# Local Privacy Laws in a Globalized World

Shantanu Sharma
New Jersey Institute of Technology
Newark, USA

Ethan Myers
Colorado State University
Fort Collins, USA

Lorenzo De Carli
University of Calgary
Calgary, Canada

Ritwik Banerjee
Stony Brook University
Stony Brook, USA

Indrakshi Ray
Colorado State University
Fort Collins, USA

## Abstract

Personal data has emerged as a highly valuable yet sensitive asset that drives business decisions, enables targeted advertising, and generates substantial revenue for companies, while simultaneously facilitating invasive monitoring of users. In recent years, research on digital privacy violations, including undue access, collection, and sharing of user data, has grown significantly. Much of this research adopts the European General Data Protection Regulation (GDPR) as the primary reference framework. This is reasonable, as GDPR was a pioneering legislation, and many of its stipulations are clear and unambiguous. However, we argue that focusing solely on GDPR (and a small set of other Western regulatory frameworks) ignores privacy-related concerns, attitudes, and problems faced by users from other locales, creating a significant research blind spot.

This work systematically normalizes the heterogeneous legal requirements of multiple data protection laws into a unified abstraction aligned with the data lifecycle, which forms the foundation for the implementation of such regulations. We further investigate the implications of these laws on different stakeholders, including users, organizations, and governments. Overall, this work aims to broaden the digital privacy research community's perspective and to serve as a set of guiding principles for developing technological privacy solutions spanning multiple countries.

## CCS Concepts

• **Security and privacy → Privacy protections**; **Social aspects of security and privacy**; **Usability in security and privacy**.

## Keywords

Data protection laws; user privacy

**ACM Reference Format:**
Shantanu Sharma, Ethan Myers, Lorenzo De Carli, Ritwik Banerjee, and Indrakshi Ray. 2026. Local Privacy Laws in a Globalized World. In *Proceedings of the Sixteenth ACM Conference on Data and Application Security and Privacy (CODASPY '26), June 23–25, 2026, Frankfurt am Main, Germany*. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3800506.3803491


*CODASPY '26, Frankfurt am Main, Germany.*

ACM ISBN 979-8-4007-2562-3/2026/06
https://doi.org/10.1145/3800506.3803491

## 1 Introduction

Personal data is a valuable and sensitive asset, driving business decisions, enabling targeted advertising, and generating revenue for companies. However, this potential for monetization also creates significant privacy risks. Investigations in data management practices have repeatedly found issues, e.g., overcollection [18, 22, 33, 39], undue data sharing [10, 22, 26, 32], and negligent data management [16, 21, 35]. Probes of user attitudes suggest that users may underestimate the risk of such violations [4, 6, 8, 9, 41], or misunderstand the implications of data collection [17, 23, 27, 30, 37]. Given these findings, it is important for academic research to continue shedding light on issues related to digital privacy.

Privacy research typically defines a *privacy threat model*, outlining specifically how data collection/processing operations may create risks for the owner of the data. While in some work this model is defined implicitly or based on informal considerations ([5, 11, 12, 24, 25, 29, 31]), the majority of research effort measure privacy violations with respect to a regulatory framework.[1] Doing so is reasonable, as regulations define unambiguous expectations that reflect the expectations of relevant stakeholders (government, citizens) in a given locale. Unfortunately, the current body of research does not reflect the global diversity of ***data protection privacy laws***. An exploratory review of 21 recent digital privacy-focused papers (see Table 1) shows that a simple majority of them (14 out of 21) only consider the European General Data Protection Regulation (GDPR); and more than 95% (20 out of 21) only consider European and/or North American regulatory frameworks (GDPR/CCPA/COPPA/CalOPPA/PIPEDA) — also refer to §1.1 to see our discussion on how existing work focused on specific definitions of personal/user data and consent models, and hence introducing a blind spot in global application of data protection laws. This narrow geographic focus opens up questions about generalizability; as it may overlook privacy-related concerns, attitudes, and problems of non-European and more broadly non-Western users, causing a significant research blind spot.

As privacy researchers, we believe it is important for research in this space to incorporate awareness of the digital privacy concerns of the global user community. Thus, this work aims to provide a comparative analysis of data protection laws/regulations, considering frameworks beyond North America and Europe, including those from Asia, Africa, and South America. Specifically,

[1] *E.g.*, [10, 13, 14, 20, 22, 23, 26, 27, 30, 32–34, 36–39] and see Table 1.

we review GDPR (EU), CCPA (California, US), DPDPA (India), PIPL (China), POPIA (South Africa), and LGPD (Brazil).[2]

**Our objective.** *Our objective is to examine how different jurisdictions implement data protection through regulatory laws.* While our goal is not to achieve exhaustive global coverage, we identify structurally distinct regulatory paradigms and demonstrate that overlooking these differences introduces critical blind spots in privacy research. This paper provides researchers with knowledge, ensuring the regulatory foundations of technical work on privacy are aware of and informed by the global diversity of regulations. Overall, the data protection laws considered in this paper apply to ≈38.3% of the world population.

**Data protection laws and data life cycle.** Conducting such a review is challenging for several reasons, such as (i) regulations across diverse countries are shaped by distinct regulatory traditions and practices, as well as by different conceptualizations of privacy rights and violations; (ii) the scope of the law itself may differ, with regulations in different locales targeting different aspects of the privacy problem; (iii) differences in how they treat user rights for actions such as data breaches, unauthorized data collection, and unauthorized data sharing.

To systematically understand these regulations, thus, we analyze them through the lens of the digital data processing life cycle, which serves as the operational axis, where users, organizations, and governments are not independent entities; rather, they represent different levels at which privacy is operationalized. We demonstrate how these laws influence each stage of the data life cycle and identify potential threats that may compromise privacy at these stages. Specifically, we study data protection laws' differences among entities and their roles based on data lifecycle abstraction, such as collection, processing, storage, transfer, and deletion, as shown in Table 2.

Overall, we find that data protection laws differ significantly in scope, definitions, and enforcement mechanisms. This creates challenges for both researchers who intend to measure and/or address privacy issues. Overall, we tackle the following research questions:

**➤ RQ1: How do differences in user-level legal protections lead to inconsistent legal outcomes for the same digital data-collection behavior?**

§4.1 shows that different laws define personal and sensitive data differently and also differ significantly in the rights users can exercise to control their data.

**➤ RQ2: How do differences in organizational obligations across data protection laws constrain the design of a unified and technically enforceable data-processing architecture?**

Organizations with a global footprint need to implement data-processing principles, breach-notification procedures, cross-border transfer rules, deletion requirements, and accountability mechanisms. However, §4.2 shows that these aspects differ across regulations, potentially causing problems for organizations.

[2] A comparative analysis of every possible data protection regulation is beyond the scope of a single paper, and we consider it unnecessary. Instead, we argue that it is enough to show structural differences between the GDPR and a small number of selected other regulations as counterexamples.

| Paper | Regulations considered | Year |
|---|---|---|
| Zimmeck et al. [39] | COPPA; CalCOPPA (US) | 2017 |
| Reyes et al. [33] | COPPA (US) | 2018 |
| Zimmeck et al. [40] | GDPR; COPPA | 2019 |
| Jia et al. [16] | GDPR | 2019 |
| Mohan et al. [23] | GDPR | 2019 |
| Ayalon et al. [6] | GDPR | 2019 |
| Fan et al. [10] | GDPR | 2020 |
| Singh et al. [36] | PDPB (India) | 2020 |
| Zhang-Kennedy et al. [38] | PIPEDA (Canada) | 2021 |
| Qamar et al. [30] | GDPR; PDPA (Singapore) | 2021 |
| Nguyen et al. [26] | GDPR | 2021 |
| Kollnig et al. [18] | GDPR; COPPA | 2021 |
| Nguyen et al. [27] | GDPR | 2022 |
| Koch et al. [17] | GDPR | 2023 |
| Xiang et al. [37] | GDPR | 2023 |
| Sassetti et al. [34] | GDPR | 2023 |
| Ferreira et al. [13] | GDPR | 2023 |
| Herwanto et al. [14] | GDPR | 2024 |
| Krämer et al. [19] | GDPR | 2024 |
| Li et al. [20] | GDPR | 2024 |
| Liu et al. [22] | GDPR; CCPA (US) | 2024 |

**Table 1: Overview of privacy compliance studies.**

**➤ RQ3: How do differences in regulatory oversight and penalty structures result in risks to be faced by developers operating across multiple jurisdictions?**

Data protection laws not only offer different things to the user and the organization collecting user's data, but §4.3 discusses that data protection laws have significantly different actions that the government/regulator takes when data protection laws are followed and/or violated by organizations.

## 1.1 Limitations of Using Localized Laws

**The majority of existing work focuses on GDPR.** A common theme among technical studies analyzing the privacy of digital systems is reliance on privacy regulations as a basis for threat modeling. As GDPR is extremely comprehensive, many studies refer to it as the gold standard, which explains why the majority of studies, as shown in Table 1, used GDPR as their legal framework baseline. However, this introduces limitations when privacy models are applied outside the conceptual and jurisdictional reach of such regulations, as the *requirements change dramatically*, as we described in this work. We also note that this problem is not specific to GDPR—any study relying on a single regulation risks being overly specific. In a globalized world, such a practice introduces blind spots that limit the ability to generalize across regions and thus the applicability of research outcomes.

Below, we investigate how ***differences in privacy regulations affect two significant limitations: variability in definitions of personal data and in consent/privacy requirements***, which have been considered in most existing privacy analysis work.

### 1.1.1 Definitions of Personal and Sensitive Data.

While data protection laws focus on personally identifiable information (PII), definitions of personal and sensitive data vary across regulations. Most regulations recognize names, addresses, and identification numbers as personal data; however, certain types of indirect identifiers, such as device metadata, behavioral data, or IP addresses, are treated differently across legal frameworks.

For example, GDPR (Article 4) defines PII as "any information relating to an identified or identifiable natural person." In contrast, India's DPDPA states (Article 2(t)) that *personal data means "any data" about an individual who is identifiable by or in relation to such*

*data*. The phrase "any data" is ambiguous and leaves room for interpretation — does it extend to handwritten records, video surveillance data, or AI-inferred attributes? Likewise, CCPA also includes "household" data, which is not covered by other regulations (Article 1798.140.(b)).

This inconsistency creates technical challenges when determining which categories of PII are in scope for privacy analysis — a data protection approach that aligns with GDPR may still fall short of Indian privacy law.

Despite this issue, a substantial portion of reviewed studies operationalized personal/sensitive data using GDPR's definition when detecting data leakage, classifying the lawfulness of data flows, or assessing privacy policy completeness [10, 13, 16, 23, 26, 27]. As discussed, using one regulation (*e.g.*, GDPR) for this definition lacks generalizability across the globe. For example, Nguyen et al. [26, 27] used GDPR's definition of personal data. Applying this from the perspective of India's DPDPA and China's PIPL would not be able to include enough PII factors.

Overall, relying on one or two regulations' definition of personal and sensitive data focuses on the risks present or considered in that jurisdiction, while omitting risks from other regulations. As a result, studies that focus on one local regulation (*e.g.*, GDPR) might omit entire classes of data protected by different regulations.

*1.1.2* **Consent and Privacy Expectations.** Many studies have analyzed the notion of ***consent*** and related requirements through the lens of: privacy policy completeness, run-time consent and privacy notices, and the alignment of collected data to natural language [17, 18, 20, 22, 27, 37]. The majority of these studies grounded their threat models using GDPR's opt-in requirements, which requires consent to be freely given, informed, and unambiguous.

As we will discuss in detail soon, consent models differ drastically across regions. For example, California's CCPA focuses on opt-out rights, Brazil's LGPD permit processing based on legitimate interest, and India's DPDPA introduces special provisions for persons with disabilities. This shows that using a single regulation (*e.g.*, GDPR) definition of lawful consent as a global standard may misclassify lawful practices and actions, or even miss compliance with different regulations (*e.g.*, California's CCPA opt-out rights vs others' opt-in rules).

A similar issue arises when characterizing the notion of ***privacy breach***. Data protection laws focus on restricting access to personal data but do not always specify which technical actions or system behaviors may result in such a breach. This ambiguity complicates the assessment of data collection appropriateness.

For instance, a health and fitness application that measures walking distance may access a smartphone's accelerometer and GPS to track movement. However, if the same app also requests access to the microphone or ambient light sensor, it may commit a privacy violations under certain regulations. Under Article 5(1)(c) of GDPR, data collection should be "limited to what is necessary in relation to the purposes for which they are processed" (data minimization principle). If an app accesses unnecessary sensors without a justified purpose, it could violate GDPR. In contrast, Brazil's POPIA (Article 9) requires "personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject." This leaves room open to collect other sensor data via the health app, unless mixed Article 10, which states "personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive."

Any technique attempting to measure breaches in the wild may therefore produce different outcomes depending on the relevant legislation.

## 1.2 Choice of Regulations in the Paper

In selecting privacy regulations, we address the tension between keeping the legal analysis workload manageable and understandable, while ensuring sufficient representativeness of worldwide laws. Our selection process is as follows. First, we add GDPR to the set because of its widespread use in relevant research. Then, we select additional regulations subject to the constraint that each new regulation covers a continent not yet in our set.[3] When adding each new regulation, we aim for populous countries with established data protection laws. We stop when we achieve approximately 40% coverage of the world population. The population criterion was to ensure broad data subject (or called user) coverage while maintaining analytical depth. Continental consideration was introduced to encourage regulatory diversity. We selected China and India because of the scale of the data subjects and the distinctiveness of their regulatory approaches. However, ultimately achieving our goal is not dependent on any specific choice of regulations, as long as the choice showcases regulatory diversity.

The resulting set includes: GDPR (EU), CCPA (California, US), DPDPA (India), PIPL (China), POPIA (South Africa), and LGPD (Brazil), covering ≈38.3% of the world population. While we acknowledge that this set does not include other representative laws, we argue that it suffices to qualitatively highlight the limitations stemming from only considering individual regulations.

## 1.3 Summary of the Paper

This paper examines how modern privacy regulations govern personal data and analyzes the challenges these regulations pose for organizations, individuals, and regulators. We adopt a data lifecycle perspective to structure this analysis for two reasons. First, these data protection laws primarily regulate automated or systematized personal data processing, which naturally unfolds across distinct phases, such as data collection, storage, processing, sharing, deletion, and bequeathal. Second, regulatory obligations and user rights are not meaningful in isolation; rather, they are triggered, constrained, and enforced depending on when and how personal data is handled within the data life cycle. In practice, organizations operationalize privacy through technical mechanisms deployed across these phases, while individuals exercise their rights in response to phase-specific data handling activities.

With this perspective, §2 discusses related work and §3 systematically maps major privacy regulations to the data life-cycle phases. Building on this mapping, §4.1 analyzes implications for individuals, highlighting variations across data protection laws in the defining personal data, sensitive data, children's data, user rights, and consent models. Next, §4.2 examines implications for organizations by identifying the essential functional requirements

[3] We consider China separately from the rest of Asia, due to its cultural specificities and outsized impact on worldwide commerce.

| Data Life-Cycle Phase | Users (§4.1) | Organizations (§4.3) | Government (§4.3) |
|---|---|---|---|
| Collection | Right to consent and right to revoke consent | Rules for purpose limitation, data minimization, and transparency (§4.2.1) | Investigate and audit the records of processing, and different types of penalties |
| Storage | Right to access and right to data portability | Rules for security, accuracy, and data retention (§4.2.1) | |
| Processing | Right to object and right to restriction of processing | Rules for accountability (§4.2.5) | |
| Sharing | Right to restriction of processing | Rules for cross-jurisdiction data transfer (§4.2.3) | |
| Deletion | Right to delete | Rules for deletion (§4.2.4) | |
| Data Bequeath | Right to nominate | Rules for accountability (§4.2.5) | |

**Table 2: Mapping of data life cycle phases to individual/user, organization, and government roles.**

that organizations must implement at each phase of the data life cycle to achieve compliance. Finally, §4.3 compares government authority roles across jurisdictions, focusing on supervisory power differentials, and mechanisms of investigation and enforcement.

## 2 Related Work

Several privacy frameworks, such as Contextual Integrity [7, 28] and Interdependent Privacy [1, 15], provide formal approaches for defining and reasoning about privacy. Contextual Integrity conceptualizes privacy as the appropriate flow of information within specific social contexts, governed by norms that specify actors, data subjects, senders, recipients, information types, and transmission principles. Interdependent Privacy emphasizes that an individual's privacy is not solely determined by their own actions but is also influenced by others' disclosures and behaviors.

While these frameworks offer valuable conceptual foundations, they do not ensure enforceable protection in practice, as they do not specify enforcement mechanisms, legal obligations, or remedies. In contrast, the data protection laws considered in this paper operationalize privacy through enforceable user rights, obligations imposed on data controllers and collectors, and mechanisms for regulatory oversight.

Commercial platforms, e.g., DLA Piper [2] and OneTrust DataGuidance [3], provide jurisdiction-based summaries. However, they are also limited, e.g., by not discussing consent and user rights, and by functioning only in operational categories to realize rights. Overall, the platforms do not provide straightforward ways for researchers to understand the differences among laws.

## 3 Laws and Data Life Cycle

A systematic understanding of data protection laws starts with the data life cycle, which captures the sequential stages through which personal data passes. At each stage of the data life cycle, data protection laws follow an *actor-centric* model, *i.e.*, they place constraints/ rules/ rights on the three main actors — the user/ individual/ personal whose data is collected, the organization that collects the individual's data, and the government that enforces the data protection law. In particular, the data protection laws provide: (*i*) the rights for individuals whose data is being processed to manage their data, (*ii*) the rules for organizations to handle individuals' data, and (*iii*) the powers to the governments and regulatory authorities to supervise and enforce compliance. In short, these laws impose constraints/rules to ensure that individuals' data is collected, processed, stored, shared, and deleted in a responsible and legally compliant manner.

Table 2 provides a mapping of each life-cycle phase to (*i*) the rights granted to users, (*ii*) the rules imposed on organizations, and (*iii*) the enforcement responsibilities for the governments. This table shows how user rights and organizational duties are distributed across different stages of the data life cycle.

Below, we outline the stages of the data life cycle, and then, the remaining paper will explain each cell of the table in detail.

(1) **Data collection (Row 1).** Personal data is collected from individuals through various methods such as online forms, surveys, or interactions with services and applications. Data protection laws ensure that individuals retain control over their data from the moment it is collected. Rights related to this phase include the right to consent and the right to revoke consent, while organizations are required to follow rules of purpose limitation, data minimization, and transparency.

(2) **Data storage (Row 2).** Once collected, data is stored for varying periods based on legal requirements or organization/business needs. Data protection laws regulate how data must be stored, protected, and managed to prevent unauthorized access. Rights related to this phase include the right to access and the right to data portability, while organizations are required to follow security, accuracy, and data retention rules.

(3) **Data processing (Row 3).** Data is processed for various purposes, such as analysis, reporting, or decision-making. During this stage, individuals retain specific rights—including the right to object and the right to restriction of processing—to ensure their data is handled in accordance with their consent, while organizations are required to follow accountability rules.

(4) **Data sharing (Row 4).** At this stage, personal data may be shared with third parties, including service providers and business partners. Data protection laws regulate how data should be shared and ensure individuals have control over how their information is distributed. Rights related to this phase include the right to restriction of processing, while organizations are required to follow cross-jurisdiction data transfer rules.

(5) **Data deletion (Row 5).** When personal data is no longer needed for its original purpose, it should be deleted/anonymized. Data protection laws empower individuals to control when and how their data is erased, ensuring it is not retained longer than necessary. Rights related to this phase include the right to erasure/deletion, while organizations are required to follow deletion rules.

(6) **Data bequeath (Row 6).** Data protection laws extend data governance beyond an individual's lifetime by allowing posthumous or delegated control over personal data. This phase governs the nomination of a representative who may exercise data-related rights on behalf of an individual in the event of death or incapacity. Rights related to this phase include the right to nominate, while organizations are required to adhere to accountability rules.

| Laws | Article/ Section | Applicable countries/ regions | Organization presence in jurisdictional region | Individual residence in jurisdictional region | Not applicable to |
|---|---|---|---|---|---|
| GDPR | 3 | EU | Applies if the organization processes data of EU residents, even if located outside the EU | Applies to individuals residing in the EU | Data collected for personal or household activities, or by authorities for crime prevention, investigation, prosecution, or public security |
| CCPA | 1798.140 | California (U.S.) | Applies to businesses processing data of California residents, whether or not based in California, and having annual gross revenues exceeding $25M or deriving 50%+ revenue from selling/sharing personal data | Applies to California residents | Not explicitly mentioned |
| DPDPA | 3 | India | Applies to businesses processing data of Indian residents, regardless of businesses' location | Applies to Indian residents | Data collected by an individual for personal or domestic purposes, or personal data made public by the individual, Art. 3(c) |
| PIPL | 3 | China | Applies to organizations processing data of individuals residing in China, regardless of organizations' location | Applies to Chinese residents | Not explicitly mentioned |
| LGPD | 3 | Brazil | Applies to businesses processing data of Brazilian residents, regardless of businesses' location | Applies to Brazilian residents | Data collected by a person for private, non-economic purposes; or for journalistic, artistic, public safety, national defense, state security, or investigation purposes, Art. 4 |
| POPIA | 3 | South Africa | Applies to organizations processing data of individuals domiciled in South Africa, regardless of organization's location | Applies to South African residents | Not explicitly mentioned |

**Table 3: Applicability of Data Protection Across Jurisdictions**

| Law | Personal Data | Examples of Personal Data | Sensitive Data |
|---|---|---|---|
| GDPR | Any information relating to an identified or identifiable natural person, Art. 4 | Name, identification number, location data, online identifier, or factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity | Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, Art. 9 |
| CCPA | Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, Art. 1798.140 | Real name, alias, unique personal identifier, online identifier, IP address, internet activity, geolocation data, account name, employment information, education data, biometric data (*e.g.*, DNA, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, faceprint) | Social security number, driver's license, state ID, passport number, account login, financial account details, precise geolocation, racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, union membership, genetic data, neural data, Art. 140(ae) |
| DPDPA | Any data about an individual who is identifiable by or in relation to such data, Art. 2(t) | Not specified | Not specified† |
| PIPL | Various information related to an identified or identifiable natural person recorded electronically or by other means, Art. 4 | Not specified | Biometrics, religious belief, specific identity, medical health status, financial accounts, and the person's whereabouts, Art. 28 |
| LGPD | Information regarding an identified or identifiable natural person (Art. 5I) | Not specified | Racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical, or political organization membership, health or sex life data, genetic or biometric data, Art. 5II |
| POPIA | Information relating to an identifiable, living, natural person, Art. 1 | Gender, marital status, education information, identifying number, symbol, email address, physical address, phone number, location data, online identifier, person's name | Religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, criminal behavior, Art. 26 |

**Table 4: Definitions of personal and sensitive data across data protection laws. Note: †: DPDPA is the only law that focuses on persons with disability, see Art. 2(j).**

## 4 Diversity in Data Protection Laws

Data Protection laws pose significant compliance challenges, particularly for organizations operating across multiple jurisdictions, as well as individuals traveling from one jurisdiction to another. No universal data protection law exists; instead, each country or region establishes its own regulations, which differ based on factors such as jurisdictional boundaries, an individual's physical presence, an organization's presence, and its turnover. Table 3 compares these laws in terms of their jurisdictional applicability. For example, GDPR applies to any EU residents, even if they are currently outside the EU, whereas CCPA introduces business-specific thresholds. Laws such as the PIPL, DDPA, LGPD, and POPIA apply to subjects who are resident or domiciled within their borders.

Beyond jurisdiction, data protection laws also vary substantially in definitions of data, consent requirements, user rights, cross-border data transfer rules, penalties for violations, and mechanisms for enforcing compliance (and due to which leads to improper implementation and/or violation of the laws [10, 20, 23]).

To systematically study these differences, in this section, we classify data protection laws according to three main actors: the *user/individual* whose data is collected (§4.1), the *organization* that collects and processes this data (§4.2), and the *government* that defines privacy regulations and enforces compliance (§4.3).

**Note that the laws we compare in this paper are divided into articles and/or sections. For simplicity, we use the word 'article' in this paper.**

### 4.1 Laws in terms of the Users

**Objectives.** Analysis of data protection laws must begin with the individual, as the user is the primary subject whose data triggers the entire data life cycle. Thus, the objective of this section is to first examine how data protection laws categorize user data as personal, sensitive, or children's data in §4.1.1. Then, our objective is to discuss how such data classifications specify the rights granted to individuals and the mechanisms for controlling their data, including its collection, use, and deletion, which we will discuss in subsequent subsections §4.1.2 and §4.1.3.

*4.1.1* **Personal Data, Sensitive Data, and Child Data.** Data protection laws classify users' data into three categories: personal, sensitive, and children's data, which are differentiated based on the specificity of data and the age of the user, as we discuss below:

**Personal data** refers to any information that directly or indirectly identifies an individual. While most data protection laws share a common foundation in terms of personal/user/individual data, their definitions vary in scope. Some laws adopt broader definitions; others provide only vague definitions. For instance, GDPR

| Law | Article | Age threshold for consent | Consent mechanism | Verification of consent |
|---|---|---|---|---|
| GDPR | Art. 8 | Under 16 years (can be lowered to 13 by member states) | Parental consent | Yes |
| CCPA | Art. 1798.120 and 999.330 | Under 13 years | Custodial parent or guardian required for children under 13; and for ages 13-16, the child can provide consent | Yes |
| DPDPA | Art. 9 | Under 18 years | Consent from a parent or lawful guardian | Yes |
| PIPL | Art. 28, 31 | Under 14 years | Consent of parents or other guardians | No |
| LGPD | Art. 14 | Under 12 years | Consent of one parent or legal representative | Yes |
| POPIA | Art. 35 | Under 18 years | Consent of a competent person | No |

**Table 5: Children's data protection requirements across data protection laws.**

| Privacy Right | GDPR | CCPA | DPDPA | PIPL | LGPD | POPIA |
|---|---|---|---|---|---|---|
| Right to Consent | Art. 6, 13 | Default opt-in. Opt-out is available, Art. 1798.120 | Art. 5, 6 | Art. 13, 14 | Art. 7 | Art. 11 |
| Right to Revocation of Consent | Art. 7(3) | No | Art. 6(4) | Art. 15 | Art. 8(5) | Art. 11(3) |
| Right to Access / Right to Explanation of Handling Policies | Art. 15 | Art. 1798.110, Art. 115 | Art. 11 | Art. 45 | Art. 18 | Art. 23 |
| Right to Data Portability | Art. 20 | No | No | Art. 45 | Art. 18 | No |
| Right to Erasure/Deletion (Right to Be Forgotten) | Art. 17 | Art. 1798.105 | 12(1) | Art. 47 | Art. 18 | Art. 24 |
| Right to Rectification | Art. 16 | Art. 1798.106 | No | Art. 12(1) | Art. 46 | Art. 24 |
| Right to Object | Art. 21 | Art. 1798.120, 121 | Art. 13‡ | Art. 44 | Art. 18 | Art. 11(3) |
| Right to Restrict Processing | Art. 18 | Art. 1798.120 | No | Art. 44 | No | Art. 11(3) |
| Right to Nominate | No | No | Art. 14 | Art. 49† | No | No |
| Right to Non-Discrimination | No | Art. 1798.125 | No | No | No | No |

**Table 6: Comparison of privacy rights. ‡: Under "Grievance redressal" rights. †: for deceased individuals.**

and South Africa's POPIA adopt broader definitions, explicitly including indirect identifiers such as online identifiers (*e.g.*, IP addresses and cookies), while India's DPDPA and China's PIPL do not clearly specify the meaning of personal data.

**Sensitive personal data** provides fine-grained information about very specific data, whose collection may impact an individual's dignity, safety, and privacy. Examples of sensitive data typically include information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, and financial details. Only India's DPDPA does not deal with such sensitive data; nevertheless, DPDPA deals with ***persons with disabilities*** and allows data collection from them if a lawful guardian provides verifiable consent.

**Children's data** is defined in terms of the age of minors, which varies according to different laws from 13 to 18. The laws also enforce that whenever data from a minor is collected, a consent must be obtained from the lawful guardian, not from the child, and there should be a mechanism to verify that the consent is really obtained from lawful guardians.

Tables 4 compares different laws in terms of the definition of personal and sensitive data, along with explicit examples of personal data. Table 5 compares different laws in terms of children's data, the way of finding children, and their consent model.

**Note.** While all the laws strictly define personal data and mechanisms to handle data, only India's DPDPA (Art. 14(1)) and China's PIPL (Art. 49) also provide rights to the individual to nominate someone on their behalf in case of their death or incapacity.

*4.1.2* **User Rights.** Data protection laws offer individuals several rights that empower them to control their personal data throughout its lifecycle, which includes collection, storage, processing, sharing, and deletion. These rights ensure that data collection and processing are conducted transparently, with user consent, and that individuals can access, modify, or delete their data as needed. By enforcing these rights, privacy regulations offer benefits such as transparency, accountability, prevention of misuse, and enhanced trust in data management practices. Table 6 compares ten user rights across different laws. No law grants all 10 such rights to the user. Only China's PIPL offers 9 out of 10, while GDPR and India's DPDPA offer 8 out of 10.

Below, we discuss these rights and their benefits to the user.

**Right to consent:** ensures transparency by offering individuals the ability to understand and control how their personal data is collected and processed. Consent must be given through a clear, affirmative act that is freely given, specific, informed, and unambiguous. This can be expressed through a written statement, electronic means, or an oral declaration. Without valid consent, data processing is generally prohibited unless justified by legitimate interests or other legally recognized grounds.

**Right to revocation of consent:** ensures flexibility to individuals by allowing them to revoke/withdraw their consent at any time. Organizations should implement easy-to-use mechanisms, *e.g.*, opt-out links. Once consent is revoked, data processing must cease unless another valid legal basis justifies its continuation.

**Right to access:** ensures transparency and accountability by allowing individuals to request and receive a copy of their personal data that is held by an organization, along with details about how their data is being used. Organizations must provide individuals with a copy of their data upon request within a reasonable timeframe, along with details on how and why it is being processed. PIPL considers the same right under "Right to explanation of handling policies."

**Right to rectification:** ensures accuracy of personal data by offering individuals the right to request corrections or updates to any inaccurate or incomplete personal data. Organizations should provide individuals with accessible means to promptly correct and update their personal data.

**Right to deletion:** ensures control over the personal data by offering individuals the right to request the deletion of their personal data under certain conditions, such as when data is no longer necessary for its original purpose or when consent is revoked. Organizations should implement procedures to delete personal data upon user request when it is no longer necessary for processing.

| Law | Article | Consent Model | Key Requirements |
|---|---|---|---|
| GDPR | 6, 7 | Opt-in, Art. 6(1a), 7(1) | Freely given, specific, informed, and unambiguous indication of the individual's wishes, signified by a statement or clear affirmative action agreeing to the processing of personal data. |
| CCPA | 1798.120 | Opt-out | Businesses must provide a clear and conspicuous "Do Not Sell My Personal Information" link, allowing consumers to opt-out of data sales. Parental consent is required for selling data of children under 13, and affirmative consent is required for those aged 13-16. |
| DPDPA | 6 | Opt-in, Art. 6(1) | Free, specific, informed, unconditional, and unambiguous consent, given through a clear affirmative action. Consent must be limited to necessary personal data for a specified purpose.† |
| PIPL | 7, 14, 17 | Opt-in, Art. (14) | Requires openness and transparency. Organizations must disclose processing rules and provide information in a clear and understandable manner. Consent must be voluntary, explicit, and based on full knowledge. |
| LGPD | 5-10 | Opt-in, Art. 5(9) | Requires free, informed, and unambiguous consent. Allows processing based on legitimate interest in certain cases without consent, but explicit consent is required for sensitive data. |
| POPIA | 11 | Opt-in (for sensitive data) and opt-out (for marketing) | Requires explicit consent for processing sensitive personal information. Allows opt-out mechanisms for direct marketing. Individuals must be informed about the purpose of data collection. |

**Table 7: Comparison of consent models across data protection laws. Note: †: DPDPA has a special provision for persons with disabilities, and only the lawful guardian should provide verifiable consent for persons with disabilities, Art. 9(1).**

| Law | Article | Consent Type | Time-bound |
|---|---|---|---|
| GDPR | Art. 4(11), 6(1a), 7(1) | Specific Consent, Art. 7(1) | Yes, Art. 7(3) |
| CCPA | Art. 1798.120 | Broad General Consent | No |
| DPDPA | Art. 6(1) | Specific Consent, Art. 6(1) | No (but the right to withdraw her consent at any time), Art. 6(4),6(7) |
| PIPL | Art. 5, 13, 15 | Specific Consent | No, (but withdraw his/her consent), Art. 5 |
| LGPD | Art. 8, 9 | Moderately Specific | Yes, Art. 9(2), and consent may be revoked at any time, Art. 8(5) |
| POPIA | Art. 13, 14 | Context-Dependent Consent | Yes, Art. 14 |

**Table 8: Granularity of consent.**

| Law | Consent Withdrawal | Key Requirements for Withdrawal | Duration for Data Deletion After Consent Withdrawal | Consent expiration |
|---|---|---|---|---|
| GDPR | Right to Withdraw Consent at Any Time, Art. 7(3) | Easy to withdraw as to give consent | No, Art. 17(1b) | Yes, Art. 5(1b), 25(2) |
| CCPA | Right to opt out of sale or sharing, Art. 1798.120 | N/A | 45 days, Art. 1798.130(a)(2) | No |
| DPDPA | Right to Withdraw Consent at any time, Art. 6(4) | Ease of doing so being comparable to the ease with which such consent was given | No, Art. 6(6), 8(7) | No |
| PIPL | Right to Withdraw Consent, Art. 15 | Convenient means to withdraw consent | No | No |
| LGPD | Consent may be revoked, Art. 8(5) | Free of charge procedure | No | Yes, Art. 9(2) |
| POPIA | Withdraw consent, Art. 11(2b) | Not given | No | Yes, Art. 13(1), 14(1) |

**Table 9: Consent withdrawal rules across laws.**

**Right to object:** ensures individuals' autonomy by allowing them to refuse their personal data processing, particularly for purposes such as marketing or profiling. Organizations must provide individuals with an easy way to opt-out of specific data processing activities.

**Right to restriction of processing:** enables individuals to request a temporary restriction in the processing of their data under certain circumstances, such as when the accuracy of the data is disputed, when the processing is unlawful and the individual opposes to its erasure, or when the data is needed for legal claims, even if the organization no longer requires it for its own purposes.

**Right to data portability:** ensures control over the personal data by offering individuals the right to receive their personal data in a structured, commonly used, and machine-readable format, and to transfer it to another data controller. This right facilitates more effortless data transfer between providers.

**Right to nominate:** enables individuals to designate another person to exercise their rights in the event of death or incapacity, such as mental unsoundness or physical infirmity. This right ensures that an individual's data protection rights can still be managed by a nominated representative if they are no longer able to do so themselves. This right is provided explicitly under DPDPA (India, Article 16) and PIPL (China, Article 49).

**Right to non-discrimination:** protects individuals from being denied goods, services, or benefits, or being charged different prices or offered different levels of service simply because they exercised their privacy rights. This ensures that individuals are not penalized or treated unfairly for asserting their data protection rights, such as opting-out of data collection or requesting data deletion. This right is included under CCPA.

*4.1.3* **Consent Models.** Consent forms a fundamental legal basis for data processing in all data protection laws; however, consent's definition, scope, and enforcement differ significantly. Table 7 compares different laws with respect to the consent model (opt-in vs. opt-out) and the consent requirements for providing information in the consent form, such as non-ambiguity and no charges for the consent form.

Note that *except for CCPA, all the laws require opt-in, i.e., explicitly providing consent for their data collection by organizations*, while CCPA instead requires explicit opt-out.

Furthermore, consent can be specific to a particular task or general to all tasks carried out by the organization using the collected data, as we discuss below.

**Granularity of consent (general vs. specific consent).**

Granularity of consent refers to the level of detail and specificity with which individuals are asked to grant permission for the processing of their personal data. ***General consent*** is a broad, overarching agreement that allows an organization to collect and use personal data for multiple purposes without requiring the individual to approve each specific use. In contrast, ***specific consent*** is narrowly defined and purpose-linked, requiring the individual to explicitly agree to each particular way their data will be processed. The purpose of differentiating between general and specific consent is to give users greater control and awareness over how their personal information is handled.

| Law | Purpose Limitation | Fairness | Transparency | Data Minimization | Accuracy | Storage Limitation | Security | Accountability |
|---|---|---|---|---|---|---|---|---|
| GDPR | Art. 5(1b) | Art. 5(1a) | Art. 5(1a), 12, 13, 14 | Art. 5(1c), 25(1) | Art. 5(1d) | Art. 5(1e) | Art. 5(1f), 25, 32 | Art. 5(2), 30 |
| CCPA | Art. 1798.100(b),(c) | Art. 1798.125 | Art. 1798.130 | N/A | N/A | N/A | N/A | N/A |
| DPDPA | Art. 4, 7 | Not explicit | Art. 5 | Not explicit, but Art. 6(1) | 12 | Not explicit, but Art. 8(8) | Art. 8(5) | Not explicit, but Art. 8 |
| PIPL | 6 | Not explicit (but good faith, Art. 5) | Art. 7 and 50 | Art. 6 | Art. 8, 46 | Art. 19 | 51(3) | Not explicit, but Art. 5 (lawfulness), 48, 54 |
| LGPD | Art. 6(1) | Art. 6(9) | Art. 6(6) | Art. 6(3) | Art. 6(5) | Art. 6(7) | 6(6), 46 | Art. 6(10) |
| POPIA | Art. 13, 18 | Not explicit | Art. 17 (Openness) | Art. 10 | Art. 16,24 | Not explicit, but Art. 14 | Art. 19, 21 | Art. 23 |

**Table 10: Core processing principles across data protection laws.**

Table 8 compares laws on the consent type and the duration for a given consent. Note that GDPR, India's DPDPA, and China's PIPL require specific consent. GDPR, LGPD, and POPIA allow data processing for a limited time under a given consent, while others require users to exercise their right to withdraw consent to prevent the organization from collecting their data.

**Consent withdrawal and expiration** are safeguards to ensure individuals retain control over their personal data. While both mechanisms restrict the scope of consent, they operate differently. ***Consent withdrawal*** empowers individuals to actively revoke their consent at any time, obligating organizations to cease further collection or use of data based on that consent. Importantly, many laws distinguish between stopping future collection and the handling of data already obtained, which may still be processed under other lawful bases. ***Consent expiration***, in contrast, is linked to the principle of purpose limitation: consent is valid only for the specific purpose and duration for which it was originally given, and it lapses automatically once that purpose has been fulfilled, without requiring any action from the individual.

Data protection laws vary in how they regulate these mechanisms; for example, some explicitly require withdrawal to be as simple as giving consent, prohibit charging fees, or specify the timeframe within which processing must cease after withdrawal. Table 9 compares data protection laws in terms of consent withdrawal mechanisms and their requirements, duration for data deletion after consent revocation, and options for consent expiration.

*4.1.4* **Lessons.** While data protection laws share a common goal of providing users with meaningful control over their personal data, they differ widely in how they define personal data and the mechanisms for exercising that control. For example, not all laws offer precise or comprehensive definitions of personal and sensitive data, nor do they align on the required granularity of consent. User rights also vary substantially. For example GDPR, while offering fine-grained information about personal, sensitive, and children data, does not include certain rights, such as the right to nominate, which is offered only under India's DPDPA. These variations influence how users understand their rights and how effectively they execute them.

Examining data protection laws through user-centric dimensions showed that GDPR and China's PIPL provide some of the strongest protections: each offers at least 8 out of 10 above-discussed rights to the user (see Table 6) as well as requires specific consent (see Table 8). In contrast, the CCPA adopts a flexible model, by not requiring prior consent for data collection, relies primarily on an opt-out mechanism, and provides only 7 out of 10 rights. As such, while user autonomy is a common objective across data protection laws, the level and form of protection differ significantly.

## 4.2 Laws in terms of Organizations

**Objectives.** Organizations that collect and process personal, sensitive, and children's data are bound not only by the requirements of consent and user rights but also by a set of broader obligations designed to ensure lawful handling of data. These responsibilities define how organizations must operate when processing information, responding to incidents, transferring data across different jurisdictions, and demonstrating compliance to oversight authorities.

In this section, our objective is to compare different data protection laws on the aspects of core processing principles to be followed by organizations (§4.2.1), rules to be followed after data breaches (§4.2.2), cross-jurisdictional data transfer rules (§4.2.3), rules around data deletion (§4.2.4), and mechanisms to ensure accountability in following/implementing regulations (§4.2.5).

*4.2.1* **Core Processing Principles.** Data protection laws provide a set of foundational principles detailing how organizations should handle data to ensure they do not collect more than is required and securely store it. As will become clear from the definition of these principles, without them, user rights (such as consent withdrawal or access) cannot be meaningfully exercised or verified. For instance, consent will become meaningless without principles of purpose limitation, transparency, and data minimization.

Below, we provide a superset of all the principles that are given in the data protection laws (note that the names of principles are directly taken from the laws):

- ***Purpose limitation*** (*i.e.*, data must be collected and processed only for specific, explicit, and legitimate purposes),
- ***Fairness*** (*i.e.*, processing does not harm individuals),
- ***Transparency*** (*i.e.*, inform individuals clearly about processing activities, purposes, and their rights),
- ***Data minimization*** (*i.e.*, should collect only the minimum amount of personal data necessary to achieve the stated purpose).
- ***Accuracy*** (*i.e.*, personal data is accurate, complete, and up to date).
- ***Storage limitation*** (*i.e.*, personal data should not be kept longer than necessary for the purposes for which it was collected).
- ***Security*** (*i.e.*, ensure data integrity and data confidentiality).
- ***Accountability*** (*i.e.*, organizations demonstrating compliance with the principles).

Table 10 compares each law under these principles. GDPR and Brazil's LGPD are the only two regulations that satisfy all the above-mentioned principles. In contrast, California's CCPA is the most flexible law that does not explicitly offer most of the principles. Furthermore, some laws do not directly offer such principles. For example, DPDPA does not explicitly offer data minimization; however, Article 6 requires consent-based specific processing, which turns into data minimization. Likewise, DPDPA does not explicitly mention storage limitations and accountability. However,

| Law | Breach Notification Trigger | Notification deadline to authority | What to inform to the authority | Notification deadline to users | What to inform to users | Security Measures Required | Penalties |
|---|---|---|---|---|---|---|---|
| GDPR | Personal data breach, Art. 34(1) | 72 hours after becoming aware of the breach (Art. 33) | (a) the categories and approximate number of individuals concerned, (b) the name and contact details of the data protection officer, the likely consequences of the personal data breach, the measures taken or proposed to be taken by the controller to address the personal data breach | Without undue delay, if high risk Art. 34(1) | b point of 4th column Art. 34(2) | Techniques to achieve confidentiality, integrity, availability, Art. 32(1b) | Up to €10m or 2% of turnover Art. 83(4a) |
| CCPA | Breach of unencrypted personal information (Art. 1798.150 and 1798.82) | "In the most expedient time possible" (Art. 1798.82) | "What Happened, What Information Was Involved, What We Are Doing, What You Can Do, and For More Information" Art. 1798.82(d) | Not explicit | Same as 4th column | Reasonable security procedures (Art. 1798.150) | $100–$750 per consumer per incident Art. 1798.150 (a) (1) (A) |
| DPDPA | "Personal data breach" defined broadly Art. 2(u), 8(6) | No time duration | Not explicit | | | Reasonable security safeguards, Art. 8(5) | Up to rupee ₹ 250 crore, Art. 33(2) |
| PIPL | Leak, falsification, or lost of personal information (Art. 57) | Immediate (Art. 57) | Types and causes of personal information leakage, falsification, and loss that have occurred or may occur, and the possible harm caused; remedial measures taken by the organization and individuals; contact information of the organization, Art. 57 | If measures to effectively avoid harm are not enough, Art. 57 | 4th column | Technical measures, encryption, de-identification, Art. 51(3) | Not explicit for data breaches |
| LGPD | A security incident that may create risk or relevant damage to the individuals, Art. 48 | "In reasonable time," Art. 48(1) | Nature of the affected personal data, information on the individuals involved, an indication of the technical and security measures used to protect the data, and the risks related to the incident, the measures that were or will be adopted to reverse or mitigate the effects, Art. 48 | Reasonable time period, Art. 48(1) | Same as 4th column, Art. 48 | Security, technical and administrative measures, Art. 46 | |
| POPIA | Security compromise of personal information, Art. 22 | "As soon as reasonably possible," Art. 22(2) | Description of possible consequences, measures taken or proposed, responsible party contacts | "As soon as reasonably possible," Art. 22(2) | Possible consequences of the security compromise, measures to be taken, measures to be taken by the individual to mitigate the possible adverse effects, the identity of the unauthorised person (if known) who may have accessed or acquired the personal information, Art. 22(5) | Yes, Sec. 19 | |

**Table 11: Data breaches across data protection laws.**

specific data collection, as outlined in Article 8(8), and the organization's obligations, as outlined in Article 8, ensure both.

*4.2.2* **Data Breaches.** All data protection laws impose obligations on organizations to implement preventive and corrective measures to reduce the risk of data breaches, typically specifying: (*i*) the conditions triggering breach notification to regulators/authorities, affected individuals, or both, (*ii*) timelines for reporting to regulators/authorities and individuals, (*iii*) information to be disclosed to authorities and individuals regarding the breach, (*iv*) security measures to be implemented to prevent breaches, and (*v*) penalties applicable in the event of a breach.

Table 11 compares different laws on parameters like notification triggers, reporting timelines, required content of notices, and penalties. Not all laws impose stringent conditions on what could trigger the organization to notify about data breaches. However, once organizations detect data breaches, only GDPR imposes a strict requirement to inform the regulator within 72 hours. In contrast, China's PIPL and Brazil's LGPD require organizations to provide fine-grained information about incidents to both users and regulators. However, India's DPDPA does not provide any explicit conditions on all such. Furthermore, China's PIPL, Brazil's LGPD, and South Africa's POPIA do not impose any specific penalties for data breaches. Only GDPR, California's CCPA, and India's DPDPA placed penalties for data breaches.

*4.2.3* **Cross Jurisdiction Data Transfer.** While data mobility enables global commerce and collaboration, it also jeopardizes individual rights and the potential loss of regulatory oversight once data leaves its country of origin.

To mitigate these risks, data protection laws impose conditions on cross-border data transfers to ensure that protection standards accompany the data. These provisions typically address four key aspects: (*i*) transfer conditions, which define the circumstances under which cross-border transfers are permitted; (*ii*) review mechanisms, which establish procedures for evaluating and approving or disallowing transfers; (*iii*) the role of individual consent, which in some jurisdictions requires explicit authorization from individuals even where the recipient country lacks adequate protection; and (*iv*) exemptions, which identify circumstances where transfers are permitted regardless of general restrictions.

Table 12 compares these laws across the above-mentioned four aspects. Note that India's DPDPA and China's PIPL require government approval to allow data transfers. Only GDPR allows cross-jurisdictional data transfers based on an individual's consent for data transfer, and it imposes a strict 4-year review deadline. In contrast, the CCPA is the only law that does not address cross-jurisdictional data transfers.

*4.2.4* **Data Deletion.** A core principle of data protection law is that personal data must not be stored indefinitely. Organizations are required to adopt retention policies ensuring data is kept only as long as necessary to fulfill the purpose for which it was collected. Once that purpose is achieved, or the legal basis for processing ceases to exist, organizations must securely delete, anonymize, or otherwise render the data unusable.

Table 13 compares the requirements across different data protection laws with respect to data deletion on parameters, such as: (*i*) the circumstances under which organizations must automatically delete data without individual intervention; (*ii*) the exemptions that allow continued retention even when individuals request deletion; (*iii*) the existence of a formal right to deletion (or erasure); and (*iv*) the time frame within which organizations must comply with a deletion request once the right is exercised.

| Law | Transfer Conditions | Review Mechanisms | Role of Individual's Consent | Exemptions |
|---|---|---|---|---|
| GDPR | Ensures adequate protection, Art. 45(1) | At least every four years, Art. 45(3) | Yes, Art. 49(1)(a) | Important reasons of public interest, the establishment, exercise or defense of legal claims, vital interests of individuals, Art. 49(1)(d,e,f) |
| CCPA | Not applicable | | | |
| DPDPA | By default, data transfer is allowed. The Government may restrict transfers by notification, Art. 16 | No | Consent alone is not sufficient unless the government permits | Legal rights, the interest of prevention, detection, investigation, or prosecution of any offense, ascertaining the financial information and assets and liabilities of any person who has defaulted in payment, Art. 17(1)(c,d,f) |
| PIPL | Only if approved by the State cyberspace administration, Art. 38 | Not exists | | |
| LGPD | Ensures adequate protection, Art. 33(1) | Yes, but not duration bound, Art. 34 | Explicit consent for data transfer, Art. 33(8) | For international legal cooperation, protect life/ physical safety, Art. 33(3,4) |
| POPIA | Ensures an adequate level of protection, Art. 72(1a) | No | Yes, Art. 72(1b) | the implementation of pre-contractual measures, the performance of a contract, and the benefit of the individual, Art. 72(1)(c,d,e) |

**Table 12: Cross-jurisdiction data transfer across data protection laws.**

| Law | Reasons for Automatic Deletion | Exemptions | Right to Delete | Duration of deletion after executing right to delete |
|---|---|---|---|---|
| GDPR | No longer than is necessary for the purposes for which the personal data are processed, Art. 5(1e) | Public interest, scientific or historical research purposes or statistical purposes, Art. 5(1e) | Yes, Art. 17 | Without undue delay, Art. 17(1) |
| CCPA | Complete the transaction, security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, debug to identify and repair errors that impair existing intended functionality, exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law, and comply with the California Electronic Communications Privacy Act, comply with a legal obligation, and purposes like scientific, historical, or statistical research, Art. 1798.105(d) | Yes, Art. 1798.105(a) | Not given | Not given |
| DPDPA | Withdrawing consent or purpose achieved, Art. 8(7)(a) | Unless retention of the same is necessary for the specified purpose or compliance with any law, Art. 13(3) | Yes, Art. 12(3) | Not given |
| PIPL | Fulfilled purpose – Art. 19, 47(1), the agreed storage period has expired – Art. 47(2), consent withdrawal – Art. 47(3), violation of laws by the organization – Art. 47(4) | Administrative regulations, Art. 19 | Yes, Art. 47 | Not given |
| LGPD | Purpose achieved, end of the processing period, right to revoke consent, a violation of the provisions, Art. 15 | Legal obligation, research entity, Art. 16 | Yes, Art. 18(6) | Not given |
| POPIA | Purpose achieved, *i.e.*, no longer authorized to retain the record, Art. 14(4) | Required or authorized by law, historical, statistical or research purposes, Art. 14(1),14(2) | Yes, Art. 24(1) | As soon as possible, Art. 24(2) |

**Table 13: Data deletion rules across data protection laws.**

| Law | Records of Processing | Data Protection Officer | Impact Assessments | Regulatory Reporting Obligations | Maximum Penalties |
|---|---|---|---|---|---|
| GDPR | Mandatory, Art. 30 | Mandatory, only if sensitive and personal information collected at large scale, Art. 37 | New technologies, high risk to the rights and freedoms of natural persons, processing on a large scale of sensitive and personal information, Art. 35(1) | Supervisory authorities may ask for records of processing, Art. 30(4) | Up to €20M or 4% of global annual turnover, Art. 83 |
| CCPA | Not defined for keeping the processing records | | | | $7,500 per intentional violation, $2,500 per unintentional violation, Art. 1798.155 |
| DPDPA | Not defined | Mandatory, Art. 10(2) | Periodic assessment report should include a description of the rights of individuals, the purpose of processing of their personal data, the risk to the rights of individuals, Art. 10(3) | Ensure compliance, Clause 27 | Rupee ₹ 250, Art. 33 |
| PIPL | Mandatory, Art. 55 | Mandatory, Art. 52 | Impact assessment will be done, but what it will include is not defined, Art. 55 | State cyberspace administration is deeply involved, Art. 60-65 | Up to RMB 50M or 5% of annual turnover, Art. 66 |
| LGPD | Mandatory, 37 | Yes, Art. 41 | Should include the description concerning the personal data processing that could pose risks to civil liberties and fundamental rights, as well as measures, safeguards and mechanisms to mitigate said risk — Art. 5(17) | The national authority may determine that the controller must prepare a data protection impact assessment, which shall include personal data, sensitive data, and data processing operations, Art. 38 | Up to 2% of revenue in Brazil, capped at 50M BRL per violation, Art. 52(2) |
| POPIA | Mandatory, Art. 17 | Mandatory, Art. 55 | Not defined | Providing authorization to organizations before they collect personal data, Art. 57(1) | At most 10M or imprisonment up to 10 years, Art. 107 and 109(2)(c) |

**Table 14: Accountability rules across data protection laws.**

Note that while all laws require data deletion once the purpose is fulfilled, only GDPR and POPIA further mandate deletion without undue delay. Others do not specify a timeline for deleting data after the purpose is completed. Furthermore, all laws, except California's CCPA, give individuals the right to delete.

*4.2.5* **Accountability.** Accountability requires organizations not only to comply with data protection obligations but also to *demonstrate compliance in a verifiable manner*. This principle ensures that organizations maintain internal governance, monitor risks, and provide transparency to regulators and individuals.

Table 14 compares the accountability principles across different parameters, such as: (*i*) *Records of Processing*, which captures the obligation of organizations to maintain detailed information about the personal data they process and the purposes of processing; (*ii*) *Data Protection Officer*, a designated officer responsible for overseeing compliance, implementing data protection policies, and serving as the point of contact with regulators and individuals; (*iii*) *Impact Assessments*, reflecting whether privacy or risk assessments must be conducted prior to high-risk processing, such as large-scale collection of sensitive data or use of new technologies; (*iv*) *Regulatory Reporting Obligations*, which describe the requirements for organizations to provide reports to government authorities to demonstrate compliance; and (*v*) *Maximum Penalties*.

Except for India's DPDPA, all laws require organizations to retain records for processing. However, all laws require an organization to appoint a data protection officer. China's PIPL is the only law that requires a higher authority, namely the State Cyberspace

| Law | Regulatory Authority | Independence | Appointment | Term Duration |
|---|---|---|---|---|
| GDPR | Supervisory Authorities in each EU member state, Art. 51(1) | Yes, Art. 52(1) | Appointed nationally according to national law, Art. 53 and 54 | At least 4 years, Art. 54(1)(d) |
| CCPA | California Privacy Protection Agency, Art. 1798.199.10 | Not explicitly mentioned | Appointed by the Governor, Art. 1798.199.10 | At most 8 years, Art. 1798.199.20 |
| DPDPA | Data Protection Board of India, Art. 18(1) | Yes, Art. 28(1) | The Indian Government, Art. 19(2) | 2 years, Art. 20(2) |
| PIPL | State cyberspace administration, Art. 60 | Not independent, work under relevant departments under the State Council, Art. 60 | Not given | Not given |
| LGPD | National Data Protection Authority (ANPD), Art. 55(1) | Yes, Art. 55(2) | Appointed by the President of Brazil and approval by the Federal Senate, Art. 55(4)(1) | 4 years, Art. 55(4)(3) |
| POPIA | Information Regulator, Art. 39 | Yes, Art. 39(2) | Members appointed by President President, Art. 41(2)(a) | At most 5 years, Art. 41(3) |

**Table 15: Regulatory authorities across data protection laws.**

Administration, to be deeply involved in the accounting process. In contrast, California's CCPA is the only law that does not impose any accountability rule for the keeping the record of processing. However, CCPA requires maintaining records of other activities, such as request by a consumer to opt out of the sale, business compliance with a consumer's opt-out request, Article 1798.185(a)(4).

*4.2.6* **Lessons.** Data protection laws share common foundational principles, such as lawful processing, transparency, purpose limitation, data minimization, and data security, yet the rigor with which these obligations are implemented and enforced varies considerably across jurisdictions. Among these obligations, accountability plays the most critical role in building user confidence: when organizations are required to document their practices, justify their processing activities, and demonstrate compliance, other obligations, such as breach management, cross-border transfer controls, and data deletion, naturally become more enforceable and verifiable.

In terms of accountability, GDPR and PIPL impose the most demanding organizational requirements, including strict purpose limitation and documentation of processing. On the other hand, CCPA follows a more flexible, business-oriented model with fewer procedural burdens. DPDPA, LGPD, and POPIA fall between these extremes: they introduce meaningful organizational responsibilities but allow jurisdiction-specific exceptions and flexibilities that limit uniformity in operational practice.

## 4.3 Laws in terms of Government

**Objectives.** The effectiveness of data protection laws depends not only on organizational compliance but also on the oversight provided by government and regulatory authorities. While accountability obligations require organizations to implement internal mechanisms for data protection, these measures must be complemented by independent authorities empowered to supervise, investigate, and enforce compliance. Data protection laws, therefore, establish regulatory bodies with varying levels of independence, appointment mechanisms, and operational mandates.

Our objective in this section is to analyze the role of governments and regulators under different data protection laws. §4.3.1 will discuss how different laws establish regulatory bodies, and §4.3.2 will discuss how regulatory bodies can investigate organizations in their jurisdictions.

*4.3.1* **Regulatory Authorities.** Regulatory authorities are responsible for ensuring the effective implementation and enforcement of data protection laws, overseeing compliance, investigating complaints, issuing guidance, and imposing corrective measures.

Table 15 compares the regulatory authorities in terms of four parameters: (*i*) *Regulatory Authority*, lists the designated body responsible for law enforcement; (*ii*) *Independence*, indicates whether the authority operates independently or is subordinate to government entities; (*iii*) *Appointment*, describes how the members of the authority are appointed; and (*iv*) *Term Duration*, specifies the length of service for the members of the authority.

In summary, while all data protection laws formally establish regulatory authorities, their design and autonomy differ substantially. GDPR, LGPD, and POPIA rely on autonomous regulators with defined appointment procedures and fixed terms. In contrast, China's PIPL places regulatory oversight under the State Cyberspace Administration, resulting in a highly centralized model with limited structural independence and no specified term durations. DPDPA and CCPA fall between these extremes.

*4.3.2* **Investigations by the Authorities.** Government authorities are vested with distinct investigative powers that determine how they monitor compliance, initiate inquiries, and respond to violations of data protection laws. Table 16 compares these laws on the following three dimensions: (*i*) *Investigation triggers* that specify the conditions under which regulators are authorized to initiate investigations, such as complaints from individuals, breach notifications, or regulator-initiated inquiries; (*ii*) *Investigative powers* that define the procedural authorities granted to regulators to examine compliance, including conducting audits, summoning individuals, demanding documents and records, performing on-site inspections, and, in some jurisdictions, seizing equipment or individuals to judicial authorization; and (*iii*) *Corrective powers* that describe measures available to regulators to remedy non-compliance.

In summary, GDPR offers corrective powers. DPDPA and POPIA offer strong investigative authority. Under DPDPA, the Data Protection Board is empowered to exercise powers similar to those of a civil court of India. Similarly, under POPIA, the Information Regulator may conduct investigations and seek court-issued warrants, with judicial involvement.

## 5 Conclusion

This paper presented a comparative analysis of privacy regulations that cover approximately 38.3% of the world's population. We examined these laws through a data life-cycle lens to understand how user rights, organizational obligations, and government enforcement mechanisms are defined and executed across the phases of data collection, storage, processing, sharing, deletion, and bequeathal. Our analysis shows that, although data protection laws pursue similar high-level goals, their interpretations, scope, and enforcement vary substantially across jurisdictions and across different stages of the data life cycle.

| Law | Investigation Triggers | Investigative Powers | Corrective Power |
|---|---|---|---|
| GDPR | Complaints lodged by an individual, another supervisory authority, or other public authority Art. 57(1)(f), 57(1)(h) | Audits and review Art. 58(1)(b), 58(1)(c) | Issue warnings, issue reprimands, a temporary or definitive limitation, including a ban on processing, Art. 58(2) |
| CCPA | California Privacy Protection Agency-initiated Art. 1798.199.55.(a) and complaints, Art. 1798.199.45 | Subpoena witnesses, compel their attendance and testimony, administer oaths and affirmations, take evidence and require by subpoena the production of any books, papers, records, or other items material to the performance of the agency's duties or exercise of its powers, including, but not limited to, its power to audit a business' compliance with this title, Art. 1798.199.65. | Not given |
| DPDPA | An intimation of personal data breach, and a complaint made by an individual regarding a personal data breach, Art. 27(1) | An inquiry, summoning and inspecting any data, book, document, register, books of account or any other document, Art. 28(3), 28(7) | Not given |
| PIPL | Complaints and reports relating to personal information protection, and illegal personal information processing activities, Art. 61(2), 61(4) | An inquiry, on-site inspection, and sealing up or seizing the equipment, Art. 63 | Not given |
| LGPD | Pleadings from an individual against the organization after the individual has demonstrated that he/she presented a complaint against the organization that was not solved in the timeframe established in the law, Art. 55J(5) | Audit, Art. 55J(16) and apply sanctions, Art. 55J(4), 55K | Not given |
| POPIA | Complaints from individuals, Art. 74 | Pre-investigation. Art. 76(1)a, 79, summon, Art. 81(1)a, search any premises, Art. 81(1)d, and a warrant by the High Court, a regional magistrate or a magistrate, Art. 82 | Not given |

**Table 16: Investigations under data protection laws.**

We further discussed that many practical compliance challenges faced by both organizations and individuals stem from non-uniform definitions and vague operational requirements in privacy regulations. Consequently, organizations struggle to design end-to-end compliant systems that function consistently across regulatory boundaries, while individuals often lack effective means to exercise and verify their rights beyond the data collection phase. Our analysis highlights the need for systematic end-to-end frameworks that bridge legal requirements with technical system design.

## Acknowledgments

Ritwik Banerjee was supported in part by the AI Innovation Institute at Stony Brook University (Award No. 102316; Project No. 1194042) and the U.S. National Science Foundation (Award No. CNS 2335686). Work of Indrakshi Ray and Ethan Myers was supported by NSF Award Number CNS 2335687 and State of Colorado Cybersecurity funding under SB 18-086.

## References

[1] Interdependent Privacy (IDP): tinyurl.com/4n9p9d3p.
[2] DLA Piper: www.dlapiperdataprotection.com.
[3] OneTrust DataGuidance (IDP): tinyurl.com/yc5vvfpf.
[4] D. Abrokwa et al. Comparing security and privacy attitudes among U.S. users of different smartphone and smart-speaker platforms. In *SOUPS*, pages 139–158, 2021.
[5] A. Ardalani et al. Towards precise detection of personal information leaks in mobile health apps. *CoRR*, abs/2410.00277, 2024.
[6] O. Ayalon et al. Evaluating users' perceptions about a system's privacy: differentiating social and institutional aspects. In *SOUPS*, page 41–59, 2019.
[7] A. Barth et al. Privacy and contextual integrity: Framework and applications. In *IEEE SP*, pages 184–198, 2006.
[8] A. Boutet et al. "I'm not for sale" - perceptions and limited awareness of privacy risks by digital natives about location data. In *AAAI*, pages 277–288, 2025.
[9] K. Dhondt et al. Swipe left for identity theft: An analysis of user data privacy risks on location-based dating apps. In *USENIX Security*, pages 5053–5070, 2024.
[10] M. Fan et al. An empirical evaluation of GDPR compliance violations in Android mHealth apps. In *ISSRE*, pages 253–264, 2020.
[11] J. Feichtner et al. Understanding privacy awareness in Android app descriptions using deep learning. In *CODASPY*, pages 203–214, 2020.
[12] Y. Feng et al. AC-Net: Assessing the consistency of description and permission in android apps. *IEEE Access*, 7:57829–57842, 2019.
[13] M. Ferreira et al. RuleKeeper: GDPR-aware personal data compliance for web frameworks. In *IEEE SP*, pages 2817–2834, 2023.
[14] G. B. Herwanto et al. Leveraging NLP techniques for privacy requirements engineering in user stories. *IEEE Access*, 12:22167–22189, 2024.
[15] M. Humbert et al. A survey on interdependent privacy. *ACM Comput. Surv.*, 52(6), 2019.
[16] Q. Jia et al. Who leaks my privacy: Towards automatic and association detection with GDPR compliance. In *WASA*, pages 137–148, 2019.
[17] S. Koch et al. The OK is not enough: A large scale study of consent dialogs in smartphone applications. In *USENIX Security*, pages 5467–5484, 2023.
[18] K. Kollnig et al. A fait accompli? an empirical study into the absence of consent to third-party tracking in android apps. In *SOUPS*, 2021.
[19] J. Krämer. The death of privacy policies: How app stores shape GDPR compliance of apps. *Internet Policy Review*, 13(2), 2024.
[20] S. Li et al. Are we getting well-informed? an in-depth study of runtime privacy notice practice in mobile apps. In *CCS*, pages 1581–1595, 2024.
[21] D. Liu et al. ihunter: Hunting privacy violations at scale in the software supply chain on iOS. In *USENIX Security*, 2024.
[22] Z. Liu et al. Opted out, yet tracked: Are regulations enough to protect your privacy? *POPETs*, 2024:280–299, 01 2024.
[23] J. Mohan et al. Analyzing GDPR compliance through the lens of privacy policy. In *Heterogeneous Data Management, Polystores, and Analytics for Healthcare*, page 82–95, 2022.
[24] A. Mohanty et al. Hybridiagnostics: Evaluating security issues in hybrid smarthome companion apps. In *IEEE Security and Privacy Workshops*, pages 228–234, 2021.
[25] S. Neupane et al. On the data privacy, security, and risk postures of iot mobile companion apps. In *DBSec*, page 162–182, 2022.
[26] T. T. Nguyen et al. Share first, ask later (or never?) studying violations of GDPR's explicit consent in android apps. In *USENIX Security*, page 3667–3684, 2021.
[27] T. T. Nguyen et al. Freely given consent? studying consent notice of third-party tracking and its violations of GDPR in Android apps. In *CCS*, page 2369–2383, 2022.
[28] H. Nissenbaum. Privacy as contextual integrity. *Wash. L. Rev.*, 79:119, 2004.
[29] R. Pandita et al. WHYPER: towards automating risk assessment of mobile applications. In *USENIX Security*, page 527–542, 2013.
[30] A. Qamar et al. Detecting compliance of privacy policies with data protection laws. *CoRR*, abs/2102.12362, 2021.
[31] Z. Qu et al. Autocog: Measuring the description-to-permission fidelity in android applications. In *CCS*, page 1354–1365, 2014.
[32] I. Reyes et al. "Is our children's apps learning?" automatically detecting coppa violations. In *Workshop on Technology and Consumer Protection*, 2017.
[33] I. Reyes et al. "Won't somebody think of the children?" examining COPPA compliance at scale. *POPETs*, pages 63–83, 2018.
[34] G. Sassetti et al. Assurance, consent and access control for privacy-aware OIDC deployments. In *DbSec*, pages 203–222, 2023.
[35] D. Schmidt et al. Leaky apps: Large-scale analysis of secrets distributed in android and ios apps. In *CCS*, pages 2459–2473, 2025.
[36] R. G. Singh et al. A technical look at the indian personal data protection bill. *CoRR*, abs/2005.13812, 2020.
[37] A. Xiang et al. PolicyChecker: Analyzing the GDPR completeness of mobile apps' privacy policies. In *CCS*, pages 3373–3387, 2023.
[38] L. Zhang-Kennedy et al. "Whether it's moral is a whole other story": Consumer perspectives on privacy regulations and corporate data practices. In *SOUPS*, pages 197–216, 2021.
[39] S. Zimmeck et al. Automated analysis of privacy requirements for mobile apps. In *NDSS*, 2017.
[40] S. Zimmeck et al. Maps: Scaling privacy compliance analysis to a million apps. *POPETs*, 2019:66–86, 2019.
[41] N. Zufferey et al. "Revoked just now!" Users' behaviors toward fitness-data sharing with third-party applications. *POPETs*, 2023:47–67, 2023.