DATA PRIVACY LAWS & REGULATIONS

GLOBAL OVERVIEW

November 2021

Executive summary

In our increasingly interconnected, digital world, data – especially personal data of consumers – is worth gold. Illegal use of personal data or personally identifiable information (PII) has become a growing problem. Governments around the world are implementing strict regulations to control and protect private data, with the EU GDPR broadly seen as the benchmark.

As of January 2021, around 130 countries had data-privacy laws in place, representing two-thirds of the world's jurisdictions. While this is a positive step, this proliferation of data-privacy rules makes developing a global approach (for companies and consumers alike) a challenge.

GDPR, leading the way

The EU GDPR is generally considered as the most far-reaching data and privacy protection legal framework. Most regulations and laws in other regions of the world – notably section 5 of the Federal Trade Commission Act (FTC Act) or the California Consumer Privacy Act (CCPA) in the USA, Brazil's LGPD or South Africa's POPI Act – follow more or less the European guidelines. According to experts, the next few years will see many other regions and countries follow suit.

How does this affect the international moving and relocation industry?

During an international move, a transferee's key sensitive personal information is shared with a number of different suppliers: the booking, origin and destination agents; the shipping line; the customs authorities at origin and destination; etc. There are inherent risks to removals companies when using their transferees' private data. They should therefore be very much aware of their data privacy protection responsibilities.

Most data protection and privacy rules are based on the same basic principles, notably that a person (also called the "data subject") has the right to:

- Know how and why their data is collected;
- Ask for correction or deletion of their data;
- Be informed of possible misuse of their data;
- Be informed if their data is shared with third-parties.

Moving companies should have documented processes in place to comply with these rules. While private data is often required on shipping documents, movers should always ask if this is absolutely necessary - and remove private information when it is not legally required.

As a moving company, you are responsible for telling your customers about any potential data-privacy risks and providing guidance to them whenever possible. By doing this, you mitigate the risks and, so, are (generally) compliant from a data protection perspective.

This report gives a general overview of the current situation of data protection laws across the world. It is not meant as an exhaustive list of existing or future laws and regulations.

For questions or comments, please contact Marie-Pascale Frix, Business Intelligence Manager at FIDI Global Alliance, at marie-pascale.frix@fidi.org .

Table of Contents

Executive summary 2
Table of Contents 4
Introduction 5
How does personal data protection legislation affect the moving industry? 6
What is 'personal data' or 'PII'? 7
Which data is Considered PII? 8
How to identify Personal Data/PII? 9
Data privacy regulations across the world 10
Laws and regulations you should be aware of for 2021 and 2022 13
1. European Union: 13
The General Data Protection Regulation (GDPR) 13
2. United States 16
The Federal Trade Commission Act 16
New York SHIELD Act 16
California Consumer Privacy Act (CCPA) 16
California Privacy Rights Act (CPRA) 17
Colorado Privacy Act (CPA) 18
3. Brazil 19
4. South Africa 20
Global compliance 20
Conclusions 21

Introduction

In the current digital age characterized by data travelling the world through borderless networks, topics such as “Personal Data Collection” and “Data Protection” are becoming increasingly important.

With the development of new information technology, **personal data is easier to access and share than ever before.** Keeping users' personal information safe is a matter of utmost importance, as fraudulent access to this information can put both the person involved and their employer at great risk. **Theft and/or fraudulent loss of personal information may lead to disastrous consequences** for the person and companies that are the victims of such acts. Of equal concerns is the collection, use and sharing of personal information to third parties without knowledge or consent from the individuals concerned.

The gathering of personal data (often abbreviated ‘PII’ for ‘Personally Identifiable Information’) has unfortunately become a very profitable market for cybercriminals across the globe. **The protection of personal information has therefore become a worldwide security issue**, resulting in governments creating stringent regulations related to private data protection.

Data privacy regulations have skyrocketed in recent years with approximately 130 countries having enacted data privacy laws as of January 2021; this represents **66% of the worldwide jurisdictions**.

While this demonstrates that most governments take the security of private information seriously, it can be challenging for companies to develop global or regional privacy compliance approaches, as most of these laws have their own specific rules.

How does personal data protection legislation affect the moving industry?

Removal companies have to be aware of the risks inherent to the handling and transfer of the private data of their transferees, **and their responsibilities in terms of data privacy protection** (see FIDI FOCUS 289 - Feb/March 2019).

While private data is often required for shipping documents, movers should question the need for such data and remove private information when not legally required. As a moving company, you are responsible to inform your customers of any potential data privacy risks and provide guidance whenever possible.

It is important to be aware that transferees' private data may be sold or shared by third parties depending on the jurisdictions, **exposing the transferees to identify theft, fraud and unwanted solicitations.** The USA is a good example of such a situation.

The CBP (US Customs and Border Protection) is legally allowed to sell vessel manifest data, including PII of transferees (such as Social Security numbers, passport numbers, home addresses and other personal data) to data brokers. While it is not the specific intention of the CBP to release sensitive data of individuals, the manifests currently provided to data brokers often includes the PII of transferees and military personnel shipping household goods to the United States. The data brokers post the manifest information online to provide analyses and trends on shipments, hence publicly exposing the PII of transferees.

Since 2017, a coalition of national military and moving associations (AMSA, WERC, IAM) has been **urging the US Senate to protect the PII of transferees** by passing the **Moving Americans Privacy Protection Act** into Law in order to prohibit US Customs and Border Protection (CBP) from releasing the PII of movers' clients to global data brokers.

On 8 June 2021, the US Senate finally passed the US Competition and Innovation Act[1] (USICA) which includes a key provision directing the US Secretary of the Treasury to ensure that any personally identifiable information is removed from a vessel, aircraft, or vehicle manifest, before that manifest is provided for public disclosure.

[1] Source: Article from Worldwide ERC

The above example illustrates how crucial it is for moving businesses to be well informed of data privacy protection regulations and related consequences for their companies in case of non-compliance.

Let us start by understanding the general concept of personal data and where it applies globally.

What is 'personal data' or 'PII'?[2]

There is no universal definition for "personal data". In simple terms, it refers to any type of data that can be used alone or combined with other relevant information to identify an individual.

In the European Union, the term generally used is "**Personal Data"**, while in the USA the term **"Personally Identifiable Information" or "PII"** is generally used.

In the USA, PII is defined as the "Information used to distinguish or trace an individual's identity (…)" and it includes "any information that is linked or linkable to a specified individual, alone, or when combined with other personal or identifying information"[3].

The General Data Protection Regulation (GDPR) of the European Union use the term "Personal Data" to describe "any piece of information that relates to an identifiable person".

The European and American philosophies around data privacy follow different approaches: the Europeans consider that personal data is private unless you give explicit permission; while the American view is that your data is public unless you expressly request that it is kept private.

[2] Sources: Wikipedia, United States Department of Defense (DOD), article from www.datacenters.com, EU GDPR website
[3] https://csrc.nist.gov/glossary/term/personally_identifiable_information

Which data is Considered PII?

What information is considered as PII **depends on where you do business**. However, despite the discrepancies between the laws of different countries and regulatory entities, the following is **generally considered sensitive "Personally Identifiable Information":**

- Full name
- Social Security Number (SSN)
- Driver's license / National Identity Card
- Physical mailing address
- Phone numbers
- Criminal or employment history
- Passport information
- Credit Card information
- Financial information
- Medical records

The EU GDPR includes a large number of **additional data elements**, such as:

- Email address
- Any online identifier (including but not limited to IP address, Login IDs, Social Media Posts, customer loyalty histories, cookie identifiers, etc)
- Geolocation data
- Biometric data (including but not limited to fingerprints, voiceprints, photographs, video footage, etc)
- Any factor specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the individual

Another recent PII legislation, the California Consumer Privacy Act (CCPA), goes even further than the GDPR by including additional data such as:

- Aliases (used for example as logins on websites)
- Online account names
- Records of personal property
- Purchased products and services
- Purchases or consuming tendencies
- Browsing history
- Search history

- Information regarding user's interaction with websites
- Audio, electronic, visual, thermal, olfactory, or similar information
- Education information that is not publicly available
- Inferred consumer profile including consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

Other types of information that can used to indirectly identify an individual are also mentioned in most current legislations. Examples of this type of information are:

- Zip code
- Race
- Gender
- Date of birth
- Place of birth
- Religion

How to identify Personal Data/PII?

Depending on the jurisdictions where you do business, it may be convenient to invest in **specialized PII scanning and discovery tools**. Such tools are useful when auditing your company's data to ensure compliance with the different regulations.

These tools not only automate a good part of the process but also help to comply with the different regulations. Among their main benefits are:

- **Comprehensive PII Data Discovery:** automatically scans cloud storage, workstations, local files shares, mobile devices, and more, in order to locate PII data such as personal, finance, health, and other sensitive information.
- **Risk assessment:** identify potential risks in all digital assets that are not properly protected or reside outside a secure environment.
- **Easier data management:** filter different types of PII data, organize it according to organization rules/needs, and export it for further analysis.
- **Remediation of PII issues:** most of these tools offer the possibility of analyzing the flow of data both passively and in real-time in order to put in "quarantine" all the sensitive information that does not comply with the appropriate security standards.

Data privacy regulations across the world[4]

The EU-GDPR has inspired many privacy regulations worldwide, from Brazil's LGPD to the CCPA in California. While many of these laws agree on the broad terms of data protection, each implements these protections in its own way.

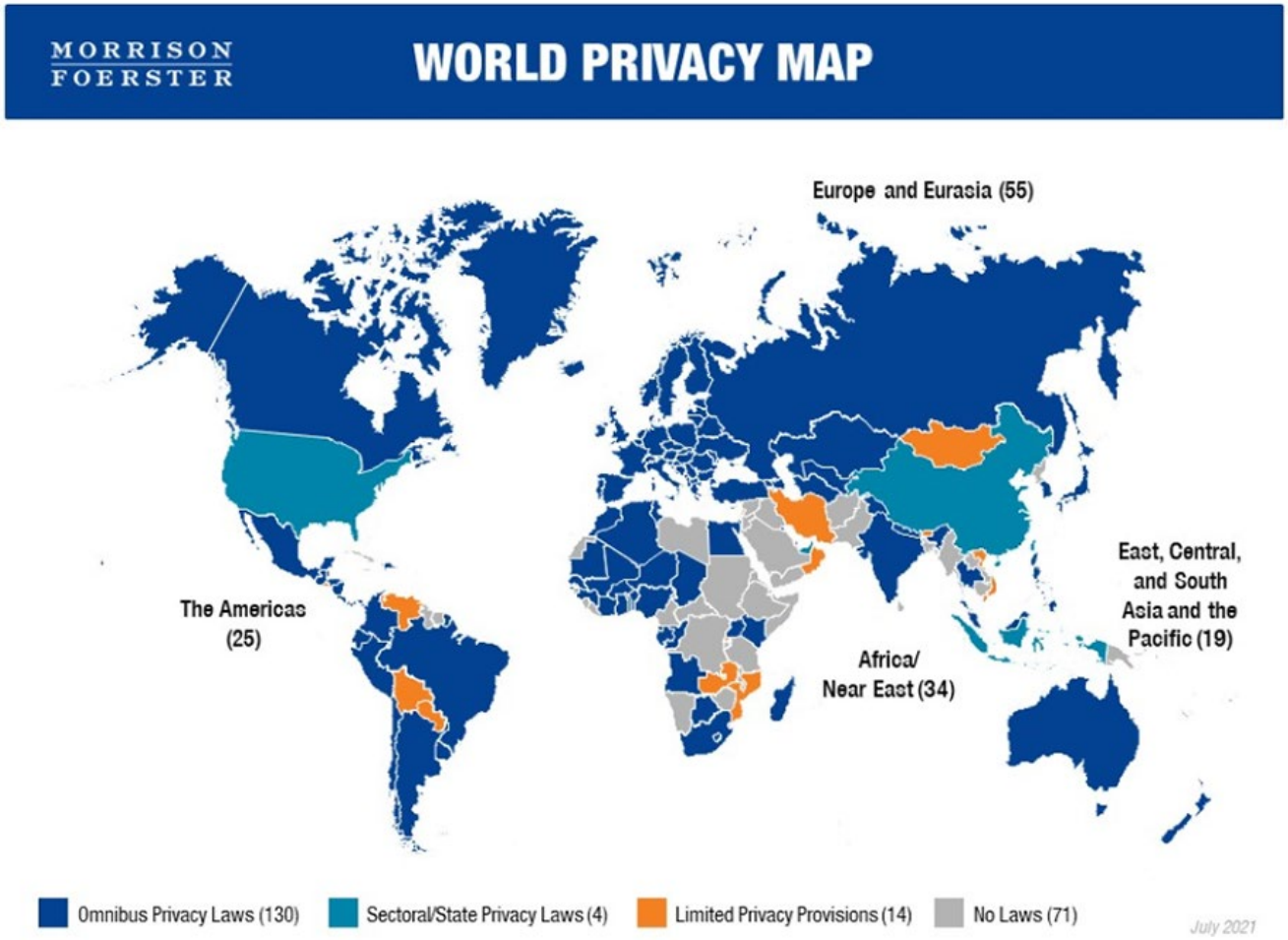
As per the latest UNCTAD[5] figures, here is the worldwide situation in terms of data privacy laws (194 countries[6]),

- 66% countries with legislation in place;
- 10% with draft legislation;
- 19% with no legislation;
- 5% with no data.

It is interesting to note that from the 128 counties with existing legislation, 102 are in jurisdictions outside the European Economic Area (EEA).

A third of the laws outside the EEA are in Africa and the Near East region (34) while the rest of the laws are distributed relatively equally among the Americas (25), Europe/Eurasia (24), and Asia-Pacific (19). This includes three jurisdictions (China, India, and Indonesia) that have de facto national privacy laws and one jurisdiction (the United Arab Emirates) that has omnibus privacy laws applicable to their two free trade zones.

[4] Main sources: A Practical Guide to Data Privacy Laws by Country [2021] by I-Sight; Analysis by Morrison Foerster; UNCTAD report on Data Protection and Privacy Legislation Worldwide, Consumer International Report – The State of Data Protection Rules around the World'
[5] United Nations Conference on Trade and Development



Source: https://www.mofo.com/resources/insights/210127-data-privacy-day.html

According to Morrison & Foerster's data privacy study (January 2021), **sixty of these laws were enacted in the past ten years and half of those within the past five years**. In the next couple of years alone, we may expect as many as 12 or more new or updated laws enacted or introduced into national legislatures.

As per Morrison & Foerster's 2021 study, **the data privacy landscape in Asia** (East, Central, and South) **and the Pacific has undergone a dramatic transformation in the past decade** and all indications are that the region's privacy rules will continue to change at an equally rapid pace into 2022 and beyond.

Prior to 2010, only six jurisdictions had comprehensive data privacy laws and two of these enacted their laws prior to 2000: New Zealand in 1993 and Hong Kong in 1995.

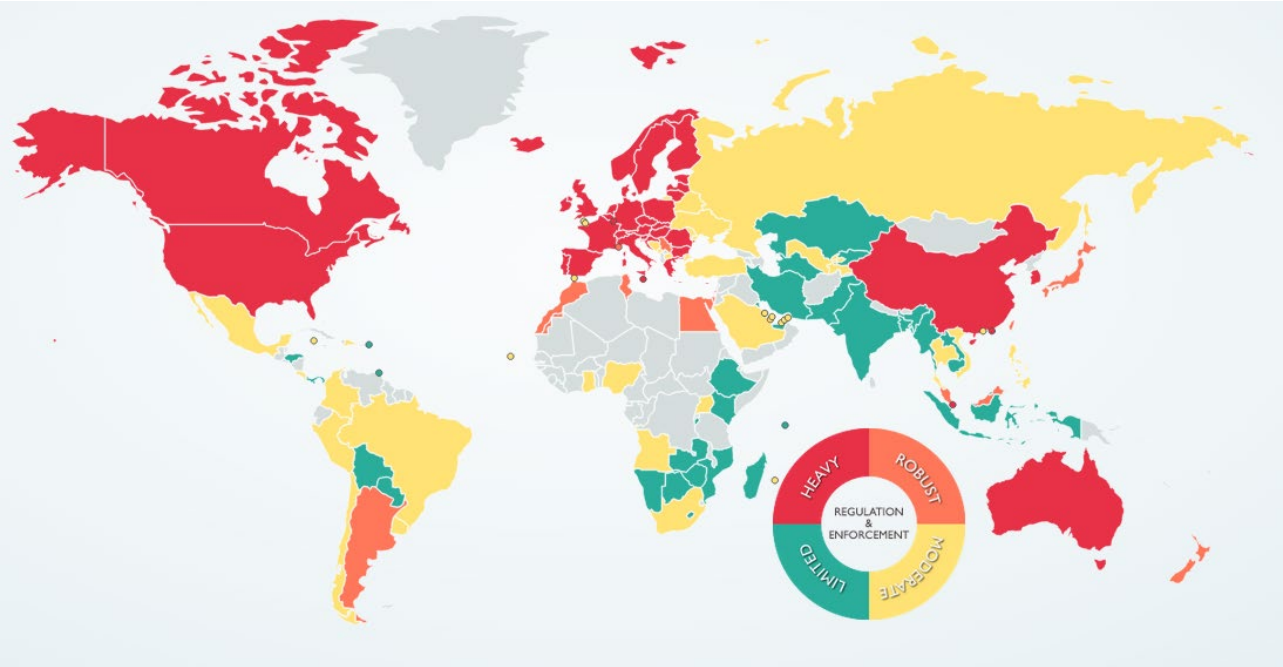
Between 2010 and 2020, 13 more jurisdictions enacted new data privacy laws and seven amended their existing laws (four of the seven jurisdictions amended their laws twice during this 10-year period).

In the next couple of years, we may see as many as eight new or updated laws enacted or introduced into national legislatures. China, India, and Indonesia are the most likely to adopt laws in the short term, followed by Australia, Hong Kong, Malaysia, Sri Lanka, and Vietnam in the longer term. This means that **one-third of the existing privacy regimes will be undergoing significant changes in the next few years.**

While **the laws in the region share the same core data protection elements found in virtually every privacy law in the world**, they each have their **own specific rules** that differ from each other and from those in other regions.

In contrast to the EU, **the wider Asia and Pacific region is characterized by varied legal systems and historical differences** that make it impossible to generalize the laws across the region. It is important to take these differences into account when developing global or regional privacy compliance programmes.

The below world map from the global law firm DLA Piper shows the level of regulation and enforcement of data protection laws across the world:



Source: https://www.dlapiperdataprotection.com/

Laws and regulations you should be aware of for 2022[7]

1. European Union:

The General Data Protection Regulation (GDPR) [8]

The GDPR is a product of the European Union's audacious data protection reform. The strict privacy standards **came into effect on 25 May 2018**. It is generally considered the **toughest existing privacy and security law in the world**.

It imposes obligations onto organizations anywhere, as long as they **handle or collect data related to citizens from or living in the EU**. The EU authorities have the power to levy harsh fines against those who violate the GDPR privacy and security standards, with penalties reaching into the tens of millions of euros.

In June 2021, for example, Luxembourg's data-protection commission (the CNPD), levied a fine proposal of over $425 million against Amazon for its collection and usage practices for personal data.

(Image credit: Cyber-Duck)

GDPR was mainly designed to protect the data subjects' rights in the EU - including citizens, residents and even visitors. It governs the collection, use, transmission, and security of data collected from residents of any of the member countries of the European Union. The law applies to all EU residents, regardless of the entity's location that collects the personal data.

[7] Main sources: A Practical Guide to Data Privacy Laws by Country [2021] by I-Sight; Analysis by Morrison Foerster; UNCTAD report on Data Protection and Privacy Legislation Worldwide, Consumer International Report – The State of Data Protection Rules around the World', GDPR article from Smashing Magazine; https://ico.org.uk/

[8] Useful links:
https://gdpr.eu/compliance-checklist-us-companies/
https://gdpr.eu/compliance/
https://gdpr.eu/checklist/

GDPR requires businesses and government agencies to get explicit consent for data processing, anonymize collected personal data, provide quick notifications of data breaches, safe handling of data transfer across borders, and to appoint a data protection officer.

What is new since May 2018?

The GDPR has become a **global point of reference** for data protection legislation worldwide. Many countries around the world are modernising their privacy rules, using GDPR as a benchmark. This creates new opportunities to increase protection for individuals and facilitate data flows, following GDPR standards.

The importance of data protection to ensure trust in the digital economy and to **facilitate data flows** has also been recognised at international level. For example:

- The mutual **EU-Japan Adequacy Decision** has created the largest area of safe and free data flows in the world, allowing personal data to flow freely between the two economies on the basis of strong protection guarantee (2019);
- The **EU-US Privacy Shield** was invalidated by the European Court of Justice in July 2020. The Privacy Shield was a major agreement between the US (major point of storage of personal data) and the EU, governing the transfer of EU citizen's data to the United States. This mechanism was designed to enable US companies to process EU citizens' data, as long as those companies signed up to its higher privacy standards.
  A privacy advocate challenged the agreement, arguing that US national security laws did not protect EU citizens from government snooping.
  On July 16 2020 the European Court of Justice (ECJ) invalidated the EU-US Privacy Shield program, finding that it did not provide adequate protection for personal data transferred from the EU to the US. The 5,300 American SMEs who used Privacy Shield were given no choice but to adopt the EU's prescribed Standard Contractual Clauses.

Data protection law in the UK after Brexit: With the UK now outside of Europe, there are some changes to GDPR requirements businesses must follow depending on whose data they are processing. The UK is now governed by the UK-GDPR (United Kingdom General Data Protection Regulation) which mirrors the EU version. The UK-GDPR was converted into UK law on 1 January 2021. The UK Data Protection Act 2018 was amended to be read in conjunction with the new UK-GDPR instead of the EU GDPR. It is likely that the UK government will move to consolidate the two amended laws (UK-GDPR and Data Protection Act 2018) into one comprehensive piece of data protection law at a later point. An **adequacy decision** for the UK was adopted on 28 June 2021 by

the EU, **securing unrestricted flow of personal dat**a between the two blocs until June 2025.

Cookie Consent has been reinforced, meaning that explicit consent must be required and cookies wall should not be used as they do not do not offer users a genuine choice.

2. United States

In the United States, **federal data protection laws are approached by sectors,** resulting in the co-existence of hundreds of sectoral data privacy and data security laws. U.S. state attorney generals oversee data privacy laws governing the collection, storage, safeguarding, disposal and use of personal data collected from their states' residents, especially regarding data breach notifications and the security of Social Security numbers. Some apply only to governmental entities, some apply only to private entities and some apply to both.

California and New York are the first states to enact broad legislation with a national impact, but many other US states are also considering data privacy laws.

The Federal Trade Commission Act

The section 5 of the Federal Trade Commission Act (FTC Act) is used to force companies to safeguard collected PII data. A company in the United States is not required to have a privacy policy, but is obliged to comply if the company disclosed a privacy policy. The company also cannot retroactively change its data collection policy without offering an opportunity for users to opt out.

New York SHIELD Act

In July 2019, New York passed the Stop Hacks and Improve Electronic Data Security (SHIELD) Act.

This law amends New York's existing data breach notification law and creates more data security requirements for companies that collect information on New York residents.

The law was enforced in March 2020. This law broadens the scope of consumer privacy and provides better protection for New York residents from data breaches of their personal information.

California Consumer Privacy Act (CCPA)

The most comprehensive state data privacy legislation to date is the California Consumer Privacy Act (CCPA). It is inspired by GDPR and was strengthened in November 2020 when the California Privacy Rights Act (CPRA) was passed (see below).

The CCPA came into effect on 1 January 2020 and gives California citizens the right to opt out of their data being sold. They can also ask for the disclosure of any data that has been collected and they can ask for that data to be deleted. Unlike GDPR, the CCPA only applies to commercial companies that:

- process the data of more than 50,000 California residents a year, OR
- generate gross revenue of more than $25m a year, OR
- make more than half of their annual revenue from selling California residents' personal data

The CCPA is cross-sector legislation that introduces important definitions and broad individual consumer rights and imposes substantial duties on entities or persons that collect personal information about or from a California resident. These duties include informing data subjects when and how data is collected and giving them the ability to access, correct and delete such information. This notice must be disclosed in a privacy policy displayed on the entity's website that collects the data.

California Privacy Rights Act (CPRA)

The California Privacy Rights Act will come into force on **1 July 2023**. Its key points include:

- **Right to rectification:** This allows a consumer to request the correction of inaccurate personal information;
- **Right to restriction:** This grants consumers the right to limit the use and disclosure of their sensitive personal information;
- **Sensitive personally identifiable information:** This updates the definition of personal information. Certain types of information, like a consumers' Social Security number, must be treated with particular care;
- One of the more progressive changes within the CPRA is **how it will be enforced:** The CPRA establishes a new privacy regulator. The California Privacy Protection Agency will be empowered to fine transgressors, hold hearings about privacy violations and clarify privacy guidelines. It is a five-member board, and it starts enforcing six months after the CPRA goes into effect on July 1, 2023.

Virginia's Consumer Data Protection Act (CDPA)

Virginia's Consumer Data Protection Act (CDPA) was passed on 2 March 2021 and will be effective as of 1 January 2023.

It grants Virginia consumers rights over their data and requires companies covered by the law to comply with rules related to the data they collect, how it is treated and protected and with whom it is shared.

The law contains some similarities to the EU GDPR provisions and the California Consumer Privacy Act. It applies to entities that do business in Virginia or sell products and services targeting Virginia residents and that also do one of the following:

- Control or process the personal data of 100,000 cnsumers or more;
- Control or process the personal data of at least 25,000 consumers and earn 50% of their revenue by selling personal information.

The Virginia CDPA requires companies covered by the law to assist consumers in exercising their data rights by obtaining opt-in consent before processing their sensitive data, disclosing when their data will be sold and allowing them to opt-out of it. It also requires companies to provide users with a clear privacy notice that includes a way for consumers to opt out of targeted advertising.

Colorado Privacy Act (CPA)

In June 2020**,** Colorado became the third U.S. state to pass a privacy law.

The Colorado Privacy Act grants Colorado residents rights over their data and places obligations on data controllers and processors. It contains some similarities to California's two privacy laws, the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), as well as Virginia's recently passed Consumer Data Protection Act (CDPA). It even borrows some terms and ideas from the EU GDPR.

While there are similarities, such as some form of a right to opt-out, special protections for sensitive data and the adoption of some privacy-by-design principles, the significant differences are in the details.

The CPA applies to businesses that collect personal data from 100,000 Colorado residents or collect data from 25,000 Colorado residents *and* derive a portion of revenue from the sale of that data.

3. Brazil

Brazil's data protection law (Lei Geral de Proteção de Dados Pessoais in Portuguese, or LGPD) was implemented in 2020 and with effectiveness date set at 1 August 2021. **The law contains provisions similar to the GDPR and aims to regulate the treatment of personal data of all individuals or natural persons in Brazil.** That means, like the GDPR, that this law applies to you if you process the data of Brazilian residents, **even if your company is not based in Brazil**. Companies and groups that do not follow the law's terms and directives may receive a fine as high as 2% of their sales revenue, or even up to $50 million Brazilian Real (approximately $12 million USD).

In a nutshell, these are the provisions set by the law:

Consent:

Under the LGPD, personal data can be processed either with a data subject's consent or when:

- It must be processed to comply with a legal obligation;
- It is necessary for the public administration to execute public policies;
- For research purposes;
- To protect the life or physical safety of the data subject.

Data breach notification:

In the case of a data breach, data controllers must notify the National Data Protection Authority within a "reasonable time" from when the breach occurs if there is a potential for risk or damage to the data subjects involved.

Data subjects' rights:

The rights granted to Brazilian subjects are similar to those granted under the GDPR and allow them to:

- Confirm the existence of treatment of their data;
- Access their data;
- Correct incomplete, inaccurate or outdated data;
- Transfer their data to another service provider or product (data portability);
- Delete their data;
- Have knowledge of any public and private entities with whom the controller has shared their data;

- Receive information on what happens if they do not provide consent to the processing of their data;
- Revoke consent to the processing of their data.

4. South Africa

The **Protection of Personal Information (POPI) Act** presents one of the most disruptive compliance changes in South Africa's business history, as it changes the way business deals with information in an information-driven society. Full compliance to the POPI Act is required as from **1 July 2021.**

Global compliance

If your customer base includes people in the EU and citizens of other countries with privacy laws, such as the State of California, **you have to comply both** with the California Consumer Privacy Act (CCPA) and with GDPR. These batches of legislation generally align — but they do not always match.

Take the use of cookies, for example. Under GDPR, you must get active consent from a user before you place a cookie on their device, bar those strictly necessary for your website to function. However, under the CCPA, you must disclose what data you are collecting, and enable your customer to deny you permission to sell their data. But they do not have to actively agree you can collect it. That is why the **EU is pushing for international standards to simplify global compliance.**

Conclusions

The need for trust and accountability for the handling and treatment of personal information is growing in the minds of customers, consumers and other stakeholders alike. But the risk is broader than regulatory compliance; **companies must have the right competence, processes and systems in place to be able to abide by these rules.**

With the number of complaints and fines related to privacy and data protection on the rise, there seems to be a growing need for guidance.

Businesses interested to further mitigate data privacy risks may consider looking into information security management systems (such as ISO/IEC 27701 standard[9]).

FIDI Global Alliance has been a pioneer in data privacy protection management by incorporating stringent data privacy elements into its FAIM quality standard as early as 2015 (FAIM 3.1), giving FIDI Affiliates an important advantage in preparation for the EU GDPR. These elements were reinforced in the following version of FAIM version (FAIM 3.2).

The FAIM Standard includes requirements related to the protection of personal information. A FIDI Affiliate needs to demonstrate that their company has a documented data (privacy) protection procedure in place, ensuring that personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments described in your privacy notice as well as a process in place to control data (privacy) protection of their supply chain.

[9] Building on the ISO/IEC 27001 requirements, ISO/IEC 27701 was published on August 6, 2019 and provides the requirements and guidance for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS) for the processing of Personally Identifiable Information (PII).

CONTACT DETAILS

For questions or comments regarding this report, please contact Marie-Pascale Frix, Business Intelligence Manager, at marie-Pascale.frix@fidi.org

FIDI Global Alliance
Fountain Plaza Building 501, 1st Floor
Belgicastraat 1
1930 Zaventem
Belgium
fidi@fidi.org

www.fidi.org