Protection Law. However, it is currently gridlocked and pending a decision by the Israeli Parliament. The amendment focuses on giving more enforcement powers to the Protection of Privacy Authority, such as the power to impose higher fines in case of a breach.

This legal review report is a demonstration report of ESOMAR as part of its **ESOMAR Plus** consultancy services. Further issues and updates may be produced in 2020. Contact us if you'd like to know about future publications and access conditions.

For more information visit esomar.org/esomar-plus or message us on: plus@esomar.org

ESOMAR