INTERNATIONAL FRAMEWORK AND STANDARDS GOVERNING PRIVACY AND DATA PROTECTION

Vikas Chaudhary, LLM, Dr. Ram Manohar Lohia National Law University, Lucknow

ABSTRACT

This chapter explores the development and application of international legal standards governing the right to privacy and personal data protection. It begins with foundational human rights instruments, particularly the *Universal Declaration of Human Rights* ("UDHR") and the *International Covenant on Civil and Political Rights* ("ICCPR"), both of which recognize privacy as a fundamental right. In response to growing concerns over digital surveillance and data misuse, several regional and international frameworks have emerged to guide the collection, use, and transfer of personal data.

Among the most influential is the European Union's *General Data Protection Regulation* ("GDPR"), which sets comprehensive rules for data processing, enshrining individual rights such as "data access", "erasure", and "portability". The chapter also reviews the *APEC Privacy Framework*, *Convention 108+*, and the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, each offering a unique perspective on cross-border data governance.

The chapter highlights key challenges in international data protection, including legal fragmentation, the complexity of cross-border data transfers, and balancing "data utility" with "privacy safeguards". It emphasizes the need for ongoing cooperation among governments, businesses, and civil society to develop adaptable, interoperable standards that protect privacy without hindering innovation.

As data continues to move across jurisdictions, the chapter argues for a harmonized, globally coherent approach to privacy governance. This is essential not only for legal compliance but also for enhancing public trust and promoting responsible digital transformation.

Keywords: Privacy, Data Protection, GDPR, ICCPR, UDHR, APEC, Convention 108+, OECD Guidelines, Data Security, Cross-Border Data Flow, Legal Compliance, International Law, Digital Rights, Personal Data, Global Governance, Accountability

Introduction

Privacy constitutes a fundamental human right, as articulated in Article 12 of the United Nations Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), along with various other international treaties.[1] The issue of data privacy is a worldwide concern, given that the collection and utilization of personal information affect individuals globally. The significance of customer data privacy lies in the necessity for individuals to maintain control over their personal information and its applications. Organizations that gather and utilize customer data bear the responsibility of safeguarding that information against unauthorized access and misuse.

A prominent data privacy framework is the General Data Protection Regulation (GDPR), enacted by the European Union (EU) in 2018. The GDPR is applicable to any entity that processes the personal data of EU citizens, irrespective of the entity's geographical location[2]. It establishes stringent requirements for the collection, utilization, and protection of personal data, including the necessity for explicit consent from individuals and the right to be forgotten[3]. Furthermore, it grants individuals the rights to access, correct, and delete their personal data, as well as the right to data portability.

In addition to the GDPR, the EU has introduced the ePrivacy Directive, which governs the use of electronic communication services and technologies, including cookies and direct marketing practices. Another notable data privacy regulation from the United States is the California Consumer Privacy Act (CCPA), which was enacted in California in 2018 and became effective in 2020. **The California Consumer Privacy Act (CCPA)** is applicable to businesses that gather and sell the personal information of residents in California. It establishes mandates for transparency and consumer rights, which encompass the ability to opt out of the sale of personal data and the right to request access to the personal data that has been collected.

[1] Md. Toriqul Islam, *A Brief Introduction to the Right to Privacy – An International Legal Perspective*, GLOBALEX (Jan./Feb. 2022), https://www.nyulawglobal.org/globalex/Right_to_Privacy1.html (last visited Jul. 28, 2025).
[2] European Union, *Data Protection Under GDPR*, YOUR EUROPE, https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm(last visited Jul. 28, 2025).
[3] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), art. 17, 2016 O.J. (L 119) 1.

Similarly, **the Asia-Pacific Economic Cooperation (APEC)** has formulated a set of data privacy principles referred to as the APEC Privacy Framework. This framework consists of voluntary guidelines designed to enhance data privacy while fostering cross-border trade and economic development within the APEC region.

Beyond these regional initiatives, various global organizations have also created guidelines and best practices pertaining to data privacy. **The International Association of Privacy Professionals (IAPP)** has introduced the Privacy by Design framework, which seeks to integrate privacy considerations into the development of products and services. Additionally, **the Organization for Economic Cooperation and Development (OECD)** has established guidelines aimed at safeguarding personal data, offering a framework for the collection, utilization, and protection of personal data on a global scale.

It is crucial to recognize that data privacy laws and regulations can differ markedly from one country to another, presenting challenges for organizations attempting to navigate these variations. To adhere to international data privacy standards, organizations must possess a comprehensive understanding of the applicable laws and regulations and implement effective data privacy policies and practices. This entails the regular review and updating of data privacy policies and procedures to ensure alignment with evolving legal requirements.

There is considerable reason for optimism. According to Gartner, by 2024[4], contemporary privacy regulations are expected to encompass the majority of consumer data. Nevertheless, the same report indicates that fewer than 10% of organizations will have effectively utilized privacy as a competitive advantage[5]. Contrary to the beliefs held by many businesses, emerging privacy regulations serve as facilitators rather than obstacles. These regulations can enhance business processes, improve data management, and lead to cost efficiencies.

As data flows become more globalized, it is essential for companies to develop a comprehensive understanding of international data privacy laws. Failing to do so could result

[4] Gartner, *Gartner Unveils Top Eight Cybersecurity Predictions for 2023–2024* (Mar. 28, 2023), https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024 (last visited Jul. 28, 2025).
[5] Ilia Sotnikov, *Why New Privacy Regulations Are a Business Enabler, Not an Enemy*, NETWRIX BLOG (Oct. 24, 2019), https://blog.netwrix.com/2019/10/24/why-new-privacy-regulations-are-a-business-enabler-not-an-enemy/ (last visited Jul. 28, 2025).

in substantial fines and other penalties[6]. Moreover, neglecting to provide adequate data protection for consumers could undermine their ability to attract and retain customers.

Key International Frameworks and Treaties

- **The Universal Declaration of Human Rights (UDHR)**

The Universal Declaration of Human Rights (UDHR) was ratified by the newly formed United Nations on December 10, 1948, as a reaction to the "barbarous acts which [...] outraged the conscience of mankind" during World War II.[7] This landmark adoption underscored the importance of human rights as essential for establishing freedom, justice, and peace.

At the time of the UDHR's adoption, there were approximately 10 million telephone lines globally. In contrast, as of this blog's publication, there are over 8.3 billion mobile connections, which include "machine to machine" links, and nearly 5.1 billion distinct mobile users. The anticipated growth of the Internet of Things is projected to connect around 30 billion devices by 2020. Additionally, research from IDC indicates that the world currently generates 16 zettabytes (equivalent to 16 trillion gigabytes) of data annually, with expectations for this figure to increase tenfold by 2025[8].

Article 12 of the UDHR states, "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*"[9] This article emphasizes that while the right to privacy is not absolute under international human rights law, any interference must be legally justified and undergo a thorough evaluation of its necessity and proportionality.

Since 2013, the United Nations General Assembly and the Human Rights Council have enacted multiple resolutions concerning the right to privacy in the digital era. The latest resolution on

[6] Mike Tierney, *Data Privacy Laws by State: Different Approaches to Privacy Protection*, NETWRIX BLOG (Aug. 27, 2019), https://blog.netwrix.com/2019/08/27/data-privacy-laws-by-state-the-u-s-approach-to-privacy-protection/ (last visited Jul. 28, 2025).
[7] Amnesty International, *Universal Declaration of Human Rights*, AMNESTY INTERNATIONAL, https://www.amnesty.org/en/what-we-do/universal-declaration-of-human-rights/ (last visited Jul. 28, 2025).
[8] Dunstan Allison-Hope, Mai Oldgard & Nicholai Pfeiffer, *The Right to Privacy, 70 Years On*, BSR BLOG (Jan. 18, 2018), https://www.bsr.org/en/blog/human-rights-to-privacy-70-years-on (last visited Jul. 28, 2025).
[9] Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III), art. 12 (Dec. 10, 1948).

this matter, A/HRC/RES/42/15, was adopted by the Human Rights Council in September 2019[10].

This resolution emphasizes that states must guarantee that any infringement on the right to privacy adheres to the principles of legality, necessity, and proportionality. It asserts that the rights individuals possess offline should also be safeguarded online, including the right to privacy. Furthermore, it recognizes that the utilization, implementation, and advancement of new and emerging technologies, such as artificial intelligence, can influence the realization of the right to privacy and other human rights.

Additionally, the resolution offers a series of recommendations directed at Member States and business entities to promote the respect and protection of the right to privacy in the digital landscape.

- **The International Covenant on Civil and Political Rights (ICCPR)**

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) articulates the following principles:

1. Individuals must not face arbitrary or unlawful intrusions into their privacy, family life, home, or correspondence, nor should they endure unlawful assaults on their honor and reputation.

2. Every person is entitled to legal protection against such intrusions or assaults.

The Human Rights Committee is responsible for overseeing the implementation of the ICCPR and provides General Comments addressing specific issues related to the Covenant.

On December 18, 2013, the United Nations General Assembly adopted a resolution concerning the right to privacy in the digital age. Additionally, the General Comment issued by the United Nations Human Rights Committee in 1988 regarding the right to privacy, family, home, correspondence, and the protection of honor and reputation under the ICCPR emphasizes that state surveillance must operate within a legal framework defined by clear and precise laws that

[10] Office of the High Commissioner for Human Rights, *International Standards*, OHCHR, https://www.ohchr.org/en/privacy-in-the-digital-age/international-standards (last visited Jul. 29, 2025).

prioritize the safeguarding of privacy rights.[11]

In the realm of privacy, General Comment No. 16, which addresses the right to privacy, family, home, and correspondence, as well as the protection of honor and reputation (Article 17) from 1988, and General Comment No. 19, which pertains to family rights, marriage, and spousal equality (Article 23) from 1990, hold significant relevance[12].

The collection and storage of personal data in computers, databases, and other devices—whether by public authorities or private entities—must be governed by law. States are required to implement e.ffective measures to ensure that information regarding an individual's private life does not fall into the hands of unauthorized individuals or entities and is not utilized for purposes that contravene the Covenant. To ensure robust protection of personal privacy, individuals should have the right to access information in a comprehensible format regarding whether, and if so, what personal data is retained in automated data files, as well as the purposes for which it is used. [13]

- **The Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which were adopted on September 23, 1980, continue to embody a global agreement on the fundamental principles governing the collection and management of personal data. By articulating essential principles, these Guidelines significantly aid governments, businesses, and consumer advocates in their endeavors to safeguard privacy and personal information, while also minimizing unnecessary barriers to transborder data flows, both online and offline. This document reflects over two decades of shared knowledge and experience among representatives from OECD member governments, the business sector, and civil society. It includes foundational instruments for global privacy protection: the 1980 OECD Privacy Guidelines, the 1985 Declaration on Transborder Data Flows, and the 1998 Ministerial

[11] Daniel Joyce, *Privacy in the Digital Era: Human Rights Online?*, 16 Melb. J. Int'l L. 1 (2015), https://law.unimelb.edu.au/__data/assets/pdf_file/0003/1586811/16109Joyce2.pdf (last visited Jul. 29, 2025).
[12] SFLC.IN, *Right to Privacy Under UDHR and ICCPR*, SFLC.IN (Oct. 24, 2017), https://privacy.sflc.in/universal/ (last visited Jul. 29, 2025).
[13] Human Rights Comm., General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) 186 (Apr. 8, 1988).

Declaration on the Protection of Privacy in Global Networks.[14]

The 2013 revision was similarly the culmination of several years of analytical efforts. A volunteer group of privacy specialists was established to support the review process, comprising experts from government, privacy enforcement authorities (PEAs), academia, the business sector, civil society, and the Internet technical community. This collaborative effort concluded that while the core principles of the 1980 Guidelines did not require fundamental changes, it was necessary to update the OECD Privacy Guidelines. The revisions in 2013 emphasized the practical application of privacy protection through a risk management framework and highlighted the need for enhanced global privacy initiatives. New concepts were introduced, including national privacy strategies, privacy management programs, and data security breach notifications. Additional updates aimed to modernize the OECD's approach to data flows, focusing on bolstering accountability and privacy enforcement[15].

The initial OECD Privacy Guidelines, established in 1980, were supplemented by an Explanatory Memorandum. In 2013, an additional Explanatory Memorandum was created to facilitate the implementation of the updated sections of these guidelines.

These guidelines pertain to personal data in both public and private sectors that, due to their processing methods, inherent characteristics, or usage context, may threaten privacy and individual freedoms. The Recommendation seeks to uphold and advance essential values such as privacy, individual rights, and the unrestricted global exchange of personal data, thereby enhancing economic and social interactions among OECD member countries.

The OECD Privacy Guidelines delineate eight Fundamental Principles of National Application in Part Two, which include limitations on collection, data quality, purpose specification, restrictions on use, security measures, transparency, individual participation, and accountability[16]. The relevance and significance of these principles were reaffirmed in both the

[14] Organisation for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Legal Instruments No. OECD-LEGAL-0188 (Sept. 23, 1980, updated 2013), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (last visited Jul. 29, 2025).
[15] Organisation for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Legal Instruments No. OECD-LEGAL-0188 (Sept. 23, 1980, updated July 11, 2013), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (last visited Jul. 29, 2025).
[16] Organisation for Economic Co-operation and Development (OECD), *OECD Privacy Principles*, http://oecdprivacy.org/ (last visited Jul. 29, 2025).

2013 revision and the 2021 implementation report. Part Three of the guidelines, introduced in the 2013 update, offers direction on applying the accountability principle. Additionally, the guidelines encompass a section on international application and justifiable limitations on the free flow of personal data (Part Four), a section detailing national implementation strategies for the basic principles (Part Five), and a section addressing international collaboration and interoperability (Part Six). [17]

- **The European Union's General Data Protection Regulation (GDPR)**

The General Data Protection Regulation (GDPR) was enacted by the European Union (EU) in 2016 and became effective on May 25, 2018. Its primary aim was to enhance individuals' rights regarding data privacy and to harmonize data protection laws across EU member states. In response to the challenges posed by the digital age and the increasing volume of online data usage, the GDPR superseded the 1995 Data Protection Directive. Its provisions are applicable to organizations both within Europe and outside of it when they handle data related to residents of the European Union[18].

The GDPR represents a thorough privacy regulation established by the European Union, which came into force in May 2018, replacing a previous EU data protection framework. It fortifies the privacy rights and safeguards for the data of EU citizens collected through online platforms.

The main elements of the GDPR include[19]:

- The requirement for explicit notice and consent prior to data collection and usage.
- The provision for users to access, amend, delete, or transfer their personal data.
- The obligation to notify about data breaches within a 72-hour timeframe.
- The necessity for evaluating data protection and security measures.

[17] Organisation for Economic Co-operation and Development (OECD), *Privacy Principles*, OECD, https://www.oecd.org/en/topics/privacy-principles.html (last visited Jul. 29, 2025).
[18] The Legal School, *What Is General Data Protection Regulation (GDPR)?*, THE LEGAL SCHOOL BLOG (2025), https://thelegalschool.in/blog/what-is-gdpr (last visited Jul. 29, 2025).
[19] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 33, 2016 O.J. (L 119) 1.

- The potential requirement to appoint a Data Protection Officer (DPO).
- The obligation for websites to provide contact information for users to exercise their data rights.

Data protection principles

When handling data, it is essential to adhere to the seven principles of protection and accountability as delineated in Article 5.1-2[20]:

1. **Lawfulness, fairness, and transparency** - Data processing must be conducted in a manner that is lawful, fair, and transparent to the individuals whose data is being processed.
2. **Purpose limitation** -Data should only be processed for the legitimate purposes that were clearly communicated to the data subjects at the time of collection.
3. **Data minimization** -Only the minimum amount of data necessary for the stated purposes should be collected and processed.
4. **Accuracy** -It is imperative to maintain the accuracy and currency of personal data.
5. **Storage limitation** -Personally identifiable data may only be retained for the duration necessary to fulfill the specified purpose.
6. **Integrity and confidentiality** -Data processing must ensure adequate security, integrity, and confidentiality, which may include the use of encryption.
7. **Accountability** -The data controller must be able to demonstrate compliance with GDPR in relation to all of these principles.

Accountable for upholding the GDPR requirements

The four key participants in the General Data Protection Regulation (GDPR) are 'data subjects',

[20]GDPR.eu, *What Is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ (last visited Jul. 29, 2025).

'controllers', 'processors', and 'Data Protection Authorities'[21]. 'Data subjects' refer to individuals—specifically, the natural persons whose personal data is being processed[22]. 'Controllers' are those who establish the purposes and methods for processing personal data, typically organizations or companies. 'Processors' are entities that handle personal data on behalf of controllers, creating a distinct hierarchy. For instance, if Company Y collects and analyzes customer survey data for Company X, following Company X's directives, then Company X acts as the controller while Company Y serves as the data processor. When two organizations collaborate to decide the reasons and methods for processing personal data, they are regarded as joint controllers, sharing the regulatory responsibilities and liabilities for any errors or mistakes that may occur.

GDPR Breaches and Fines

The General Data Protection Regulation (GDPR) delineates two categories of penalties for breaches, differentiating between minor and major infractions[23].

Minor Infractions:

1. Penalties may reach up to €10 million or 2% of the company's total global annual revenue, depending on which amount is greater.

2. These infractions pertain to regulations governing data controllers and processors, as well as certification and monitoring entities.

3. Both processors and controllers are required to comply with data protection regulations, ensuring lawful processing among other obligations.

4. Certification bodies are expected to perform evaluations in a transparent and unbiased manner.

[21] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4(1), 2016 O.J. (L 119) 1.
[22] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4(7), 2016 O.J. (L 119) 1.
[23] Tata Communications, *What Is General Data Protection Regulation (GDPR) Compliance?*, TATA COMMUNICATIONS KNOWLEDGE BASE, https://www.tatacommunications.com/knowledge-base/general-data-protection-regulation-gdpr/ (last visited Jul. 30, 2025).

Major Infractions:

1. Fines can amount to €20 million or 4% of the company's total global annual revenue, whichever is higher.

2. These infractions violate fundamental GDPR principles, such as the right to privacy and the right to erasure.

3. This category includes principles related to lawful data processing, conditions for obtaining consent, and the rights of data subjects.

4. The transfer of data to international organizations or third countries is also included in this classification.

- **The Asia-Pacific Economic Cooperation (APEC) Privacy Framework**

APEC established its privacy policy in 1994, paralleling the OECD's privacy policy from 1980[24]. The organization comprises 21 member countries, including notable examples such as the United States and Australia. APEC was created to address and deliberate on issues related to trade liberalization, promoting free trade throughout the Asia-Pacific region. India was excluded from membership due to its non-trading economy, which explains its absence from APEC since 1989.

In 2007, APEC launched the Data Privacy Pathfinder Initiative to operationalize its privacy framework. A key achievement of this initiative was the creation of the APEC Cross Border Privacy Rules (CBPR) system, designed to foster trust among consumers, businesses, and regulators regarding the cross-border transfer of personal information[25].

On November 23, 2018, Australia joined the APEC CBPR system[26]. This system mandates that participating businesses formulate and enforce data privacy policies that align with the APEC Privacy Framework. These policies are evaluated by an Accountability Agent, an independent entity recognized by APEC, typically from the private sector. By adhering to a mutually

[24] Karnika Seth, *Computers, Internet and New Technology Laws* (LexisNexis 2012).
[25] Ellyce R. Cooper & Alan Charles Raul, *APEC Overview*, in The Privacy, Data Protection and Cybersecurity Law Review (Alan Charles Raul ed., Law Bus. Rsch. Ltd. 2014).
[26] Attorney-General's Department, *Asia-Pacific Economic Cooperation and Privacy*, https://www.ag.gov.au/rights-and-protections/privacy/asia-pacific-economic-cooperation-and-privacy (last visited Jul. 30, 2025).

accepted set of regulations, the CBPR system reconciles the variations in domestic privacy practices across the region.

The established rules must conform to both the APEC Privacy Framework and the local laws of the economies in which the businesses operate. Furthermore, national privacy regulators provide additional oversight through the APEC Cross Border Privacy Enforcement Arrangement.

Accountability serves as the fundamental privacy principle that underpins the CBPR system. Businesses are responsible for upholding the commitments they make to their customers regarding the management of their personal data[27].

In contrast to the GDPR, which functions as a directly enforceable regulation, the CBPR system does not override or modify a nation's existing laws and regulations. In instances where a country lacks relevant domestic privacy protection standards, the CBPR system aims to establish a baseline level of protection.

The privacy enforcement authorities in a participating country should possess the authority to implement enforcement actions in accordance with applicable domestic laws and regulations, ensuring the protection of personal information in alignment with the requirements of the CBPR program[28].

- **Convention 108+**

Convention 108, established in 1981, currently has 55 Parties, which include 46 member states of the Council of Europe (not limited to the 26 EU Member States), as well as 10 non-member states from outside Europe—three from Latin America and five from Africa[29]. Additionally, the Russian Federation, although no longer a member of the Council of Europe, remains a Party to Convention 108. The Committee of Ministers of the Council of Europe has the authority to

[27]Graham Greenleaf, *APEC's Privacy Framework Sets a New Low Standard for the Asia-Pacific* (2006), in *Five Years of the APEC Privacy Framework: Failure or Promise?*, https://www.researchgate.net/publication/292357057_APEC's_privacy_framework_sets_a_new_low_standard_for_the_Asia-Pacific (last visited Jul. 30, 2025).
[28] Alex Wall, *GDPR Matchup: The APEC Privacy Framework and Cross-Border Privacy Rules*, INT'L ASS'N OF PRIV. PROS. (May 31, 2017), https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules (last visited Jul. 30, 2025).
[29] Council of Europe, *Portugal Joins Convention 108+* (Oct. 18, 2023), https://www.coe.int/en/web/data-protection/-/portugal-joins-convention-108 (last visited Jul. 30, 2025).

invite any non-member state to join the Convention (Article 23, paragraph 1). Consequently, Convention 108 has the potential for global reach. Any new Parties joining Convention 108 are also required to simultaneously accede to the updated Convention 108+ (CETS 223). The text for 108+ was finalized in 2018 and mandates 38 ratifications from the 55 Parties to Convention 108 for it to take effect. As of early 2024, there have been 31 ratifications, meaning that seven additional ratifications are needed from the remaining 23 Parties. Throughout 2024, the number of ratifications has remained at 31. It is anticipated that 108+ may come into force in 2025, contingent upon increased interest in securing the necessary 'decisive' ratifications[30].

Basic principles of Convention 108+, and benefits

The responsibilities of the Parties to Convention 108+ can be summarized in three main points:

(i) They are required to implement and rigorously enforce laws that realize all the stipulations of the Convention;

(ii) They must facilitate the transfer of personal data to other Parties of the Convention without obstruction;

(iii) They must refrain from permitting personal data transfers to nations that do not offer a sufficient level of protection. Essentially, this involves establishing a mutually recognized standard of data protection, which includes controls on data exports[31].

Challenges in International Data Protection

In the contemporary interconnected landscape, organizations encounter a multitude of challenges in adhering to global privacy regulations. As data privacy legislation continues to develop, companies must adjust their practices to fulfill the requirements set forth by various nations. This article will explore the primary obstacles associated with global privacy compliance, which include:

[30] Treaty Office, Council of Europe, *Memorandum on the Procedure for the Accession by States Which Are Not Member States of the Council of Europe* ¶ 8 (July 2022), https://rm.coe.int/16809028a4
[31] Graham Greenleaf, *The New Data Protection Convention 108+ and Its Importance for Asia* (Jan. 2025), https://ssrn.com/abstract=5032699 (last visited Jul. 30, 2025).

1. **Varied privacy legislation across nations:** Each country has its own set of privacy laws and regulations, complicating compliance for businesses that operate internationally. For instance, the European Union enforces the General Data Protection Regulation (GDPR), whereas the United States features a fragmented array of state and federal privacy laws. Navigating these differing legal frameworks can prove to be intricate and labor-intensive for organizations.

2. **Cross Broder data transfers**: As companies increasingly depend on cross-border data transfers for their operations, they must adhere to a range of legal frameworks that govern these transactions. Frameworks such as the Asia-Pacific Economic Cooperation (APEC) Privacy Framework establish specific requirements for data transfers, including notice, choice, accountability, security, and access. Ensuring compliance with these stipulations can be particularly challenging for businesses operating across multiple jurisdictions[32].

3. **Monitoring compliance**: Given the constantly evolving nature of privacy regulations, organizations must consistently track their adherence to various laws and standards. This involves staying informed about new privacy legislation, making necessary adjustments to their data protection practices, and ensuring that employees are well-trained on the latest privacy obligations.

4. **Achieving a balance between privacy and data utility:** Techniques designed to preserve privacy, such as encryption, anonymization, and differential privacy, focus on safeguarding individual privacy while facilitating data analysis[33]. Nonetheless, a compromise often exists between privacy and the utility of data, as enhanced privacy measures may result in the loss of critical information. Organizations must navigate this delicate balance to ensure both the protection of privacy and the retention of data usefulness.

5. **Safeguarding data security**: Protecting personal data is a fundamental component of privacy compliance. Given the rapid increase in data volume, organizations are required to adopt suitable security technologies and strategies to shield sensitive and personally

[32] Asia-Pacific Economic Cooperation (APEC), *APEC Privacy Framework* (2015), https://www.apec.org/docs/default-source/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_EC_APEC-Privacy-Framework-(2015).pdf (last visited Jul. 31, 2025).
[33] Benjamin C. M. Fung, Ke Wang, Rui Chen & Philip S. Yu, *Privacy-Preserving Data Mining in the Age of Big Data: A Survey of Recent Developments* (2023).

identifiable information. This process involves categorizing data based on risk levels and implementing measures to prevent potential breaches.

6. **Enhancing consumer awareness and control**: As consumers gain a better understanding of their privacy rights, it is essential for businesses to offer them more options for managing their privacy. This includes simplifying the process for consumers to submit data subject access requests (DSARs) and engage with cookie consent banners. By providing clear and user-friendly privacy management tools, businesses can foster trust with their customers and adhere to privacy regulations.

Conclusion

International viewpoints on data privacy legislation underscore the increasing significance of protecting personal information in today's digital environment. While regions such as Europe have made significant progress with the implementation of the General Data Protection Regulation (GDPR), other areas are at different stages of formulating and enacting comprehensive laws. As global connectivity intensifies, collaboration and the establishment of common standards will be essential for maintaining a secure and privacy-conscious digital ecosystem.

To tackle the challenges arising from varying legal frameworks and the rapid development of new technologies, continuous dialogue and partnership among governments, businesses, and civil society are imperative. The progression of data privacy regulations is expected to be influenced by technological innovations, societal demands, and the necessity to strike a balance between individual privacy protection and the encouragement of innovation. Moving forward, it is crucial for all stakeholders to collaborate in developing a unified and effective global framework that upholds the privacy and rights of individuals in the digital age.