Data Privacy Law

Guidebook

Version: 1.0

Revised: January 2024

Contents

Summary

Data privacy laws are rapidly proliferating around the world. As the number of data breaches have soared and consumers have become increasingly aware and savvy, governments have responded by enacting new, strict regulations that govern how online data is collected, processed, stored, and sold.

This trend is unlikely to relent. The success of landmark legislation like the General Data Protection Regulation (GDPR) in Europe and other recent laws have created a snowball effect where jurisdictions increasingly build upon the progress of others, resulting in an accelerating movement toward broad, wide-reaching data privacy standards. By 2025, it is predicted that 75% of the world's population will be covered by modern privacy regulations.

For hoteliers, the increasing scope and stringency of data privacy law adds unprecedented complexity to an already high-stakes regulatory compliance game. Organisations seeking to avoid the potentially huge financial costs and make-or-break reputational damage of noncompliance will now have to contend with multiple overlapping (and potentially conflicting) sets of legislation.

Given this landscape, forward-thinking hoteliers should prioritize education and awareness. Although it is wise to rely on qualified counsel to navigate certain legal questions, it is also incumbent upon organisational leaders to have a foundational understanding of the precepts of data privacy law, be aware of the regulatory terrain in which they operate, and act accordingly to establish strong data privacy and security cultures on their teams.

To that end, this guide introduces and discusses the core concepts, requirements, and laws related to data privacy.

Fundamentals

For those new to the field, data privacy law can appear to be unapproachable and overwhelming. Due to its expansive impact and legalistic terminology, it has often been sidelined or tasked only to specialists and lawyers.

This does not need to be the case.

Privacy laws, at their core, are governed by principles that are both logical and straightforward.

To understand them, however, it is necessary to operate with a set of basic, fundamental knowledge. The following concepts are essential to grasp the meaning of these laws.

Protected Data

Privacy law is centered on protecting certain types of data that can be used to identify, contact, locate, or infer information about an individual, either directly or indirectly, in order to safeguard individuals' rights to privacy and autonomy in their personal information.

Most commonly, this type of data resides in a category of information that is termed *personal data*.

As defined in the GDPR, "personal data" includes any information relating to an identified or identifiable natural person. Examples include the following:

Identifiers Names, ID numbers, SSNs, etc.	**Contact Information** Addresses or phone numbers.	**Demographics** Age, gender, ethnicity, etc.
Financial Information Credit card numbers, bank accounts, income, etc.	**Health Data** Medical records, insurance information, genetic data.	**Employment Data** Work history or evaluations.
Educational Information Academic records, certifications, or training records.	**Online Identifiers** IP addresses, cookies, or RFID tags.	**Location Data** GPS data or other geo-location information.

In the United States, the narrower term "personally identifiable information" (PII) had often been used historically. However, with the increasing influence of the GDPR standard, modern state laws have frequently adopted the "personal data" language.

Although terminology in data privacy laws around the world can very, the core concept is frequently common—they each refer to information related to an individual that can identify them, either on its own or in conjunction with other data.

This consistency reflects a global convergence towards a broader, more inclusive understanding of what constitutes identifiable information in the digital age.

Key Players

Data privacy law involves various stakeholders with unique roles, rights, and obligations. Each has a distinct function and is impacted differently by law.

The table below breaks down the common categories of players and the typical way they are affected by privacy law.

Category	Definition	Legal Effect
Data Subject	Identified or identifiable natural person whose personal data is processed by a controller or processor. Formal name for a consumer or user.	*Rights*
Data Controller	Entity that determines the purposes and means of processing personal data. Formal name for the business or collecting entity.	*Responsibilities*
Data Processor	Entity that processes personal data on behalf of the data controller. The processor acts under the controller's instructions. For example, a cloud service provider or CRM provider.	*Responsibilities*

Regulatory Body	Authorities established by data privacy laws to oversee compliance and enforcement. For example, under GDPR, each EU member has a Data Protection Authority (DPA) responsible for monitoring and enforcing the regulation in their jurisdiction.	*None*

Elements of Law

Each data privacy law contains certain common elements that define its operation. Being aware of these will allow you to quickly assess the relevance and implications of new laws for your organisation.

The table below lists these elements and provides definitions for each.

Element	Definition
Timeline	Specific dates and milestones within the law. Note that the *enactment* date and *entry into force* are distinct.
Rights	Entitlements or privileges afforded to data subjects under the law.
Requirements	Obligations imposed by the law on entities that handle personal data.
Enforcement Mechanism	Procedures to address violations and ensure compliance. Typically, this is government enforcement by regulatory agencies, but can also include a private right of action.
Penalties	Sanctions or fines imposed for non-compliance. This can include disciplinary actions including injunctions or even criminal charges.

Requirements

Data privacy laws impose a series of requirements that alter the way personal data is collected, processed, and stored.

These mandates ensure that data is handled in a manner that respects individual autonomy and protects against misuse. The purpose of these laws is not to stifle innovation or impede the flow of information but to instill a culture of privacy that aligns with ethical use and societal expectations.

Data Subjects
Individuals / Consumers

Data Controllers
Organisations / Businesses

Typically, the requirements embedded within these regulations can be divided into two principal categories. The first category encompasses the rights granted to *data subjects* – the individuals to whom the data pertains. The second category delineates the obligations placed upon *data controllers*, the entities that determine the purpose and means of processing personal data.

Together, these rights and obligations form the dual pillars upon which the edifice of data privacy law stands.

This section will provide a detailed description of each type.

Consumer Rights

Many data privacy laws grant consumer additional rights that increase their ability to control how their data is collected or used. This section highlights some of the most common and significant rights found within recent legislation.

Opt-Out

Opt-out rights for data subjects refer to provisions within data privacy laws that allow individuals to choose not to have their personal data collected, used, or disclosed for certain purposes.

This right is particularly relevant in contexts such as direct marketing, where data subjects have the option to prevent organisations from using their personal data to send them promotional materials.

Opt-out rights can also apply to other data processing activities, such as selling personal data to third parties or sharing it for research purposes.

When data subjects exercise their opt-out rights, the data controller must comply with the request within a reasonable timeframe and cease the specific data processing activities for which the opt-out was requested.

Data privacy laws may mandate that organisations provide clear and straightforward mechanisms for data subjects to exercise their opt-out rights, often requiring that the opt-out option be as accessible and uncomplicated as the process of giving consent.

Data Use and Modification

Use and modification rights are included in many data privacy laws as a means of ensuring that individuals retain control over their personal information.

These provisions—which include rights such as access, correction, and deletion, and more—represent the central avenues through which data subjects can exert sovereignty over their data.

The implementation of these rights marks a shift towards greater transparency and agency for individuals in the management of their personal data.

It underscores the influence of the global movement towards recognizing the significance of personal data as an extension of personal autonomy.

The following table breaks down common data use and modification rights, their definitions, and their prevalence in modern privacy laws.

Right	Definition	Prevalence
Access	The right of a data subject to obtain from the data controller confirmation as to whether personal data concerning them is being processed, and, where that is the case, access to the personal data and information about its processing.	*Widespread*
Correction	The right of a data subject to have inaccurate personal data rectified, or completed if it is incomplete.	*Widespread*
Deletion	The right of a data subject to have their personal data erased by the data controller under certain circumstances, such as when the data is no longer necessary for the purpose it was collected or when the data subject withdraws consent. Also known as the "right to be forgotten."	*Widespread*
Objection to Automated Processing	The right to object to decisions made solely on automated processing, including profiling.	*Less Common*
Portability	The right to transfer personal data from one controller to another in a structured, commonly used, and machine-readable format.	*Increasing*

Controller Obligations

Under data privacy law, controller obligations are the comprehensive suite of legal and ethical duties that entities designated as data controllers assume when they determine the purposes and means of personal data processing.

These responsibilities are established to enforce accountability and ensure that data controllers operate not just within the bounds of legality, but also in a manner that respects the privacy and autonomy of data subjects.

This section details the most common and impactful types of obligations.

Privacy Notices

Privacy notices are formal communications that inform individuals about how their personal data is being collected, processed, and managed by an entity.

They serve to provide transparency regarding data processing activities and articulate the privacy practices of the data controller in clear terms. They ensure individuals are aware of the processing of their personal data and understand their rights in relation to that data.

Notices may cover several different types of activity. The table below details their usual forms and whether they are commonly found in modern privacy regulations.

Type	Definition	Common Requirement
Data Breach Notification	Sent to individuals and authorities in the event of a data breach that poses a risk to data subjects.	✓
Inferential Notice	Notices about data that has been inferred or derived from the analysis of collected data.	✗

Initial Notice	Provided at the time personal data is collected, detailing how and why data will be processed.	✓
Internal Notice	Communications within an organisation about general data handling practices not specifically directed at data subjects.	✗
Updated Policy Notice	Issued when there are significant changes to data processing activities or policies.	✓
Third-Party Marketing Notice	Specific disclosures to individuals regarding the use of their data for third-party marketing when the data has not been shared with the marketer.	✗

Consumer Consent

The consumer consent requirement is a central element in most data privacy laws, serving as a cornerstone of user autonomy over personal information.

Consent is defined as a freely given, specific, informed, and unambiguous indication of the data subject's agreement to the processing of their personal data.

This means that individuals must be provided with a clear choice regarding whether their data is used and for what purposes, without being subjected to any form of coercion, undue pressure, or deception.

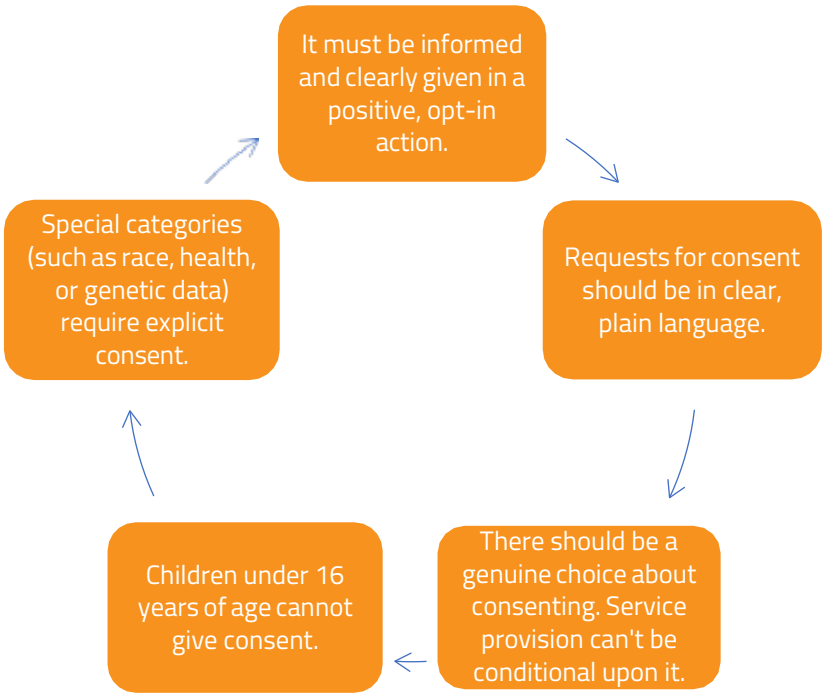
For consent to be valid, it must be given through an affirmative action that signifies agreement, such as checking a box on a website, choosing technical settings, or another

statement that clearly indicates acceptance of the proposed processing of personal data. Silence, pre-ticked boxes, or inactivity generally do not constitute valid consent under stringent data protection regimes like the GDPR.

Data subjects must be informed adequately and transparently about the scope and consequences of the data processing to which they are consenting. This includes who is collecting the data, what data is being collected, how it will be used, and whether it will be shared with third parties.

For sensitive categories of data, which include information about health, race, sexual orientation, religious beliefs, and more, the requirement for consent is typically more stringent, necessitating explicit consent.

The consent requirement reflects the overarching goal of data privacy laws to empower individuals with control over their personal data, ensuring that entities that collect and process data do so with the individual's explicit permission.



Key Criteria for Consumer Consent

Purpose Limitations

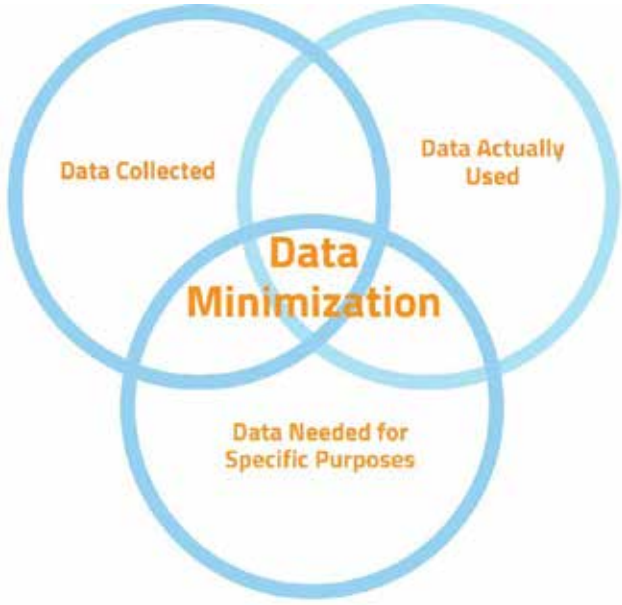
In addition to precise requirements, many privacy laws include principles that serve as overarching guidance for ethical and legal behavior. One such example is the "purpose limitation" principle, first established by the GDPR (Article 5 (1) (b)).

Put simply, this principle states that:

> *"Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes."*

This principle ensures that organisations are transparent about their reasons for processing data and restricts them from using the data for new, unrelated, or unlawful purposes without obtaining the data subject's consent or establishing another legitimate basis under the applicable law.

Purpose limitation helps maintain the data subjects' trust and upholds the integrity of the data processing activities.



Data Minimization Visualized

DPIA

A Data Protection Impact Assessment (DPIA) is a systematic and comprehensive analysis of how a particular project or system will affect the privacy of the individuals involved.

DPIAs are often required by data privacy law to help identify and minimize the data protection risks of a project.

For example, laws may make DPIAs mandatory when certain triggers occur, such as processing that involves systematic and extensive evaluation of personal aspects based on automated decision-making, large-scale processing of sensitive data, widespread surveillance of public areas, or other high-risk events.

DPIAs operate as standardized processes. Their exact implementation may vary, but it is helpful to understand them as involving four phases:

Data Protection Impact Assessment (DPIA) Process

- **Phase 1 – Preparation and Planning**

The initial phase determines whether a DPIA is necessary, defines its scope, and plans how it will be conducted. It includes identifying the data processing activities and the purposes for which personal data is being processed.

- **Phase 2 – Risk Assessment**

Phase two identifies and evaluates the potential risks to the rights and freedoms of data subjects that might result from its activities. This includes considering the nature, scope, context, and purposes of processing, as well as the likelihood and severity of risks.

- **Phase 3 – Mitigation Strategy Development**

Based on the risk assessment, phase three identifies measures that can mitigate risks. This involves deciding on actions to be taken to avoid or reduce the impact of the risks identified, ensuring data protection, and complying with applicable laws.

- **Phase 4 – Documentation and Integration**

The final phase documents the DPIA process and its findings. The DPIA report details the risks and mitigating actions. If necessary, the DPIA may be reported to a supervisory authority.

Laws

Interest in data privacy has been ramping up globally.

Since the passage of the landmark GDPR law in Europe, jurisdictions around the world have increasingly recognized the importance of protecting consumer data and have taken steps to require that businesses handle that information properly.

As illustrated below, most countries now have national-level data privacy laws:

Country-Level Data Privacy Law, 2024

GDPR

The GDPR is a European Union (EU) regulation that protects the privacy and personal data of EU citizens by setting guidelines for the collection, processing, and storage of personal information by organisations and businesses.

At the time of passage, it was a landmark achievement. It set new ambitious standards for data protection (such as consent requirements for data processing, Data Protection Officer requirements, and data minimization rules) and used the geopolitical and economic weight of the EU to forever shape the terms of the debate over consumer rights and privacy.

Its effects have been global. With reach that affects companies that do business entirely outside the EU (known as "extraterritoriality"), businesses around the world have been impacted by the law. In years following its passage, GDPR heavily influenced last in other jurisdictions, such as the CPRA in California and PIPEDA in Canada.

The significance of GDPR quite literally cannot be overstated.

Major requirements of GDPR include:

1. **Lawfulness, Fairness, and Transparency**

Personal data must be processed legally, fairly, and in a transparent manner in relation to the data subject. Organisations must have a legitimate basis for processing data, such as consent, and must clearly inform individuals about how their data is used.

2. **Purpose Limitation**

Data collected must be for specified, explicit, and legitimate purposes and not further processed in a way that is incompatible with those purposes.

3. **Data Minimization**

Organisations should only process the personal data that is necessary to achieve the processing purposes. This means limiting the data collected to what is directly relevant and necessary for the specified purpose.

4. **Data Subject Rights**

Individuals have rights over their data, including to access, rectify, erase, restrict processing, object to processing, and the right to data portability.

5. **Accountability and Data Protection by Design and by Default**

Organisations must demonstrate compliance by implementing data protection principles and integrating necessary safeguards into their data processing activities from the outset (by design) and ensure that by default, only personal data which is necessary for each specific purpose of the processing is processed.

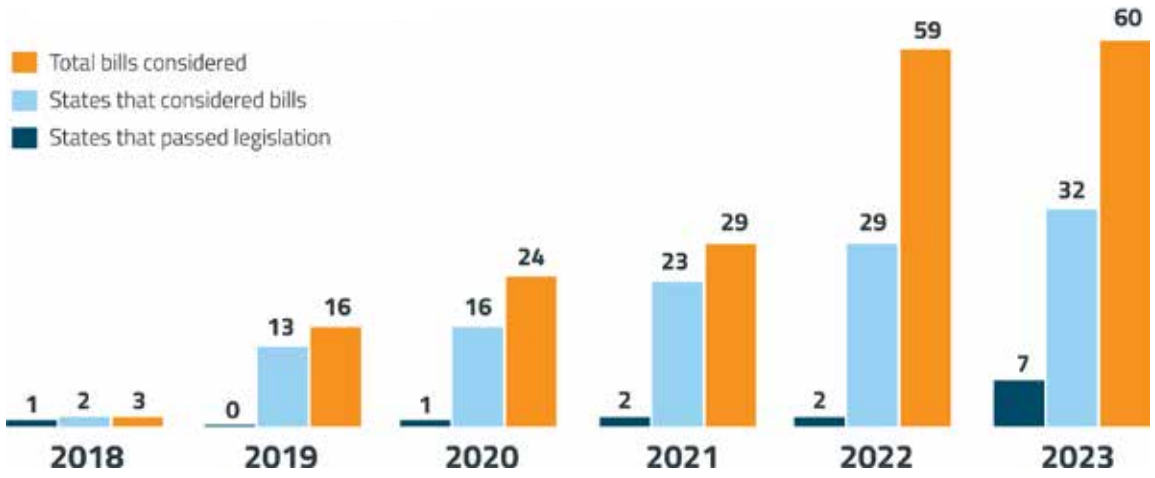
United States

The privacy law landscape in the United States differs significantly from that of the EU.

The United States is one of the few nations with no major overarching federal privacy legislation. While 2022 saw a new law—the American Data Privacy and Protection Act (ADPPA)—be introduced and gain some traction in Congress, it appears to have stalled without support in the Senate and analysts predict it will remain sidelined in the near future.

Because of federal inaction, U.S. data privacy law is primary governed at the state level.

As we have seen globally, interest in state privacy legislation has been exponential. The number of bills considered and passed has increased markedly over the past five years.



In many ways, 2023 was a breakthrough year for the passage of legislation. New bills were enacted in seven states, including the following:

Delaware
Delaware Personal Data Privacy Act (DPDPA)

Florida
Florida Digital Bill of Rights (FDBR)

Indiana
Indiana Consumer Data Protection Act (ICDPA)

Montana
Montana Consumer Data Privacy Act (MCDPA)

Oregon
Oregon Consumer Privacy Act (OCPA)

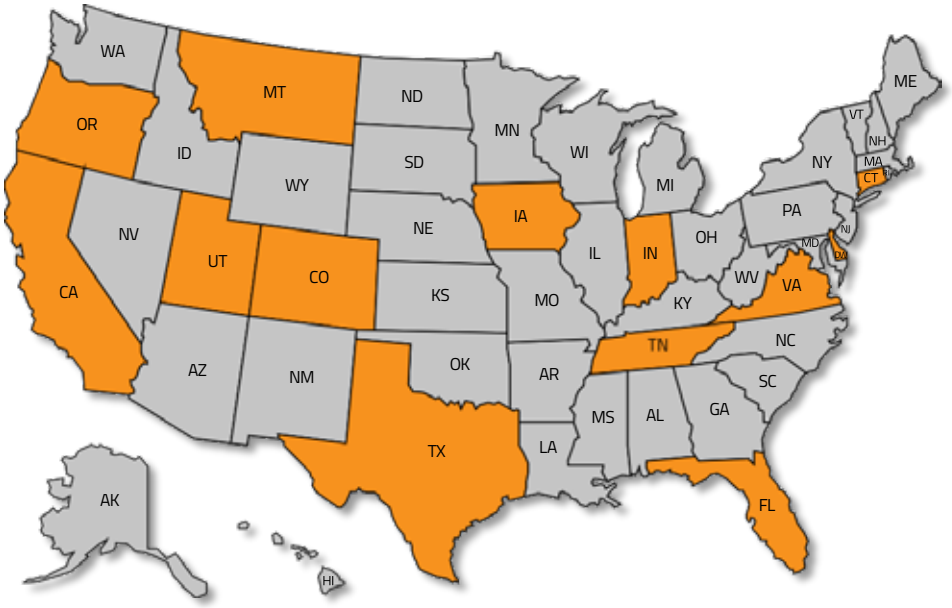
Tennessee
Tennessee Information Protection Act (TIPA)

Texas
Texas Data Privacy and Security Act (TDPSA)

Legislative action in the above jurisdictions is in addition to previously existing legislation in the following states:

 **California** California Privacy Rights Act (CPRA)	 **Colorado** Colorado Privacy Act (CPA)	 **Connecticut** Connecticut Data Privacy Act (CDPA)
 **Iowa** Iowa Law (Act Relating to Consumer Data Protection)	 **Utah** Utah Consumer Privacy Act (UCPA)	 **Virginia** Virginia Consumer Data Protection Act (VCDPA)

As a result, the current overall landscape of U.S. data privacy law is as follows:



State-Level Data Privacy Laws, 2024

Although each state law has some commonalities (they each seek to increase consumer rights and, for now, organizations seeking to comply would need to meet the highest applicable standard among states), there are enough dissimilarities that legal commentators refer to U.S. privacy law as a "patchwork." For example, opt-out and opt-in rights for digital advertising vary significantly and there is further potential for future changes as each state finalizes its rulemaking.

Given this, there is potential for the coming years to be a "pivotal milestone" in the push for regulatory convergence. Look for future steps to align state laws or seek ways to prevent overregulation. A long-time goal, there are signs that this year may see meaningful progress toward harmonization.

Other

Canada

Canada's current data privacy framework is primarily governed by the Personal Information Protection and Electronic Documents Act (PIPEDA).

Enacted in 2000, PIPEDA sets out the rules for the collection, use, and disclosure of personal information in the course of commercial activities across all provinces, except for those that have their own equivalent privacy laws. It applies to private-sector organizations and is overseen by the Office of the Privacy Commissioner of Canada.

PIPEDA is based on the principle of obtaining consent for the collection, use, and disclosure of personal information. It emphasizes the need for organizations to collect information only for reasonable purposes and requires them to maintain accurate, complete, and up-to-date data. Individuals have the right to access their personal information held by an organization and challenge its accuracy. The act also mandates appropriate security measures to protect personal data.

Over the years, PIPEDA has undergone amendments to address emerging privacy concerns, particularly relating to digital information and cross-border data flows. Currently, major updates to Canada's national laws have been proposed but not yet enacted.

India

India's data privacy laws are currently governed by the Digital Personal Data Protection Act (DPDP Act), enacted in 2023. The Indian government has not yet set an effective data and will likely pass follow-on legislation that will determine how the law is implemented.

The DPDP Act creates obligations for data fiduciaries, including requiring user consent before data processing and the establishment of safeguard measures to prevent breaches.

Consumers are granted rights, including to request a summary of their collected data and to correct, update, or delete it.

The Act also creates a Data Protection Board in India with significant power to investigate potential violation of the law and enforce its mandates.

The DPDP Act has extraterritorial scope. It applies to data processing outside of India if in connection with activity offering goods or services to subjects within India. This means international companies must comply with the law in processing data of Indian users.

Mexico

The Federal Law on the Protection of Personal Data Held by Private Parties in Mexico is the cornerstone of the country's legal framework for data protection in the private sector.

Enacted in 2010, it was a significant stride in aligning with global data privacy standards, reflecting principles like those in the European Union's GDPR.

The law's primary intent is to regulate the lawful, informed, and fair processing of personal data by private entities, ensuring the protection of individuals' privacy and fundamental rights.

It mandates data controllers to obtain explicit consent for the processing of personal data, except in specific exemptions provided by the law. Additionally, it emphasizes transparency, obligating data controllers to disclose the purpose and means of data processing.

It also empowers individuals with ARCO rights, granting them control over their personal information.

Resources

Continuing education on current developments is vital for professionals, organisations, and individuals who handle personal data.

To support this need for ongoing learning and legal compliance, the following section presents a curated list of external resources.

These resources, accessible without cost, offer a wealth of knowledge ranging from introductory materials to in-depth analyses and practical guidance on various aspects of data privacy.

International Association of Privacy Professionals (IAPP)

As the largest and most comprehensive global information privacy community and resource, the IAPP offers extensive training, policy guidance, and resources for privacy professionals. Read more here.

Baker McKenzie Global Data Privacy & Security Handbook

This resource hub, created by the law firm Baker McKenzie, offers guidance for companies to navigate data protection, privacy, and cybersecurity laws across various jurisdictions. Read more here.

Privacy Matters

DLA Piper's Global Privacy and Data Protection Resource includes reporting and expert legal analysis on data privacy trends. Read more here.

Google Business Data Responsibility Resources

Google offers training, as well as access to free analytics tools and open-source privacy technologies that help businesses understand and manage their data more effectively and responsibly. Read more here.

Glossary

Term	Definition
Biometric Data	Personal data resulting from specific technical processing related to physical characteristics that can identify an individual.
Consent	A freely given, specific, informed, and unambiguous indication of the data subject's wishes signifying agreement to personal data processing.
Data Breach	A security incident in which information is accessed without authorization.
Data Controller	The entity that determines the purposes and means of processing personal data.
Data Minimization	The principle that personal data collected should be limited to what is necessary in relation to the purposes for which they are processed.
Data Portability	The right of a data subject to receive their personal data in a structured, commonly used, and machine-readable format.
Data Processor	An entity that processes personal data on behalf of the data controller.
Data Protection Authority (DPA)	A public authority responsible for monitoring and enforcing data protection laws.

Data Subject	The individual to whom personal data belongs.
De-identified Data	Information from which identifiers have been removed to prevent a direct association with individuals.
Encrypted Data	Personal data that has been transformed through technological means to secure it against unauthorized access.
General Data Protection Regulation (GDPR)	A regulation in EU law on data protection and privacy in the European Union and the European Economic Area.
Information Commissioner's Office (ICO)	The UK's independent authority set up to uphold information rights in the public interest.
Legitimate Interest	A reasonable interest that a data controller has in processing personal data that is weighed against the data subject's interests or fundamental rights.
Personal Data	Information relating to an identifiable individual, such as names, ID numbers, and location data.
Privacy Impact Assessment (PIA)	A tool used to identify and reduce the privacy risks of entities by analyzing how personal information is handled.
Privacy by Design	A principle that calls for privacy to be taken into account throughout the whole engineering process of a product or service.
Processing	Any operation performed on personal data, from collection to destruction.
Profiling	Any form of automated processing of personal data to evaluate certain personal aspects relating to a natural person.
Pseudonymization	Processing personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information.

Right to Be Forgotten	The right of individuals to have their personal data deleted under certain circumstances.
Sensitive Personal Data	Personal data that includes genetic data, biometric data, data concerning health, racial or ethnic origin, political opinions, or sexual orientation.
Subject Access Request (SAR)	A request made by a data subject to obtain a copy of the personal data that an organisation holds about them.
Third Party	Any entity that is not the data subject, the controller, the processor, or persons who are authorized to process personal data under the direct authority of the controller or processor.
Transparency	The principle that information about the processing of personal data should be easily accessible and understandable to the data subject.
Two-Factor Authentication (2FA)	A security process in which the user provides two different authentication factors to verify themselves.
Unstructured Data	Information that does not reside in a traditional row-column database and is often text-heavy.
User Data	Data related to the behavior and interaction of users with services or products, often collected through online activities.
Violation	Failure to comply with data protection laws, which can result in enforcement actions and penalties.

About Venza

Venza is the leading provider of data protection and regulatory compliance for the hospitality industry. Drawing on decades of experience, Venza provides 360-degree visibility that enables proactive risk management to mitigate vulnerabilities and keep your guests and their data safe. Know your risks and protect your enterprise with Venza.

Visit www.venza.io for additional details.

Contact Us

Sales: sales@venza.io

Customer Success: success@venza.io