

A Systematic Analysis of Data Protection Regulations

Alexandra Klymenko*
 Technical University of Munich
alexandra.klymenko@tum.de

Stephen Meisenbacher*
 Technical University of Munich
stephen.meisenbacher@tum.de

Ali Asaf Polat
 Technical University of Munich
aliasaf.polat@tum.de

Florian Matthes
 Technical University of Munich
matthes@tum.de

Abstract

Data privacy has become central to the discussion surrounding the ever-growing usage of user data for advanced information systems. A strong legal response has come in the form of comprehensive and far-reaching data protection regulations, most notably spearheaded by the European General Data Protection Regulation (GDPR). Following in the footsteps of the GDPR, similar regulations have surfaced globally. With this steadily rising number of regulations, it becomes increasingly difficult to stay informed about new regulatory specifics; moreover, performing a comparative analysis of regulations can be quite complex. In this work, we perform a systematic analysis of 14 prominent data protection regulations from eight countries and the European Union, identifying a set of regulatory “aspects” as the basis for a comparative analysis. We present an artifact with side-by-side comparisons of these aspects for all selected regulations, helping researchers and practitioners alike who wish to comprehend the current data protection regulation landscape.

Keywords: Data Protection, Regulation, Data Privacy, Compliance, Comparative Analysis

1. Introduction

In the modern technological landscape, regulations have become central to the conduction of business, particularly in data processing scenarios. Where data originating from individuals is involved, companies processing such data must strictly comply with relevant data protection regulations, or else they run the risk of incurring significant fines (Wolff & Atallah, 2021). As

such, it is very important that data processing entities stay aware of applicable regulations and establish proper compliance programs. This task can be challenging, however, as modern data protection regulations outline somewhat complicated frameworks for data processing (Piras et al., 2019), with different regulations defining specific rules in often similar yet distinct ways.

While the trend towards stronger and more comprehensive regulations worldwide can be protracted as progress, the regulatory landscape continues to grow in a way that makes keeping up to date quite challenging for practitioners. Moreover, it becomes difficult to view different regulations from various jurisdictions in a comparative manner, even when well-versed in one’s native regulation (Bakare et al., 2024). This becomes especially important in large information systems within international enterprises, potentially involving multiple regulatory jurisdictions (Mattoo & Meltzer, 2018).

In this work, we are motivated by the prospect of comparatively analyzing data protection regulations from around the world, with the goal of exploring key similarities and differences. Most notably, we identify a set of *comparison aspects* which facilitate a side-by-side comparison of various regulations. As a result, we create a useful resource for researchers and practitioners alike, in the form of a systematic comparison of data protection regulations represented by a series of comparison tables. This described work is guided by two research questions:

- RQ1: What are the predominant data protection laws and regulations?
- RQ2: What are the most important comparative aspects of data protection laws and regulations?

Our work makes the following contributions to the intersection of information systems and regulation:

*Equal contribution.

1. We perform a comparative analysis of 14 selected data protection regulations from around the world.
2. We identify 37 comparison aspects under six categories that serve as the basis for this and future analyses of data protection regulations.
3. We provide a publicly available resource in the form of comparison tables summarizing the findings of our work, which can be found at <https://github.com/sebischair/regulations>.

2. Background and Related Work

The development of technology and an increasing amount of data gathered from individuals have resulted in a legal response from the authorities in the form of numerous *data protection regulations*. According to official records of UN Trade and Development, 137 out of 193 member countries have put legislation in place to secure data and privacy protection (UNCTAD, 2024).

Little work has been performed to analyze the growing number of global data protection regulations in a systematic way. From the legal sphere, *The Privacy, Data Protection and Cybersecurity Law Review* (Raul, 2021) presents a cursory survey of relevant legislation, but not in a structured manner that directly compares regulations, while another work (Bakare et al., 2024) focuses on comparing regulations from the EU and USA. Otherwise, to the best of the authors' knowledge, there are no structured reviews or comparisons of modern regulations in the academic literature. Instead, such comparisons can mainly be found in gray literature sources, for example from the IAPP, OneTrust Data Guidance, and others, as discussed in Section 5.

Regulations such as the GDPR are comprehensive and far-reaching, and as a result, are “difficult to apply also for its length [and] complexity” (Piras et al., 2019). As such, establishing proper compliance programs in organizations may be a challenging task, particularly in multinational companies facing international data transfer scenarios (Mattoo & Meltzer, 2018).

Klymenko et al. (2023) investigate challenges in the implementation of technical measures for data privacy compliance, among them *Many Regulations and Settings*, *Interpretation of Regulations* and *Technical-Legal Deadlock*. These challenges highlight the crucial role that the interpretation of regulations plays in compliance, particularly in cross-disciplinary communication. Therefore, we propose that a more structured overview of relevant regulations globally can aid practitioners of differing backgrounds to understand better the underlying foundations of modern data protection regulations, and accordingly, compliance programs can be made more effective.

3. Methodology

We describe the method followed in this work, consisting of a review of current regulations and an analysis of these regulations with the help of legal experts.

3.1. Review of Regulations

We reviewed the texts of the regulations and their corresponding recitals. The primary source of information for our comparative analysis is naturally the texts of all selected regulations (introduced in Section 4). These texts were read in full by one researcher and reviewed holistically as a team. A focus was placed on annotating key articles where important concepts were introduced. The concepts were iteratively updated and reviewed by the research team, in conjunction with evaluation sessions with legal experts, as discussed next.

In addition to these primary sources, we reviewed gray literature, as proposed by Adams et al. (2016), and used reports and articles from different organizations that focus on data privacy compliance. In particular, we relied on three main resources: The International Association of Privacy Professionals (IAPP)*, OneTrust Data Guidance*, and Baker McKenzie*. Above all, these sources were useful in guiding the creation of the comparison aspects presented in this work.

3.2. Iterative Evaluation with Experts

This research leverages an iterative and collaborative approach with legal experts to enrich the study's quality and insights from a legal perspective. Throughout the research process, a continuous and close dialogue with the experts was maintained, providing opportunities to seek their guidance and address pertinent inquiries effectively. Their expertise played a large role in shaping the presented research and evaluating our results.

To establish connections with these experts, both personal contacts and LinkedIn were used. An important criterion for selecting legal experts was the possession of certifications from the IAPP; such experts were given preference. The purpose of the research and the role of the experts in the study was clearly explained. Before conducting feedback sessions with the legal experts, assurance of confidentiality was provided, namely that their identities were to be kept anonymous in the research documentation to maintain privacy.

Table 1 presents the demographic details of the legal

*<https://iapp.org/>

*<https://www.dataguidance.com/>

*<https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook>

Table 1. Privacy Experts involved in Evaluation

ID	Role	Industry Domain	Organization size	Country	Experience
I1	Head of Legal	IT Consulting	Large	Germany	25+
I2	Senior Privacy Consultant	IT Consulting	Large	Germany	10-20
I3	Data Protection Officer	IT Consulting	Large	Germany	10-20
I4	LL.M. Candidate	Academy	-	Germany	0-5
I5	Privacy & Compliance Compliance Executive	Legal Compliance	Large	Germany	10-20
I6	Privacy Consultant	Legal Compliance	Medium	USA	5-10
I7	Data Security Specialist	Legal Compliance	Medium	USA	5-10
I8	Attorney at Law	Legal Compliance	Medium	USA	0-5
I9	Lawyer	Legal Compliance	Large	Japan	20-25
I10	Legal Partner	Legal Compliance	Medium	South Korea	20-25

experts who participated in the study, where *Experience* denotes years of professional experience. Experts I1-I5 supported the evaluation of selected regulations and comparison aspects via online interviews, while experts I6-I10 provided explanations for provisions under data protection regulations in a written form.

The sessions held with the legal experts were unstructured in nature. The live sessions began with an introduction of the current research progress (i.e., selected regulations and the comparison aspects), and proceeded by asking for any feedback regarding the aspects. Likewise, asynchronous feedback in written form was facilitated by first sending a draft of the current aspects to the expert, and receiving comments in return.

4. Selected Regulations

To narrow the scope of this study, we only consider a selection among the many laws and regulations around the globe. In particular, we use DLA Piper’s global data privacy tracking map*, which classifies data privacy legislation into four groups: heavy, robust, moderate, and limited. Initially, we decided to select only regulations from the “heavy” category, which is classified by DLA Piper accordingly to three metrics: *level of legislation*, *level of sanctions*, and *enforcement*.

According to the classification provided by DLA Piper, most of the European countries are marked as having heavily enforced laws, which are locally enhanced versions of GDPR. Since it is not feasible to examine all of them, we grouped these countries under the umbrella of the GDPR and named them the *European Data Protection Area*. Other countries that were marked as heavy and initially selected for examination are the USA, Canada, China, Bahrain, Mexico, South Korea, Singapore, and Australia.

To validate our choice of regulations, we conducted four evaluation sessions with legal experts working in privacy, namely I1, I2, I3, and I5. The goal of these sessions was to determine whether the chosen set of regulations was comprehensive and represented the

most relevant and predominant global data protection regulations. The primary feedback received was that the regulations of Mexico and Bahrain lack global impact, and rather the regulations from Brazil and Japan should be included. Additionally, it was suggested to study regulations stemming from multiple US states, leading to the choice of six predominant US state regulations.

Table 2 summarizes the data protection regulations selected for analysis in this study, specifically after the conducted evaluation sessions. Note that for the CCPA (California), we study both the CCPA and the additional CPRA (California Privacy Rights Act), the latter of which extends the CCPA with additional protections.

5. Results: Comparison Aspects

The first step in extracting comparison aspects for regulations was to conduct a literature review, gaining a deeper understanding of how separate laws are compared. In the legal field, various resources serve as reference handbooks. One such resource is OneTrust DataGuidance (2024). This initial resource was very valuable as it illuminated the key points within data protection regulations, along with their distinct characteristics. Secondly, we also utilized the privacy law directory available from the IAPP (2024). These resources served as the basis for our presented aspects, which were then validated and improved based on feedback received from experts, as discussed in Section 3.2. These steps resulted in a total of 37 comparison aspects in six categories, introduced in the following.

5.1. Principles

From our selected regulations, we extract the principles defined within that ensure organizations process personal data lawfully and treat individuals fairly, in a way that establishes trust, protects individual privacy, and responsibly manages personal data in compliance with data protection regulations.

Lawfulness. The lawfulness principle is one of the key principles of data privacy compliance, and most data

*<https://www.dlapiperdataprotection.com/>

Table 2. Selected Data Protection Regulations

Region	Acronym	Regulation	Source (English) Text
European Data Protection Area	GDPR	General Data Protection Regulation	(GDPR, 2016)
California (USA)	CCPA	California Consumer Protection Act	(CCPA, 2018)
Colorado (USA)	CPA	Colorado Privacy Act	(CPA, 2021)
Utah (USA)	UCPA	Utah Consumer Privacy Act	(UCPA, 2022)
Virginia (USA)	VCDPA	Virginia Consumer Data Protection Act	(VCDPA, 2021)
Connecticut (USA)	CTDPA	Connecticut Data Privacy Act	(CTDPA, 2022)
Iowa (USA)	IPA	Iowa Consumer Data Protection Act	(IPA, 2023)
Brazil	LGPD	General Data Protection Regulation of Brazil	(LGPD, 2018)
China	PIPL	Personal Information Protection Law	(PIPL, 2021)
South Korea	PIPA	Personal Information Protection Act	(PIPA, 2023)
Japan	APPI	Act on Protection of Personal Information	(APPI, 2021)
Canada	PIPEDA	Personal Information Protection and Electronic Documents Act	(PIPEDA, 2019)
Singapore	PDPA	Personal Data Protection Act	(PDPA, 2020)
Australia	-	The Privacy Act 1988	(“The Privacy Act 1988”, 2024)

Table 3. Summary of Comparison Aspects

Principles	Controller and Processor	Rights of Data Subjects
Lawfulness Fairness Transparency Purpose Limitation Data Minimization Accuracy Storage Limitation Integrity, Confidentiality, and Availability Accountability	Defining the Data Controller Defining the Data Processor Assigning a Data Protection Officer Binding Contract Between Controller and Processor Keeping Record of Data Processing Activities Data Breach Notifications Providing Safeguards for International Data Transfers Conducting a DPIA for High-Risk Activities Security Requirements	Right to Opt Out of Specific or All Processing Right to Access Right to Erasure Right to Data Portability Right Against Automated Decision Making Right to Correct Opt-in Right for Minors Right to Redress
Legal Basis	Enforcement	Thresholds
Consent Legal Obligation Performance of Contract Vital Interest Public Interest Legitimate Interest	Administrative Fines for Non-compliance Supervisory Authorities Personal Liability Private Right of Action	Compliance Requirements Based on Thresholds

privacy laws introduce legal bases to make processing lawful. Those are generally listed as consent, contract of performance, legal obligation, vital interest, public interest, and legitimate interest. Some laws also have additional legal bases, such as “protection of credit” in LGPD or “performance of statutory duties” in PIPL.

Fairness. The fairness principle is defined differently under various regulations. It is important to note that this principle is highly related to the transparency principle in terms of informing individuals about the purpose of collection, processing duration, existence of third parties, whether the personal data is sold or not, etc. Additionally, it requires informing data subjects about the existence of profiling and targeted advertising, as well as potential consequences of them. It can be clearly observed that all the laws agree on the fairness principle.

Transparency. Regulations require data controllers to be transparent, informing data subjects about collected data, the purpose of processing, and how to exercise their rights. We observe a common understanding of transparency amongst all studied regulations.

Purpose Limitation. Many data protection regulations, with the exception of UCPA, address the purpose limitation principle in a similar manner,

which is the collecting and processing of personal information with specific, explicit, and legitimate purposes. Additionally, they do not allow processing incompatible with the initial purpose, and when processing is required for a new purpose, additional consent from individuals must be collected.

Data Minimization. The data minimization principle is addressed in differing manners (see Table 4). Generally, all regulations agree upon minimizing data collection and processing to what is adequate, relevant, and necessary in relation to the purposes for which they are processed. As an exception, UCPA and PDPA have no explicit requirement for data minimization.

Accuracy. The notion of accuracy is addressed similarly amongst the different regulations we study. Generally, it is described as keeping personal data accurate and up to date, and if not, either correcting or deleting the data. Although the majority of the selected laws have a provision for accuracy, the regulations in the USA have no explicit requirement for the data controller to keep personal information up to date.

Storage Limitation. The storage limitation principle under different regulations is defined as keeping personal data only as necessary and deleting, destroying,

or making it anonymous after realizing the purpose of processing. Additionally, PIPL states that retention periods shall be the shortest period necessary to realize the purpose of personal information handling. On the other hand, CPA, CTDPA, UCPA, VCDPA, and IPA have no provisions for storage limitation.

Integrity, Confidentiality, and Availability. The integrity, confidentiality, and availability principle is addressed similarly for all selected regulations. It obligates the data controller and processor to establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and availability of personal data. The CCPA/CPRA does not make an explicit reference to integrity, confidentiality, and availability, but it states reasonable security procedures and practices that could be interpreted as an equivalent. Although controllers and processors are obligated to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks, it is not explicitly mentioned under CPA.

Accountability. The requirement for accountability varies rather significantly across regulations. For example, GDPR, LGPD, PIPL, PIPEDA, and PDPA emphasize that the data controller is responsible for the personal information under its control and shall demonstrate that it complies with the law. On the other hand, PIPA and the Privacy Act 1988 emphasize that supervisory authorities may request materials and documents to check the data controller's compliance. There are some exceptions to the data privacy laws in the USA. The principle of accountability is not an explicit requirement under these laws, but they recognize that the primary entity collecting data is ultimately responsible for the obligations. Also, APPI does not have any explicit reference to accountability, but it states that the data controller shall maintain a record of processing activities and implement appropriate measures to ensure data privacy. In this sense, accountability is partially covered.

5.2. Data Controller and Processor

According to data protection regulations, the responsibilities of data controllers and processors play a critical role in ensuring the protection of personal data. Data controllers have the responsibility for determining the purposes and means of processing personal data and must comply with applicable data protection laws. Data processors process personal data on behalf of controllers. In this section, we introduce aspects related

to data controllers and processors.

Defining the Data Controller. A key actor in privacy compliance is the data controller, and the majority of regulations define a data controller as the natural or legal entity that determines the purposes and means of the processing of personal data. Three exceptions include APPI, PIPEDA, and the Privacy Act 1988, which do not distinguish between the data controller and processor, although they are generally different actors.

Defining the Data Processor. The data processor is commonly defined under the majority of the regulations as a natural or legal person who processes personal data on behalf of the controller. As noted above, APPI, PIPEDA, and the Privacy Act 1988 do not distinguish between the data controller and processor.

Assigning a Data Protection Officer. The data protection officer (DPO) is also central to many regulations. The DPO is commonly defined as a person with expert knowledge of data protection law who assists the controller and processor in compliance. In addition, the DPO acts as a channel of communication between the data controller, data subject, and supervisory authorities. The regulations in the USA and APPI have no explicit requirement to assign a DPO. Similarly, the Privacy Act 1988 has no explicit requirement for DPO, but it is recommended in the compliance guidelines.

Binding Contract between Controller and Processor. In general, when the data controller decides to work with a processor, they shall have a legally binding contract that clearly sets forth instructions for processing data. LGPD states that when processors do not follow those instructions, they are jointly liable for damages caused by the processing. On the other hand, APPI, PIPEDA, PDPA, and the Privacy Act 1988 have no explicit requirement for such a binding contract.

Keeping Record of Data Processing Activities. Keeping a record of processing activities is one of the most controversial aspects of the studied regulations. While GDPR and LGPD define it as the data controller and processor maintaining records of processing activities carried out by them, APPI requires this record-keeping only for certain transfers of personal information. Furthermore, there are many differences in record-keeping amongst other laws. For example, CCPA/CPRA requires the data controller to keep records of consumer requests. CTDPA and

VCDPA stipulate obligations for deleting personal data when a data subject exercises his/her right. PIPA requires data controllers to manage and store login records, which document the access to data processing systems. PIPEDA requires keeping and maintaining a record of every breach of security involving personal information. PDPA requires organizations to preserve a copy of personal data that has been requested from an individual, where the organization refused to provide such data. Lastly, the Privacy Act 1988 does not have any requirements, but it is recommended to keep a record of the steps taken to comply with regulations.

Data Breach Notifications. One of the key obligations of data controllers is data breach notifications. All studied regulations agree on the definition by mentioning as soon as the controller becomes aware of a breach, supervisory authorities should be notified with relevant information. Based on the risk of possible consequences of the breach, the controller is obligated to inform affected individuals. In contrast, the regulations in the USA do not have provisions for data breach notifications, as generally, US states have separate laws for data breaches.

Providing Safeguards for International Data Transfers. The data controller is responsible for personal information in possession, including transferring it internationally. The majority of regulations include provisions regarding this matter. If there is not an adequate level of protection of personal data, the controller and processor shall take measures to ensure proper protection when transferring to foreign countries. There are no explicit requirements related to international data transfer in the US-based regulations.

Conducting a DPIA for High-Risk Activities. Conducting a Data Protection Impact Assessment (DPIA) for high-risk activities is obligated under the majority of data protection regulations. The regulations state that the data controller shall conduct a DPIA when processing personal data is likely to present a high risk to personal privacy. Some of these processing activities are exemplified by targeted advertising, profiling, selling personal data, and processing personal data, as given by CPA, CTDPA, and VCDPA. On the other hand, UCPA, IPA, APPI, and PIPEDA have no explicit requirement to conduct a DPIA. It is worth mentioning that although there is no explicit requirement under the Privacy Act 1988, it is recommended in the guidelines.

Security Requirements. Security requirements are an essential part of data privacy compliance and are highly related to the integrity, confidentiality, and availability principle. All of the selected regulations have obligations related to security. Generally, they state that the data controller and processor shall implement appropriate security measures like pseudonymization and encryption to protect personal information from unauthorized or illegal access, destruction, use, modification, or disclosure. In addition, the controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices as mentioned by the regulations in the USA, as well as LGPD, PIPA, and PIPEDA.

5.3. Rights of Data Subjects

Above all, data protection regulations aim to protect the rights of individuals. The rights of data subjects are addressed differently under different regulations. In this section, we will introduce the various rights of data subjects as outlined by our selected regulations.

Right to Opt Out of Specific or All Processing. The right to opt out of specific or all processing activities is one of the data subject rights and has a broad definition under data protection regulations. For example, the GDPR and PIPL have provisions that data subjects have the right to object and restrict the processing of their personal data unless laws or administrative laws stipulate otherwise. CCPA/CPRA and IPA state that data subjects have the right to opt out of the sale of their personal data. The CPA, UCPA, and VCDPA state that data subjects have the right to opt out of processing their personal data for different purposes, such as targeted advertising, the sale of personal data, or profiling. The Privacy Act 1988 allows data subjects to choose not to receive direct marketing communications. On the other hand, PIPEDA and PDPA have no explicit reference to the right to opt out of specific processing, but individuals may withdraw consent at any time, subject to legal or contractual restrictions and with reasonable notice.

Right to Access. Another right of data subjects is the right to access, and it is addressed very similarly under different data privacy laws. It states that the data subject has the right to confirm whether a data controller is processing his/her personal data, and to access this data.

Right to Erasure. The right to erasure is covered very similarly by all selected regulations. A data subject has the right to have his/her personal data erased when such data is no longer needed. However,

this is slightly different for PIPEDA, which states that the data controller shall delete personal information when the data subject demonstrates the inaccuracy or incompleteness of the personal information. On the other hand, this right has not been explicitly referenced in PDPA and the Privacy Act 1988.

Right to Data Portability. Yet another right of data subjects is the right to data portability, and the majority of the selected regulations have provisions for this right. It is generally mentioned that the data subject has the right to obtain personal data in a portable and readily usable format that can be transmitted to another entity. It should be noted that recently, the PDPA passed a provision on the right to data portability, to take effect when the regulation is issued. On the other hand, PIPA, APPI, PIPEDA, and the Privacy Act 1988 have no explicit requirements for data portability.

Right Against Automated Decision Making. Data subjects have the right under different regulations against automated decision-making. Generally, the right is introduced as the right not to be subject to a decision based solely on automated processing, including profiling, which has legal consequences concerning this person. While half of the selected laws have the same or similar provisions, the rest do not explicitly mention this right of data subjects.

Right to Correct. The right to correct is addressed similarly amongst the regulations, stating that data subjects have the right to correct inaccuracies in his/her personal data, taking into account the nature of the data and the purposes of the processing. UCPA and IPA do not explicitly mention this right.

Opt-in Right for Minors. The processing of personal information of a child can be lawful under certain regulations, where consent from a parent or legal guardian is obtained. Regulations based in the USA additionally cover the selling and sharing of the personal information of a child. The IPA states that personal data collected from a child is categorized as sensitive data and shall not be processed without complying with the Children's Online Privacy Protection Act (COPPA). This is also valid for other states in the USA. Another notable point is the age limit set under certain regulations. While GDPR and the USA-based laws set the age limit as sixteen, it is fourteen under PIPA and PIPL. PIPEDA and LGPD set the limit for thirteen, and PDPA and APPI define it as eighteen. There is no explicit statement about age under the Privacy Act 1988.

Right to Redress. Although regulations address the right to redress similarly, LGPD provides a broader definition, which concerns the controller or processor, who must redress damage in the case where data processing causes material, moral, individual, or collective damage to others in violation of applicable law. PIPEDA states that the court may award damages to the complainant. CPA, CTDPA, VCDPA, IPA, and APPI state no provisions regarding redress.

5.4. Legal Basis

Collecting and processing personal information depends a lot on the context, yet there usually must be an exact basis for data use. This comes with the exception of the US-based regulations, which generally allow processing information without any legal basis. In the following, we introduce six primary legal bases.

Consent. Consent is defined as a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Processing personal data is lawful with consent, where the data subject gives consent to processing their personal data for one or more specific purposes. This legal basis is addressed by nearly all studied regulations.

Legal Obligation. One of the legal grounds to make the processing lawful is a legal obligation. The controller has to comply with regulations, and in the case where processing is necessary to be compliant, the data controller is allowed to collect and process personal data. One example of this could be when employers are legally required to deduct income tax from their employee's paychecks and submit the correct amounts to the relevant tax and social security authorities. Here, they are allowed to collect and process the personal data of employees without their consent. Legal obligation is addressed under GDPR, LGPD, PIPL, PIPA, APPI, and PDPA; meanwhile, there are no explicit provisions under PIPEDA and the Privacy Act 1988.

Legitimate Interest. Another legal ground for lawful data processing is legitimate interest. The controller can process personal data if there is a *legitimate* reason for doing so. The most important point is that the legitimate reason can not override the interest or fundamental rights and freedoms of the data subject, especially if the data subject is a child. Examples of legitimate interests would be direct marketing, fraud detection and prevention, and network security. Legitimate interest is addressed under GDPR, LGPD, PIPA, and PDPA, which

allows data controllers to process personal information when they have legitimate interests, while the rest of the selected regulations make no mention.

Performance of Contract. Performance of contract means that each party included in a contract has to fulfill their respective obligations. Article 6 of GDPR states that when a contract requires so, it is allowed to collect and process personal information. Amongst the selected data privacy laws, only the GDPR, LGPD, PIPL, PIPA, and PDPA have explicit provisions for this basis.

Public Interest. Public interest concerns the welfare or well-being of the general public. Article 6 of GDPR states that processing personal data is allowed when public interest is involved, for example during a pandemic. Public interest is addressed under GDPR, LGPD, PIPL, and PDPA as a legal basis.

Vital Interest. Processing personal data is allowed to protect the vital interest of the data subject or another natural person. For example, when a data subject is unable to provide consent due to a medical condition, vital interest can be used as a legal basis for processing personal data. Vital interest is addressed as a legal basis under GDPR, LGPD, PIPL, PIPA, APPI, and PDPA.

5.5. Enforcement

Undoubtedly, the enforcement of data protection regulations has crucial importance in ensuring the compliance and accountability of organizations. Supervisory authorities are responsible for monitoring and enforcing these regulations, and they have the power to impose penalties in case of non-compliance.

Administrative Fines for Non-compliance. Enforcing data protection regulations often entails using administrative fines as a key tool to deter violations performed by data controllers. To incentivize controllers and processors to follow the rules, administrative fines may be imposed, and the amount of these fines varies based on the infringement and by regulation. For example, most of the USA-based regulations set the amount up to \$7500 for each violation, while under LGPD, fines amount to two percent of a private legal entity's revenue, up to 50 million BRL. The exact amounts and stipulations regarding fines vary amongst all studied regulations. In the case of CPA and CTDPA, no explicit provisions are made, as in these states, there are separate laws to address fines.

Personal Liability. Another method of enforcement provisioned within data protection regulations pertains to personal liability, wherein administrative fines are applicable to individual actors. While this provision is largely absent in many regulations, explicit mentions are made in PIPL, APPI, PIPA, PDPA, and the Privacy Act 1988. In addressing administrative fines for data controllers, authorities may also specifically charge a responsible person who causes the data violation or noncompliance. PIPL also states that it can be decided to prohibit these persons from holding future managerial positions for a certain period of time. In fact, APPI has provisions that state a person who violates the law can be punished by imprisonment or monetary fines.

Supervisory Authorities. Supervisory authorities to monitor compliance are an indispensable part of data protection regulations, and all studied regulations contain provisions for such bodies. Generally, these supervisory authorities are independent organizations that are responsible for enforcing regulations and ensuring that data controllers and processors act in compliance. Supervisory authorities have the power to investigate organizations when justified and impose sanctions and penalties for non-compliance. The naming of these authorities differs amongst the selected regulations; for example, the responsibility falls under the Attorney General in the US, and the Commission or Commissioner under PIPA, APPI, PIPEDA, PDPA, and the Privacy Act 1988.

Private Right of Action. Private right of action enables data subjects to initiate a civil action against data controllers in case of violation, where they can claim to recover damages and remedy. While the majority of selected data protection regulations have provisions for this right, there is no explicit provision in CPA, CTDPA, UCPA, VCDPA, IPA, and the Privacy Act 1988.

5.6. Thresholds

Compliance Requirements based on Thresholds. Data protection regulations obligate data controllers to comply, but some exceptions called thresholds place data processing activities out of scope. Compliance thresholds are present in all USA-based regulations, with GDPR and the Privacy Act 1988 also incorporating similar measures. Under USA-based regulations and the Privacy Act 1988, thresholds are defined based on metrics such as the amount of processed personal data, the percentage of selling data with respect to gross revenue, and others. The GDPR states that organizations with fewer than 250 employees are not subject to

Table 4. An Example Comparison Table for the Data Minimization Principle

Principles	
Data Minimization	
GDPR	"Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed." (<i>Article 5</i>)
CCPA/CPRA	"A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information is collected." (<i>Article 1798.100 of CCPA</i>)
CPA	"A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to specified purposes." (<i>Article 6.1.1308</i>)
CTDPA	"A controller shall limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer" (<i>Section 6</i>)
UCPA	N/A
VCDPA	"A controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer." (<i>Article 59.1.578</i>)
IPA	Personal data shall be processed to the extent that is "reasonably necessary and proportionate to the purpose listed in this section". It shall be "adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section." (<i>Article 715D.7</i>)
LGPD	Processing personal data shall be done with the necessity principle, which states the "limitation of the processing activity to the minimum necessary for the accomplishment of its purposes, with the comprehensiveness of the relevant data, proportional and not excessive in relation to the purposes of the data processing." (<i>Article 6</i>)
PIPL	"Personal information handling shall have a clear and reasonable purpose and shall be directly related to the handling purpose, using a method with the smallest influence on individual rights and interests." (<i>Article 6</i>)
PIPA	"A personal information controller shall collect the minimum personal information necessary to attain the purpose. The burden of proof that the minimum personal information is collected shall be borne by the personal information controller." (<i>Article 16</i>)
APPI	"A business operator handling personal information shall not handle personal information about a person (...) beyond the scope necessary for the achievement of the Purpose of Utilization." (<i>Article 16</i>)
PIPEDA	"The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization."; "Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified." (<i>Article 4.4</i>)
PDPA	N/A
The Privacy Act 1988	"The entity must not collect personal information unless the information is reasonably necessary for or is directly related to one or more of the entity's functions or activities." (<i>Article 3.1</i>)

keeping a record of processing activities, unless such processing poses a threat to the rights of data subjects.

6. Results: Artifact

Although we provide introductions to each of the 37 identified comparison aspects, we aggregate these analyses into a publicly available resource for a comprehensive comparative overview of data protection regulations. We make this resource available at the following link: <https://github.com/sebischair/regulations>. A sample comparison aspect table is found in Table 4. The resource we provide contains similar tables for each of the 37 comparison aspects.

Our artifact presents a side-by-side analysis of all 14 studied regulations for each comparison aspect. Relevant excerpts from the original texts are utilized for support, and all comparison points contain a brief explanation of the regulation-specific coverage of an aspect. In the cases where a comparison aspect is not relevant to a regulation, this is marked with "N/A".

Notably, the artifact maps each aspect to specific articles in the corresponding regulation texts, a detail we have left out in this work for brevity and readability. This feature is useful for readers to refer to the reference texts for the complete and original language.

7. Conclusion

In this work, we conduct a comparative analysis of 14 selected data protection regulations, guided by the foundation of 37 identified *comparison aspects*. In

addition, we release a public resource in the form of a comprehensive comparative overview of data protection regulations, which encompasses the findings of our work. We propose that the basis of comparison aspects can serve as a guiding directive for future comparative analyses of data protection regulations, while still being flexible to allow for comparison aspects to be updated.

With the ever-shifting regulatory landscape, it becomes important for researchers and practitioners to stay abreast of relevant changes. Our artifact enables this, while additionally serving as a comparative guide for those interested in learning about regulations beyond one's jurisdiction. This becomes especially important for organizations operating in a multinational context, particularly for privacy practitioners to be knowledgeable of data protection regulations beyond those that they might encounter in their daily work. On the academic side, our work opens the door for researchers to explore deeper into the topic of global data protection regulations, where future research can use this basis to uncover gaps, investigate practitioner perceptions, and develop other useful artifacts.

Accordingly, we hope for future works to extend and update our artifact, so that it becomes a living resource rather than a static document. Furthermore, the artifact would be well-served to be validated in more expert-based studies, potentially also with non-legal experts involved in the compliance process. As a final path for future work, we propose the creation of educational materials that will help to raise awareness about data privacy and applicable regulations in an easy-to-understand and interactive manner.

Disclaimer

The authors do not claim the information presented in this work to be a legal reference and do not assume liability. It is advisable for individuals and organizations to seek legal counsel tailored to their circumstances.

References

- Adams, R. J., Smart, P., & Huff, A. S. (2016). Shades of grey: Guidelines for working with the grey literature in systematic reviews for management and organizational studies. *International Journal of Management Reviews*, 19(4), 432–454.
- APPI. (2021). Act on the Protection of Personal Information [Accessed on: 14.06.2024]. <https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf>
- Bakare, S. S., Adeniyi, A. O., Akpuokwe, C. U., & Eneh, N. E. (2024). Data privacy laws and compliance: A comparative review of the eu gdpr and usa regulations. *Computer Science & IT Research Journal*, 5(3), 528–543. <https://doi.org/10.51594/csitrj.v5i3.859>
- CCPA. (2018). California Consumer Privacy Act [Accessed on: 14.06.2024]. https://coppa.ca.gov/regulations/pdf/coppa_act.pdf
- CPA. (2021). Colorado Privacy Act [Accessed on: 14.06.2024]. https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_enr.pdf
- CTDPA. (2022). The Connecticut Data Privacy Act [Accessed on: 14.06.2024]. <https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF>
- DataGuidance. (2024). Global privacy directory [Accessed on: 14.06.2024]. <https://www.dataguidance.com/laws>
- GDPR. (2016). The General Data Protection Regulation [Accessed on: 14.06.2024]. <https://gdpr-info.eu/>
- IAPP. (2024). Global privacy law and DPA directory [Accessed on: 14.06.2024]. <https://iapp.org/resources/global-privacy-directory/>
- IPA. (2023). Iowa Consumer Data Protection Act [Accessed on: 14.06.2024]. <https://www.legis.iowa.gov/docs/publications/LGE/90/SF262.pdf>
- Klymenko, O., Meisenbacher, S., & Matthes, F. (2023). Identifying practical challenges in the implementation of technical measures for data privacy compliance. *AMCIS 2023 Proceedings*.
- LGPD. (2018). General Data Protection Regulation of Brazil [Accessed on: 14.06.2024]. <https://lgpd-brazil.info/>
- Mattoo, A., & Meltzer, J. P. (2018). International Data Flows and Privacy: The Conflict and Its Resolution. *Journal of International Economic Law*, 21(4), 769–789. <https://doi.org/10.1093/jiel/jgy044>
- PDPA. (2020). Personal Data Protection Act [Accessed on: 14.06.2024]. <https://sso.agc.gov.sg/Act/PDPA2012>
- PIPA. (2023). Personal Information Protection Act [Accessed on: 14.06.2024]. https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG
- PIPEDA. (2019). Personal Information Protection and Electronic Documents Act [Accessed on: 14.06.2024]. <https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf>
- PIPL. (2021). Personal Information Protection Law [Accessed on: 14.06.2024]. <https://personalinformationprotectionlaw.com/>
- Piras, L., Al-Obeidallah, M. G., Praitano, A., Tsohou, A., Mouratidis, H., Gallego-Nicasio Crespo, B., Bernard, J. B., Fiorani, M., Magkos, E., Sanz, A. C., et al. (2019). DEFEND architecture: a privacy by design platform for GDPR compliance. *Trust, Privacy and Security in Digital Business: 16th International Conference, TrustBus 2019, Linz, Austria, August 26–29, 2019, Proceedings 16*, 78–93.
- Raul, A. C. (2021). *The privacy, data protection and cybersecurity law review*. Law Business Research Limited.
- The Privacy Act 1988 [Accessed on: 14.06.2024]. (2024). <https://www.legislation.gov.au/C2004A03712/>
- UCPA. (2022). Utah Consumer Privacy Act [Accessed on: 14.06.2024]. <https://le.utah.gov/~2022/bills/sbillenr/SB0227.pdf>
- UNCTAD. (2024). Data protection and privacy legislation worldwide [Accessed on: 14.06.2024]. <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>
- VCDPA. (2021). The Virginia Consumer Data Protection Act [Accessed on: 14.06.2024]. <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/>
- Wolff, J., & Atallah, N. (2021). Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020. *Journal of Information Policy*, 11, 63–103.