Around the World in Regulation

An overview of the global regulatory environment for data privacy and protection in the modern contact center

NICE

CONTENTS

Introduction

Consumer protection regulations, including data privacy and protection requirements, are primarily designed to prevent deceptive business practices and fraud. The global regulatory environment is becoming more encompassing, with updated laws covering a broader scope of activities and more extensive enforcement options. For all enterprises, but especially global entities handling a tremendous amount of sensitive personal information, the web of regulations can be a source of significant compliance risk.

Multichannel, asynchronous, and noncontinuous customer interactions make adherence an even greater challenge. Regulatory complexity and requirements can change quickly, impacting the capability of organizations to balance compliance with good customer experience.

If not managed well, compliance can become a drain on resources and time – either through unnecessarily hesitant customer service or through non-compliance when it really counts. Customer complaints can stem from such compliance failures or lead to them when issues are not handled correctly or with sufficient speed. In either case, the best outcome is a quick resolution mitigating the risk of an escalation, which could lead to enforcement action and reputational harm.

And the penalties for any misstep can be pretty high.

In one year, from January 2022 to January 2023, data protection authorities across Europe issued fines collectively totaling €1.64 billion, which was a 50% increase over the previous year. The ,most significant fine for non-compliance issued under the General Data Protection Regulation (GDPR) to date (May 2023) was €746 million ($877 million), imposed in July 2021 by a Luxembourg court against tech giant Amazon.

Globally, the largest fine was $1.19 billion levied against the Chinese firm Didi Global for violating China's data security and personal information protection laws.

Other noteworthy fines due to regulatory non-compliance (but not triggered by actual security breaches or data leaks), include:

- €12.3 million was imposed on Vodafone by the Italian data protection authority due to unlawful processing of personal data, including violations of GDPR consent requirements, accountability, and data protection design (2020).
- €17 million was imposed on Meta by the Irish data protection authority for failing to have appropriate technical and organizational measures to demonstrate how security measures protect user data. (2018)
- €35.3 million imposed on H&M's Service Center by the Hamburg (Germany) data protection authority for violating recording consent requirements. An important and unusual aspect of this case is that the unlawful recordings were of several hundred H&M employees, rather than customers. (2020)

CONTENTS

Contact centers are the frontline of compliance.

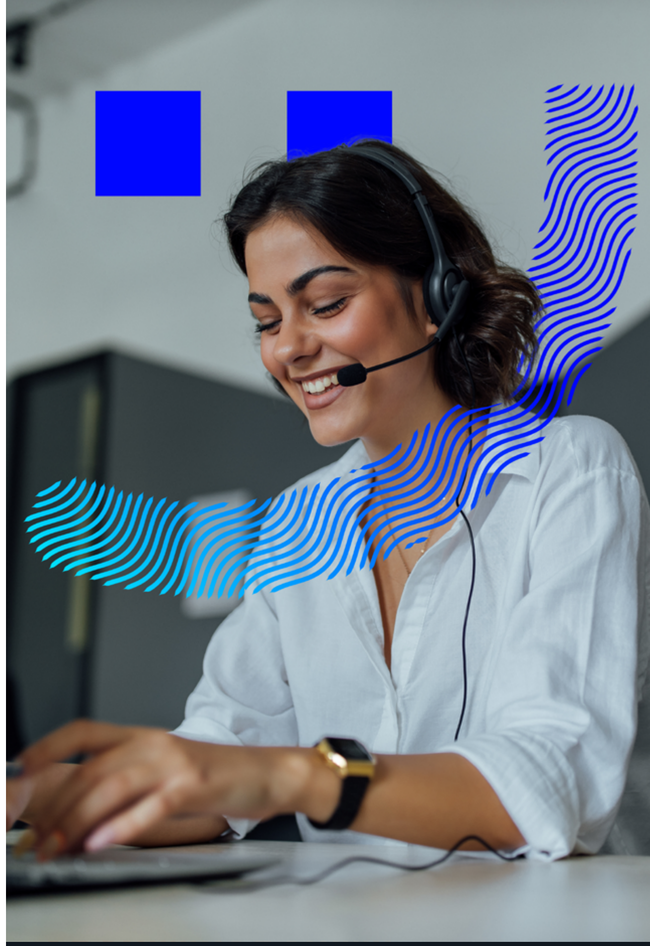
Contact centers face the most exposure in terms of regulatory compliance, as frontline agents navigate disclaimer scripts and customer consent in high-pressure, unpredictable and dynamic interactions. Customers often share sensitive, sometimes complicated, information with agents of varying skill sets, all of whom are naturally fallible and liable to be inconsistent. In addition, contact centers tend to handle high volumes of customer interactions, which they need to consistently monitor, record and analyze.

In a 2022 survey of 200 senior US and European call center decision-makers commissioned by NICE, 73% said that adhering to regulatory requirements is among their most significant concerns. While this is more pronounced in Europe (88%) than in North America (58%), privacy and regulation issues universally top the list of concerns for compliance officers. Despite this, 66% of call centers reported relying on traditional processes for handling sensitive authentication data, such as directing customers to a separate channel that is not recorded, and more than two-thirds say they manage data requests manually.

Contact centers are, in many cases, the weakest link in the data protection chain. Therefore, risk and compliance awareness must be promoted among customer-facing operational and support staff, without unintentionally leading to compromises on service quality.

Two prerequisites for creating conditions and procedures for compliance are understanding the issues at hand and familiarity with the current regulatory regimes worldwide.

This eBook is intended to provide just such an overview.



NICE

CONTENTS

What is Regulatory Compliance All About?

There are three primary issues related to regulatory compliance in the modern contact center.

- **Consent** – Gathering personal data generally requires the consent of the people whose data is being collected, in accordance with the view (exemplified by the GDPR) that individuals have a right to maintain control over their personal information even after it is shared. This approach is set to become even more widespread in 2023, with the introduction of new legislation in many US jurisdictions (see below). Some companies use a consent management platform (CMP) to handle compliance with relevant consent regulations.
- **Recording and retention** – Many governmental jurisdictions include regulations regarding recording and retention in their data protection legislation, detailing what can, cannot, and must be recorded. Such recordkeeping laws – covering collection, storage, and disposal practices – serve an essential purpose in ensuring people have access to the personal information they share with service providers, on the one hand, and preventing such providers from retaining certain kinds of information, on the other. The United States, Singapore, Brazil and European countries, for example, regulate access to personal data under the rubric of privacy protection. Recording and retention regulations are also instrumental in compelling companies to maintain records that allow for effective auditing. This is especially valuable in the medical and financial services sectors, for example. The larger the enterprise, and the more they serve customers across various lines of business and departments, the more critical compliance-centered recording and retention becomes. For contact centers, this means comprehensive recording tools, long-term data retention capabilities, and sophisticated retrieval mechanisms. Automated interaction recording and data storage procedures can mitigate reputational and regulatory risk, as well as support responsible and effective business conduct.
- **Privacy and security** – Regulations regarding data privacy and security obligate organizations to institute risk and compliance programs, information governance processes, and data access controls to protect the confidentiality and integrity of corporate and consumer data. Among other aspects, regulators assess whether an organization's risk management programs are appropriately resourced, including funding, technology, and staff, and their ability to respond to emerging risks or significant corporate structural changes.

Let's see how these ideas find expression in data protection regulations in different areas of the globe.

NICE

CONTENTS

Europe

GDPR

Member states of the European Union have tackled the issue of data privacy and security head-on and produced the General Data Protection Regulation (GDPR), which has become the model for subsequent legislation worldwide. The GDPR was designed to give people more control over their personal data (which could include a name, ID number, location data, online identifiers such as email addresses and Twitter handles, and specific physical, genetic, mental, economic, cultural, or social information). Another objective of the GDPR is to consolidate the different privacy regulations across European Union member states, to create a clearer legal environment, streamline data sharing and improve business opportunities.

Some key aspects of the GDPR are:

- The collection and processing of personally identifiable information requires "clear and affirmative consent" by the individual. In other words, residents of the EU can choose to, "opt-in", share their information. In the United States, in contrast, the default position has generally been that consumers are willing to share some level of information. In addition, the GDPR protects the right of an individual to transfer personal data that has already been shared to another service provider.
- Recordings of conversations are considered personally identifiable information; therefore, contact centers must secure authorization from consumers before recording an interaction. For the same reason, consumers have the right to request copies of these recordings, as well as other electronic data, in a "commonly used machine-readable format."
- Privacy policies must be explained in clear and understandable language. Moreover, consumers have the right to know when their data has been hacked or unintentionally leaked.
- Very significantly, the GDPR applies to organizations located both in and outside the European Union "if they offer goods or services to, or monitor the behavior of, EU data subjects."

The GDPR also guides how data protection legislation should be interpreted and applied regarding workplace monitoring. While such monitoring is not prohibited categorically, employers are obligated to identify a specific lawful basis for doing so. Employees must provide complete, and accurate information about the monitoring and processing activities and, if there is a high risk to employee privacy, the employer must carry out a data protection impact assessment before they begin monitoring.

The GDPR states explicitly that some violations are more severe than others, with non-compliance fines divided into two tiers. Less severe infringements can result in a fine of €10 million or 2% of a company's annual worldwide revenue from the preceding financial year, whichever is higher. More serious violations can result in a fine of up to €20 million or 4% of a company's annual global revenue from the preceding year, whichever is higher.

NICE

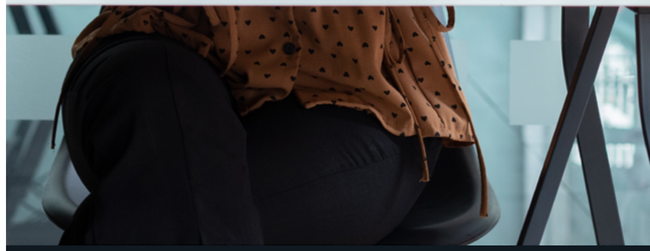
CONTENTS

United Kingdom

Following Brexit, the United Kingdom is no longer bound by European Union regulations such as the GDPR. However, the provisions of the GDPR have been incorporated directly into British data protection law as the UK GDPR, which is complemented by the updated Data Protection Act of 2018 (DPA 2018). In this way, data protection principles, rights, and obligations in the UK post-Brexit are nearly identical to what they were before.

On 28 June 2021, the EU recognized the UK legislation as providing an equivalent level of protection for personal data as the EU's GDPR and its Law Enforcement Directive (for processing personal data "for law enforcement purposes"). This recognition, known as an adequacy decision, is expected to be in effect until June 2025. The combined impact of the UK's legislation and the EU's decisions is that data can continue to flow normally between entities in the UK and the EU.

In October 2022, the UK Information Commissioner's Office (ICO) released draft guidance on workforce monitoring in accordance with the UK GDPR and the DPA 2018. The ICO made it clear in its guidelines that an employer is permitted to monitor workers in principle, but – like the EU's GDPR – there are several conditions that must be met to ensure monitoring activities are compliant.



CONTENTS

North America

USA

Data protection legislation in the United States of America is not uniform. Different states have different laws, and each sector has its approach to data privacy and security.

The legislative approach in the US has been primarily focused on preventing harm, which means that there is not always an across-the-board expectation of privacy regarding personal data. However, a shift is underway. Over 10 states are in the process of implementing new comprehensive and rights-based data protection laws. The California Privacy Rights Act (CPRA) and the Colorado Privacy Act (CPA) came into effect in July 2023 and such laws were already in effect in Connecticut (CTDPA) and Virginia (VCDPA). As of this writing, the Utah Consumer Privacy Act (UCPA) is slated to go into effect by the end of 2023 and the Montana Consumer Data Privacy Act (MCDPA) in October of 2024. The Tennessee Information Protection Act (TIPA) and the Iowa Consumer Data Protection Act (ICDPA) will do so in 2025, and the Indiana Consumer Data Privacy Act (INCDPA) by January 2026. Similar pieces of legislation, the Texas Data Privacy and Security Act (TDPSA) and the Florida Digital Bill of Rights (FDBR), have yet to be signed into law. If they are passed, which is overwhelmingly likely, then they will take legal effect in July 2024.

All the new state laws attempt to standardize the collection and use of consumer's personal information by imposing similar obligations on businesses regarding transparency and privacy notifications, as well as limiting their ability to process certain kinds of data. Companies in those states must also perform data protection assessments for the information they collect and retain. Like the GDPR, the new laws in all five states explicitly protect the individual's control over their personal information, including access, correction, deletion, transfer, and the option to block certain uses.

'Sensitive Personal Data'

While there is some commonality among the newest state laws, there are also distinct differences. The various states all agree that race, ethnic origin, religion, philosophical beliefs, biometric data, and personal health information fall under the rubric of sensitive personal data. On the other hand, the CPA, VCDPA, UCPA and CTDPA, for example, generally adopt the definition of "personal data" and other terms from the GDPR, while the CPRA does not. Yet, California has adopted the broadest definition of all, including items that no other state does, such as ID numbers (SSN, passport, etc.), account and credit card numbers, union membership, and email texts. Virginia and Colorado, on the other end of the scale, use the most limited definition of all the states on our list.

Enforcement and Penalties

Some of the latest state data privacy laws required the establishment of new enforcement agencies or the extension of existing regulatory powers. The CPRA,

NICE

CONTENTS

for example, creates the California Privacy Protection Agency, while VCDPA grants enforcement authority to the Attorney General and the UCPA authorizes the Utah Department of Commerce Division to investigate compliance issues raised by consumers.

Most of the US state data privacy laws do not include a provision providing a private right of action, although a civilian complaint may trigger an investigation. On the other hand, the CPRA allows private individuals to initiate legal action in response to data breaches that compromised their personal data such as a username and password, for example. Similarly, the California regulations apply only to for-profit businesses, while the other states affirmatively name specific exemptions (such as government agencies and educational institutions, depending on the state).

Penalties for violating the various laws differ according to state. Utah and Connecticut, for example, impose a fine of $5,000 per violation; however, Iowa and Utah allow the organization a grace period of 90 and 30 days, respectively, to correct the breach of data privacy. Montana's 60-day cure period provision, on the other hand, will terminate on April 1, 2026. The California law is among the most strict out of the gate, as it allows no grace period to correct reported breaches and a fine of up to $7,500 for each violation. According to the Colorado Privacy Act, meanwhile, if you fail to take action during the 60-day cure period, then you can face a whopping fine of up to $20,000 per violation. Tennessee will triple fines for willful or knowing violations of the law, while Colorado caps possible penalties at $500,000.

The IAPP Westin Research Center tracks proposed and enacted privacy bills from across the US. This convenient chart, part of a report* released by the IAPP on June 19, 2023, presents key features of some recent state laws:

US State Privacy Legislation Tracker **2023**

Comprehensive Consumer Privacy Bills

STATE	LEGISLATIVE PROCESS	STATUTE/BILL (HYPERLINKS)	COMMON NAME	CONSUMER RIGHTS: Right to access	Right to correct	Right to delete	Right to opt out of certain processing	Right to portability	Right to opt out of sales	Right to opt in for sensitive data processing	Right against automated decision making	Private right of action	BUSINESS OBLIGATIONS: Opt-in default requirement age	Notice/transparency requirement	Risk assessments	Prohibition on discrimination (exercising rights)	Purpose processing limitation
LAWS SIGNED (TO DATE)																	
California		CCPA	California Consumer Privacy Act (2018; effective Jan. 1, 2020)	X		X		X	X			L	16	X			X
		Proposition 24	California Privacy Rights Act (2020; fully operative Jan. 1, 2023)	X	X	X	S	X	X		X	L	16	X	X	X	X
Colorado		SB 190	Colorado Privacy Act (2021; effective July 1, 2023)	X	X	X	P	X	X	X	X	-	13	X	X	X	X
Connecticut		SB 6	Connecticut Data Privacy Act (2022; effective July 1, 2023)	X	X	X	P	X	X	X	X	-	13	X	X	X	X
Indiana		SB 0005	Indiana Consumer Data Protection Act (2023; effective Jan. 1, 2026)	X	X	X	P	X	X	X	X	-	13	X	X	X	X
Iowa		SF 262	Iowa Consumer Data Protection Act (2023; effective Jan. 1, 2025)	X		X		X	X		X	-	13	X		X	X
Montana		SB 384	Montana Consumer Data Privacy Act (2023; effective Oct. 1, 2024)	X	X	X	P	X	X	X	X	-	13	X	X	X	X
Tennessee		HB 1181	Tennessee Information Protection Act (2023; effective July 1, 2024)	X	X	X	P	X	X	X	X	-	13	X	X	X	X
Texas		HB 4	Texas Data Privacy and Security Act (2023; effective Jan. 1, 2024)	X	X	X	P	X	X	X	X	-	13	X	X	X	X
Utah		SB 227	Utah Consumer Privacy Act (2022; effective Dec. 31, 2023)	X		X	P	X	X				13	X		X	
Virginia		SB 1392	Virginia Consumer Data Protection Act (2021; effective Jan. 1, 2023)	X	X	X	P	X	X	X	X	-	13	X	X	X	X

Consent Laws

Contact centers need to pay special attention to the various consent laws across all US states for the purpose of recording interactions. Federal law and most states only require one party to a conversation to give consent for recording, meaning that the contact center agent, for example, is legally permitted to hit the record button without informing the customer. Eleven states (California, Delaware, Florida, Illinois, Maryland, Massachusetts, Montana, Nevada, New Hampshire, Pennsylvania, and Washington), on the other hand, require all-party consent. This imposes an important and critical obligation on frontline agents to obtain consent during customer interactions or risk compliance violations.

NICE

CONTENTS

Adding to the patchwork quilt of recording laws is the fact that some states require consent to be explicitly stated. In contrast, other states accept implied consent based on behavior or location. Similarly, some legislation only mandates consent when those involved in a conversation have a "reasonable expectation of privacy." In other words, privacy may be expected inside an individual's home, but not in a public place like a coffee shop.

As for data collection, all the new state laws allow people to opt-out at any time and demand that their personal information (as defined in each state) not be captured by a particular company. Most have an opt-in clause, which requires businesses to obtain consent from individuals before collecting sensitive personal information (or information on known children). Some states also require businesses to recognize and respect automated opt-out preference signals (global privacy controls, such a browser settings and the like).

Employee Rights

In general, companies can only collect the personal data of employees if it is necessary and relevant to their job. And that was generally the extent of the protection offered in the past, with some companies obligated to issue notices that they were using the data and employees having a limited right to private action in the event of a data breach.

Recently, some global and US legislation has extended consumer data privacy rights to include employees. According to CPRA, for example, companies are now required to provide employees with the right to access, correct, and delete any personal data held by their employer. Employees also have the right to opt-out of sales or sharing, to limit the use and disclosure of sensitive personal information, and to not be retaliated against for exercising the other rights.

Federal Law and International Agreements

While there is no federal law governing online privacy in the United States, a new bill – the American Data Privacy and Protection Act, H.R. 8152 (ADPPA) – passed through the House Energy and Commerce Committee nearly without opposition in July 2022. According to the congressional notes on the ADPPA, the proposed law establishes requirements. It imposes limitations on organizations that handle any information "that identifies or is reasonably linkable to an individual." It includes provisions that protect an individual's right to access, correct, delete and control the transfer of their personal data, as well as to opt out of targeted advertising. The bill would also obligate companies to implement security practices to protect and secure personal data against unauthorized access, giving the Federal Trade Commission (FTC) the authority to issue regulations and enforce compliance. Four years after the law takes effect, individuals would be allowed to bring civil actions for compliance violations.

The relationship between US and European data protection laws is established in the EU-US Data Privacy Framework, which is intended to protect personal information transferred from Europe that is essentially equivalent to the protection it receives under the GDPR. On 7 October 2022, US President Joe Biden signed an executive order that outlines the steps the US will take to implement its commitments under the terms of the agreement.

NICE

CONTENTS

Canada

The Personal Information Protection and Electronic Documents Act (PIPEDA) is Canada's federal private sector privacy law. PIPEDA applies to all organizations operating in Canada that collect, use, or disclose personal information in the course of their commercial activity, including across provincial or national borders.

PIPEDA strictly limits the collection, use, and retention of personal information to what is needed for specific purposes defined by the company, unless the individual whose data is being collected explicitly consents otherwise. In any event, personal information cannot be obtained, used or disclosed without prior "meaningful consent." To that end, the purpose of collecting the data and ways how it will be processed must be transparent and clearly communicated. In addition, any personal information retained must be accurate, complete, and up-to-date.

Consent is also required in most cases for recording a phone call, such as at a contact center. This can be accomplished in a variety of ways, but for it to be considered valid (i.e., "meaningful"), the organization would have to inform the customer of their privacy practices in a comprehensive and understandable manner. In any case, however, organizations can only record a call for purposes that a reasonable person would consider appropriate under the circumstances.

The fines for noncompliance with PIPEDA regulations can be up to CAD $100,000.

The Canadian government proposed a new private sector privacy law, the Consumer Privacy Protection Act (CPPA), tabled as Bill C-27 in 2022. The bill proposes strengthening consumer privacy protections and adding more federal government enforcement powers. In April 2023, Bill C-27 passed its second reading in the House of Commons and has been sent to the Industry and Technology Committee for further detailed examination.

NICE

CONTENTS

Asia

Japan

The Personal Information Protection Commission, a central agency, acts as the supervisory governmental organization on issues of privacy protection. In 2022, the Amended Act on Protection of Personal Information (AAPPI) came into effect in Japan. The legislation regulates the privacy and data protection activities of a "personal information handling business operator," defined as any business that provides a personal information database for commercial use. Notably, such a business does not need to directly operate in Japan to fall within the scope of the AAPPI.

While the AAPPI does not mandate that businesses proactively publicize how they are using collected data, they are obligated to reply to consumer requests regarding the purpose of collecting their personal information, how they can access, correct or withhold it, and where they can submit complaints. Individuals can also request to receive the collected data in digital and hardcopy format. If a business fails to reply to any AAPPI-based request within two weeks, then the individual making the request can initiate a civil suit against them.

In order to transfer personal data outside of Japan, businesses must proactively seek consent from the individual whose data is to be shared or establish a personal information protection system with the recipient in the foreign jurisdiction. For the opt-in to be effective, the business must provide the data subject clear and accessible information on the transfer for their review.

The AAPPI notes that a business transferring anonymized personal information does not need to follow the same strict processing rules (such as user consent), although they are obligated to publicly acknowledge that the data is anonymized. Another category is "pseudonymously processed" data, which is information that relates to an individual but cannot be linked to them without additional data. Pseudonymously processed information can be used for a purpose other than the originally stated reason for handling it, access and correction rights do not apply, and it can be retained in perpetuity.

In 2019, the revised Japanese law became the first foreign legislation to be recognized by the European Union as providing an equivalent level of protection for personal data as the EU's GDPR. This adequacy decision governs cross-border data transfers from the EU to Japan.

NICE

CONTENTS

India

The Information Technology (IT) Act (2000) mandates that commercial or professional organizations handling sensitive personal information implement and maintain reasonable security practices and procedures. While this legislation does not specifically define what constitutes "reasonable" measures, the Sensitive Personal Data or Information (SPDI) Rules drafted under the auspices of the IT Act specify minimum standards of protection for sensitive personal data, including: passwords; financial information; physical, physiological and mental health conditions; sexual orientation; medical records and history; and biometric information.

The Indian law requires consent for processing personal data; however, how, when and through which means that consent is obtained and recognized is not clearly defined. Businesses therefore commonly rely on general principles of contract law in daily practice. In addition, the IT Act requires all companies that process personal data to display on their websites a notice regarding the types of data they collect and for what purposes, any disclosure practices, descriptions of their security safeguards, and other data processing activities.

While the SPDI Rules state that businesses should not retain information and recordings for longer than required, they do not specify a fixed period. The current general practice is to retain data for as long as a cause of action pursuant to the IT Act could theoretically arise. Similarly, individuals have no express right of erasure under the SPDI Rules. However, they do have a right to withdraw consent for processing their personal data, and a recent market trend is to bundle an implied right to erasure within such a withdrawal.

Another consent requirement of significant importance to contact centers in India was recognized by the Delhi High Court in 2022. The court stated that monitoring phone lines or recording calls without the consent of those involved in the interaction constitutes a breach of privacy under Section 21 of the Indian Constitution. Therefore, compliance would require such activity to be carried out in a contact center only with the customer's consent.

Noncompliance with the IT Act can lead to damages being awarded for any loss caused by negligence in protecting an individual's personal information. The IT Act also prescribes criminal penalties that include both imprisonment of up to three years and fines for the disclosure of personal information without consent, in the event that such disclosure is a breach of contract or results in wrongful loss or gain.

NICE

CONTENTS

Hong Kong

In Hong Kong, although officially part of the People's Republic of China, data protection is regulated by the Personal Data (Privacy) Ordinance (the PDPO) passed in 1995, before the area's transfer to Chinese sovereignty. The PDPO is one of Asia's longest-standing comprehensive data protection laws and went through significant amendments in 2012 and 2021, including the introduction of provisions regarding direct marketing, new technology privacy challenges, doxing, and other public concerns.

The PDPO, which applies to activity in both the private and the public sectors, is technology-neutral and lays down a series of general principles. These Data Protection Principles (DPPs) – outlining how data users should collect, handle and use personal data – can be summarized as follows:

- DPP1 provides that personal data shall only be collected for a lawful purpose directly related to a function or activity of the organization. The data collected should be necessary and adequate, but not excessive, for such purpose. The means of collection should be lawful and fair.
- DPP2 requires organizations collecting and using personal information to take all practicable steps to ensure that the data is accurate and is not retained longer than is necessary for the fulfillment of the purpose for which it was collected.
- DPP3 prohibits the use of personal data for any purposes other than those originally stated when collecting the data, unless the individual data subject provides express and voluntary consent. The individual whose data has been collected can withdraw previously given consent by written notice.
- DPP4 requires that organizations take all practicable steps to protect the personal data they collect and retain against unauthorized or accidental access, processing, erasure, loss or use.
- DPP5 obliges organizations to take all practicable steps to ensure their personal data policies and practices are transparent, including the kind of data they hold and the main purposes for holding it.
- DPP6 provides individuals with the right to request access to and correction of their data. An organization may refuse such a request, but only if they can provide an acceptable justification.

The six DPPs of the PDPO, complemented by other provisions, set out the basic compliance requirements for handling personal data. Employers must also ensure they do not contravene the DPPs while monitoring employee activities.

Regarding recording conversations, Chinese law allows such activity on condition that all parties involved have given their consent. Such consent must be given explicitly and not implied.

Hong Kong's Office of the Privacy Commissioner for Personal Data (PCPD) is authorized to issue enforcement notices for contraventions of the six DPPs. Although noncompliance with one of the DPPs does not officially constitute an offense, disregarding a PCPD enforcement notice does.

Notably, the PDPO applies to foreign organizations with offices or operations in Hong Kong. For example, if a foreign company has a subsidiary in Hong Kong, the subsidiary will be responsible for the personal data that it controls, and it must ensure adherence to PDPO directives even if the data is immediately transferred to the foreign parent company for processing.

NICE

CONTENTS

Oceania

Australia

Australia's Privacy Act of 1988 (Privacy Act) governs individual data privacy in the country and regulates how government agencies and major private organizations handle personal information. The Privacy Act includes 13 Australian Privacy Principles (APPs), which are technology-neutral standards, rights, and obligations regarding: the collection, use, and disclosure of personal information; an organization's governance and accountability; the integrity and correction of personal information; and the rights of individuals to access their own information.

The Privacy Act provides Australians control over the way their personal information is handled, including the right to:

- Know why personal information is being collected, how it will be used, and to whom it will be disclosed;
- Access one's personal information (including health information);
- Request that inaccurate personal information be corrected.
- File a complaint about an organization or agency that has mishandled personal information.
- Refuse to identify oneself or to use a pseudonym.
- Stop receiving unwanted direct marketing.

Contact centers in Australia are bound by the terms of the Telecommunications Interception and Access Act of 1979, making it an offense to listen to most live phone calls or call recordings without the permission of those involved. In most cases, therefore, contact centers can only record calls if the customer has given their consent. A statement or automated message delivered up front saying that a conversation will be recorded qualifies as requesting consent under Australian law, as the other party could disconnect the call or request an unmonitored communication channel.

On 26 October 2022, the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 was tabled in Parliament by Australia's Attorney-General, Mark Dreyfus. Once passed, the bill will amend: the Australian Communications and Media Authority Act 2005 to enable disclosure of certain information to non-corporate Commonwealth law enforcement entities; the Privacy Act 1988 to expand the Australian Information Commissioner's enforcement and information sharing powers, and increase penalties for serious or repeated privacy interference; and the Australian Information Commissioner Act 2010 to allow the Australian Information Commissioner to delegate certain functions or powers.

NICE

CONTENTS

New Zealand

The key legislation in New Zealand about data protection is the Privacy Act 2020 (the 2020 Act). This legislation is relatively new, receiving Royal Assent on 30 June 2020. Among its stipulations:

- "Personal information" is defined as information about an identifiable individual.
- An organization is required to consider whether the data in question is "sensitive" when assessing the likelihood of serious harm being caused by a privacy breach; however, the 2020 Act does not expressly define "sensitive data."
- Unlike many other privacy laws, consent is not a prerequisite for collecting and using personal data. This is on condition that the organization lawfully collected the information, is only doing what it intended to do with it at the time of collection, and is transparent about how it is being used.
- An organization, such as a contact center, must appoint an internal or external "privacy officer" who is responsible for overseeing and ensuring privacy regulation compliance.

Regarding the recording of conversations, slightly different laws apply in different Australian states and territories. Generally, however, the consent of all parties involved is required to legally record an interaction. Therefore, call centers will need to obtain customer consent to be monitored and recorded, whether for inbound or outbound calls, which provides them the option to hang up or request an alternate non-recorded communication channel. Notably, Queensland is an exception to the general rule, with a limited one-party consent requirement for recording private conversations.

NICE

The AI Behind Better Connections

About NICE

With NICE (Nasdaq: NICE), it's never been easier for organizations of all sizes around the globe to create extraordinary customer experiences while meeting key business metrics. Featuring the world's #1 cloud native customer experience platform, CXone, NICE is a worldwide leader in AI-powered self-service and agent-assisted CX software for the contact center – and beyond. Over 25,000 organizations in more than 150 countries, including over 85 of the Fortune 100 companies, partner with NICE to transform – and elevate – every customer interaction.

www.nice.com