DATA PROTECTION WORLD FORUM

GROUND LABS

The Six Foundations of Data Privacy Regulation

eBook produced by Ground Labs in association with Data Protection World Forum

Contents

The six most commonly discussed data protection regulations are the European Union's GDPR, the California Consumer Privacy Act (CCPA) and Health Insurance Portability and Accountability Act (HIPAA) in the United States, Brazil's LGPD, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the Australian Data Privacy Law.

These regulations establish the who-what-when-where-how and why of data governance - a set of principles, practices and in some cases obligations that define how data is managed, reported and maintained. Effective data governance ensures that data is consistent and trustworthy and is not misused. Importantly, defining what data governance means to an organisation is one of the good practices that should be adopted in an organisation's journey towards compliance.

By understanding the common elements in each regulation as it relates to data governance, we can gain a more thorough understanding of the actions available to businesses in the stated regions which will subsequently help to prepare organisations for likely additions to data law as they become enacted. Also it's important to note that organizing and improving data flows does not just ensure compliance with current regulatory regimes but acts as a strong foundation for future legal developments.

The Big Six

1. GDPR

General Data Protection Regulation

EU law on data protection and privacy in the European Union and the European Economic Area.

2. CCPA

California Consumer Privacy Act

State statute intended to enhance privacy rights and consumer protection for residents of California, United States.

3. HIPAA

Health Insurance Portability and Accountability Act

Stipulate how personally identifiable information maintained by the healthcare and healthcare insurance industries.

4. LGPD

Lei Geral de Proteção de Dados Pessoais

Applies to any business or organization that processes the personal data of people in Brazil.

5. PIPEDA

Personal Information Protection and Electronic Documents Act

Foverns how organizations collect, use and disclose personal information in the course of commercial business.

6. DPL

Data Protection Law

Gives individuals control over their personal data and protects against its misuse in both public and private sectors.

01:

Commonalities in Relation to Data Governance

Scope

In June 2018, California passed the CCPA – a law designed to enhance and protect consumer privacy, modelled primarily on the EU's General Data Protection Regulation (GDPR). The act went into effect in 2020 and is due to be updated in 2023. CCPA shares many commonalities with GDPR. Regarding personal scope, both share a focus on information regarding an identifiable natural person but differ on how they define such a person. GDPR protects the data subject or individual residing within the EU despite their nationality.

The CCPA on the other hand protects the rights of California "consumers" and "residents", the law goes as follows: "(1) every individual who is in California for other than a temporary or transitory purpose, and (2) every individual domiciled in California who is outside the State for a temporary or transitory purpose." Unlike GPDR, CCPA protects personally identifiable information relating to an individual or their household.

Similarly, Brazil's Lei Geral de Proteção de Dados (LGPD) which passed in 2018 and became effective in February 2020, attempts to standardise data protection laws across Brazil. Taking direction from the GDPR, LGPD's scope is notable.

Any business or organisation that processes Brazilian citizens' personal data, regardless of location of the business must abide by LGPD.

Australian Data Privacy Laws were introduced in 1988 with the Privacy Act. Amendments were made in 2013 with the Privacy Regulation, and the latest change was made in 2017 to cover notifiable data breaches. The Australian Privacy Principles (APPs) apply only to certain people, known as "APP Entities". These include, Australian or Norfolk Island government agencies, Australian businesses with a turnover of more than $3 million AUD, Australian businesses with a turnover of less than $3 million AUD that trade in personal information, provide health services, or have opted-in to be bound by the APPs.

In comparison, HIPAA, passed in 1996, differs greatly from GDPR in terms of its focus. HIPAA relates only to legal persons, i.e. entities and their business associates covered by the Privacy Rule. The law has emerged into greater prominence in recent years with the proliferation of health data breaches caused by cyberattacks and ransomware attacks on health insurers and providers. It protects individually identifiable health information, i.e. protected health information. Likewise, Canada's PIPEDA, amended in 2015 to include The Data Privacy Act, applies to businesses based in Canada and businesses that collect data from Canadian visitors.

This law does not apply to non-profits, political parties, and associations. Quebec, Alberta, and British Columbia are exempt from PIPEDA unless the business operates entirely from these provinces. Unlike the GDPR, PIPEDA's scope is limited and does not have a strong international reach.

Privacy by Design

Implementing a Privacy by Design (PbD) approach is key for many businesses to unlock a compliance strategy that is compatible with numerous privacy frameworks. Article 25 of the GDPR outlines the implementation of proactive privacy measures into the design process. The aim is to maximise privacy when collecting user data from the architectural stage by embedding relevant safeguards and procedures. In other words, privacy is as integral to an operation as functionality.

The CCPA does not require explicit PbD obligations, although it does require businesses to adopt organization-wide security protocols that are appropriate to safeguard collected consumer data.

Various PbD requirements are fully compatible with CCPA. For example, purpose specification and limitation requirements are obligated under CCPA and should be implemented from the start.

Additionally, PbD is also compatible with HIPAA through obligations such as purpose specification, data minimisation, purpose limitation, security and transparency. Brazil's LGPD is also compatible with a PbD strategy via Article 6 of the LGPD, the eighth principle of prevention demands "measures to prevent the occurrence of harm due to the processing of personal data". Furthermore, PbD is a principle that is not formally required under Australian Privacy Laws but is indirectly addressed in APP 1. APP entities are required to take reasonable steps to implement practices, procedures, and systems to ensure compliance.

PbD is a recognised deficiency in PIPEDA. The Department of Justice is currently examining what greater accountability would look like in a renewed Privacy Act. It has been noted that an amendment should be made to "demonstrate meaningful and accountability including effective oversight" according to the Department of Justice. Implementing a PbD approach through oversight by a Data Protection Authority, conducting data protection impact assessments as well as a legal requirement to ensure privacy by design and default are key amendments that would make the law's data governance more robust.

Personally Identifiable Information (PII)

The GDPR defines PII as any data that can be used to clearly identify an individual. Examples include, national insurance numbers, mailing address, email address and phone numbers, IP addresses, login ID details, social media posts and digital images, geolocation, and behavioural and biometric data. Sensitive personal data requires its own encryption security strategies and categorisation. The legislation requires organisations to be extra strict with the handling and storage of sensitive personal data. CCPA's definition of PII is more comprehensive than the GDPR's. It includes any information that is capable of being associated with either a consumer or a household. However, CCPA does not provide additional restrictions on sensitive data, unlike GDPR.

Australia's privacy law refers to 'personal information (PI)', the conceptual equivalent of the GDPR's PII. It is defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable, regardless of whether the opinion may be true or recorded in material form. However, The Privacy Act 1988 does not make it clear whether IP addresses, metadata and cookies fall within this category. Under the APPs, an APP entity is obligated to provide a Privacy Policy that contains information about what types of personal information it collects and stores, how it collects and stores it and for what purposes.

GDPR has the same requirements but includes additional information such as

contact details of certain representatives within the company, details of the how long that PI is stored, and the lawful basis for which it is processed.
LGPD does not offer a specific definition but loosely defines personal data as any information relating to an identified or identifiable natural person in Brazil. Anonymised data is not considered personal data unless it can be easily de-anonymised.

Under HIPAA and revisions to HIPAA made in 2009's Health Information Technology for Economic and Clinical Health (HITECH) Act, HIPAA individually identifiable information is defined as information that is a subset of health information, including demographic information collected from an individual, information that is created or received by a healthcare provider, health plan, employer, or health care clearinghouse, and information that relates to the past, present, or future physical health or condition of an individual.

Additionally, it includes the past, present, or future payment for the provision of health care to an individual and any information that identifies an individual or presents a reasonable basis to believe the information can be used to identify an individual. Furthermore, HIPAA defines protected health information (PHI) as any individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted/ maintained in any other medium. Under PIPEDA, PII is defined by any factual or subjective information about an identifiable natural person. Examples include, age, name, ID numbers, opinions, credit records, medical records, social status, income, and existence of a dispute between a consumer and a merchant.

Right to be Forgotten

Article 17 of GDPR enforces stronger data subject rights and has strengthened the conditions for consent. One of the most notable data subject rights includes the "right to be forgotten", otherwise known as the "right to erasure". This entitles the data subject to force the data controller to erase the personal data held on them and to cease further diffusion of data.

Additionally, the right provides the potential to stop third parties from processing the data. This requires an organization to locate all an individual's PII and any information that can be cross-referenced with other data points to become PII. It is therefore essential that companies incorporate such flexibility within their data governance strategies from the architectural level.

CCPA offers an equivalent, commonly referred to as the "right to deletion" but it differs significantly to GDPR in the sense that it is not an absolute right and only applies under certain circumstances. Likewise, PIPEDA offers a very limited right to deletion, section 4.9 states: "Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information." On the other hand, LGPD enumerates a similar law to GDPR's by granting the right to access, rectify and erase personal information.

Australian Privacy Act does not currently provide data subjects with the right to be forgotten. However, the federal government is currently analysing potential reforms to the law that include the right to erasure on request. This is unlikely to be implemented for many years.

HIPAA differs greatly from GDPR in this regard. It permits some degree of PHI disclosure without explicit consent from patients, unlike GDPR which puts a strong emphasis on gaining active consent for PHI when it exists outside of direct health care. The right to erasure is also unavailable to patients under HIPAA. Healthcare organisations in the US who collect data on EU residents will need to have the ability to locate and delete all data pertaining to EU residents in order to comply with GDPR.

02:

Data Discovery as Part of an Overall Data Governance Strategy

Discovering the value behind structured and unstructured data that is scattered across an organisation's multiple storage systems (such as servers, workstations, personal devices etc) is a sizable task, but one that is paramount to developing good data governance strategies and compliance. With a continuous flow of data to the back end, analysts can become preoccupied with locating where relevant data is stored, leaving little time to actually analyse and secure it. The importance of discovering and rationalising data in the modern market cannot be understated.

Knowing what data is in an organisation's possession, understanding why it was collected, and pinpointing where it is stored (and how it moves in the system), are steps that must be taken periodically before any value can be extracted from the data for actionable business and compliance purposes. Data discovery is the cornerstone of a solid data governance plan that provides teams across an organisation with the veracity needed to make critical business decisions.

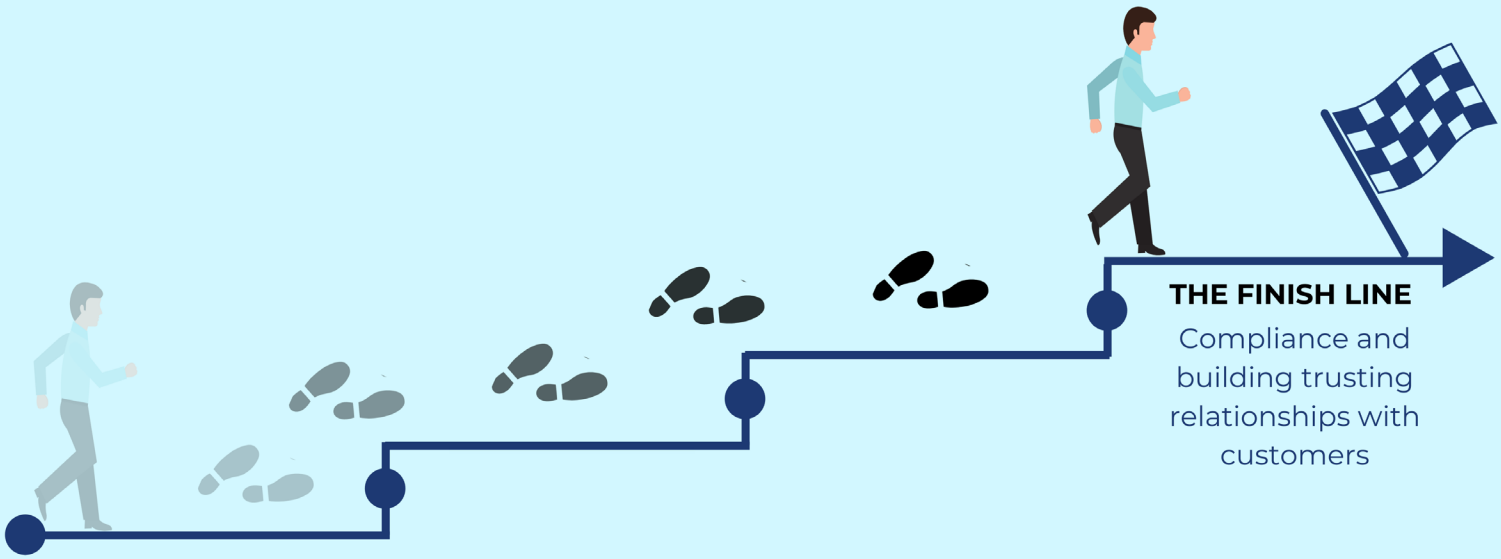
Sole dependence on human labour to find, rationalise and make sense of relationships between data, is quickly becoming unfeasible and an unrealistic expectation to place on employees, who, many of which, may not be experts in IT.

The shift from manual processing to smart governance and discovery of data is providing organisations with various invaluable advantages such as: cleansing data for future use, aggregating data from multiple sources in a shorter amount of time, providing greater control over data, and scaling data across an organisation with clear fidelity.

> *"The shift from manual processing to smart governance and discovery of data is providing organisations with various invaluable advantages."*

Crucially, data discovery auditing tools can be used to facilitate the detection of unencrypted personally identifiable information (PII), such as credit card information and names that are sprawled across an entire enterprise. This is a key practice to be undertaken to ensure compliance with data protection regulations such as GDPR and CCPA, and to prevent sensitive information from being hijacked by cybercriminals. It is essential to a corporate reputation, customer relationships and the bottom line that PII and sensitive information is governed securely and is consistently classified. With the verification of GDPR compliance by a DPA often being managed irregularly, it can be difficult to distinguish if an organisation has been consistently abiding by GDPR principles, as well as other regulations. At the same time, data subjects are becoming more literate in regard to their privacy rights. However, despite the greater ease GDPR has afforded to requesting access to the personal data held on them by an organisation, it is beyond the data subject's capability to perceive just how protected their PII and sensitive information is.

It is imperative that businesses prioritise a good data governance strategy if they are to utilise the competitive advantage that GDPR compliance affords them.



As more regulations are predicted to be enacted and continue in the pattern of extraterritorial scope, a gradual shift towards implementing a smarter way to locate, secure and manage data is key to staying ahead in an increasingly privacy-aware market.

Data may be secured using a variety of methods. Examples include:

Mask in Place
Overwrite the data making it unidentified

Before	After
123-555-1212	12########12
jwhite@domain.com	jw##############om
5270 4267 6450 5516	5270 4##########5516

Permanent Delete
Permanently delete (Wipe) the data

Encrypt
Encrypt the data with a password or token

Secure Quarantine
Move the data to a s ecure location

03:

Good Practice in Managing and Improving Data Workflows

Workflows are an integral element in data analytics, but as the volume of data being handled increases within an organisation, manual workflows fall short in mitigating the complexities involved in business analytics. After you have discovered what data your organisation has, streamlining your data processing workflows will enable your organisation to be more efficient and responsive; it serves as an important impetus for businesses to improve their GDPR compliance.

Good data management requires businesses to provide an appropriate interpretation of GDPR that aligns with their organisational structure and aims. Tools and resources that streamline and support the automation of repetitive tasks can be leveraged to effectively meet GDPR's requirements.

Undertake a workflow analysis

Understanding your workflows is an important first step in optimisation. A workflow analysis would allow you to review and document your workflows for weaknesses before the process can be automated. Often, businesses find themselves tackling the issue of spending too much time manually sending emails back and forth to follow up on data workflows. This is time consuming and increases the risk of error. Workflow analysis goes beyond just automating those workflows but building a thorough understanding of who access to data at each step, what their process is and why it exists.

Integrate consent into workflows

Under GDPR, organisations are obliged to take appropriate actions to ensure revocation of consent is managed effectively. This comes back to implementing a privacy by design approach; an automated workflow can provide clarity in each step of fulfilling the data subject's request. A central dashboard that allows Data Protection Officers to oversee and manage all requests within GDPR's response time frame is essential to upholding data subject rights.

Automating the proportionality principle

This principle says that all personal data collected and processed must be done so only to the extent that it is necessary. Data must be deidentified and used insofar as it meets the identified purpose that is sought by the workflow. Automating the process can ensure that unnecessary or excess data is deleted or anonymised and can provide airtight compliance.

Ensure flexibility and adaptability to changing legislation

An automated workflow can adapt to changing business models and legal provisions without requiring employee intervention. This allows employees to spend their time more valuably on tasks that require manual processing.

Follow audit trails

A workflow management software system can be extremely useful in tracking both internal and external audit trails. In a large organisation with many employees focusing on many different workflows, an audit trail can provide verification of all activities and their participants with exact precision. It can provide specifics such as names, dates, times, and the information that was captured. Importantly, reviewing an audit trail can be used to identify errors, allowing the system to be continuously improved.

04:

Building Trust in Data Management

Gaining the trust of your customers, vendors and employees is vital for creating and growing a successful business. But trust, which can take years to build, can very quickly disintegrate, when it becomes apparent that data management has gone wrong – whether the issue is data protection, data privacy or cybersecurity.

Perhaps the most high-profile problem, regularly hitting the headlines, are data breaches. And they don't just cause the hard-won trust of customers to drain away. They can also have an unwanted impact on the company stock share price and result in eye-wateringly large penalties.

So, how do you build and retain trust in your data management, in this challenging environment, while simultaneously dealing with heavy regulation, the pressure of customer expectations and the imperative of compliance?

Strategy and Plan

Building customer trust in your data management starts with robust data governance and a strong data-management strategy and plan. No business wants to be caught out by a data problem and have to 'firefight'. Instead, it's better to embed the importance of good data governance and management within the culture of the organisation and put in place solid policies and procedures. That's not enough, however.

Good data governance means that data is used correctly across the organisation and that everyone is committed to this goal, not just the data managers. The policies and procedures therefore need to be communicated throughout the organisation, clearly, consistently and regularly.

Customers must also, of course, be kept informed appropriately of the company's effective and thorough approach. Brands build trust with their consumers not just by having responsible data-management practices, but also by ensuring customers know their data is in safe hands.

> *Trust, which can take years to build, can very quickly disintegrate, when it becomes apparent that data management has gone wrong.*

There are a number of key elements to include in an effective data-management strategy and plan. It should encompass, for instance, how you gather and analyse data; how you approach data discovery – i.e. making sure you know exactly what data you hold, why and where; how you organise, store and protect it; and how you share it.

The data management strategy and plan, similar to the company's other operational strategies and plans, must be aligned with its business objectives. The organisation will be seeking to deliver value to customers, to retain its

existing customer base and attract new business. That includes gaining and keeping the trust of its customers, when it comes to data management.

The days of gathering and storing every piece data possible are over, you now only retail data to meet business objectives.Otherwise, you run the risk of obtaining, storing and analysing the wrong data, which could be a costly mistake.

Data Breach Challenges

The job of retaining customers' trust has not been helped by a number of high-profile data breaches over the years. This means that customers may have even higher expectations around the security of the data they provide to companies, and how it is managed. Recent research shows businesses can lose more than half their customers after a data breach.

They are well aware that sensitive and confidential data can be accessed and may well have had their fingers burned already. They know that criminals can do serious damage, armed with a date of birth, email address and financial information. And no company wants to be the one that has to break the bad news to customers that their credit-card details have fallen into the wrong hands.

There are many examples of reputable, globally recognised brands taking a hit. Take the example of Verizon, which had 6 million customer accounts exposed in 2017 after a contractor failed to secure their systems.

Compliance obligations will remain central to an organisartion's concerns, not least because of the monetary impacts that failure will bring. A report released in June revealed that in Q1 this year alone, more than 1.6bn consumer records in the US were breached, indicating that 2020 is likely to exceed 2019's figures.

Any data management problem can be a hard blow for a company to recover from. But there are some key points for businesses looking to do things better. Transparency can build trust, as can demonstrating genuine commitment to managing data securely, appropriately and effectively.Customers won't want to get the impression that it's just a tick-box exercise for the company or that it's mainly motivated by fear of paying fines.

However, despite the many challenges, it's clear that good data governance and management is key for delivering competitive advantage. As BCG reports in its 2019 paper Good Data Starts With Great Governance: "In the coming years, the companies with the best data capabilities—and best data quality—will dominate."

05:

Interview with Stephen Cavey, Chief Evangelist and Co-founder at Ground Labs

The biggest development in data protection in the last two years is that companies are starting to move away from 'perimeter-based

It's not about having the biggest wall around your 'castle'. With the increase in regulations over the last few years, businesses need an 'inside-out' strategy now, where they protect every single area, starting with the data itself, but also continuing with traditional protection systems such as firewalls. Another development is that with sweeping laws coming through, data security is becoming a board-level issue, as the cost of getting it wrong is so great.

Looking to the future, the biggest data-protection challenge that companies will face in 2021, is that they may be falling victim to assumptions about how ready they are for compliance with new data-protection laws. For instance, some processes within businesses are 'off the radar' of data-protection managers. There are also legacy issues arising from practices undertaken five-eight years or so ago, where the employees have since left the business. There might be applications in place in archives full of millions of records that today's data protection teams are not aware of. Handover notes may be lost. The only way to understand the risk is to remove assumptions, start from scratch and undertake data discovery across the whole business. This often reveals problems that the company wasn't even aware of – unspeakable amounts of data are being found within companies that it had no idea they were holding . The world has 'data-breach' fatigue – there are not so many breaches making headline news anymore, as it has become such a common issue.

> *"The world has 'data-breach' fatigue – there are not so many breaches making headline news anymore, as it has become such a common issue."*

Coronavirus has had a big impact on organisations' approaches and concerns around data protection. Companies found themselves having to introduce remote working overnight, with no time to put in place the tools and platforms needed to ensure data is handled securely. One of the challenges was that laptop manufacturers couldn't meet the demand for equipment for employees working at home, and there were delays in the supply chain. Many organisations therefore had to adopt BYOD even if they had previously been against it. This meant that company data was ending up on personal devices, with no control over it. Companies can mitigate the risk, but that takes time and they didn't have time. They also didn't know how secure each employee's wi-fi was.

> *The biggest data protection challenge that companies will face in 2021, is that they may be falling victim to assumptions about how ready they are for compliance with new data protection laws.*

Companies have limited resources to deal with their defences, whereas well-funded criminals have unlimited resources and time. And the 'bad guys' are taking advantage of the coronavirus situation. Criminals are adapting – they know employees are working from home and that they are more vulnerable to phishing attacks. There have already been reports of criminals impersonating email accounts and asking for urgent transfers of large sums of money, which have been made.

Steve Cavey co-founded Groundlabs in 2007 – he is a security professional with a historical focus on electronic payments and data security compliance.

Contact Details

UK: +44 203 137 9898

US: +1 737 212 8111

Ireland: +353 1 903 9162

Australia: +612 8459 7092

Asia: +65 3133 3133

Visit Ground Labs