COVESTIC
A MILESTONE COMPANY

Privacy Laws, Consumer Rights and The ServiceNow Solution

servicenow
Partner
Elite

Table of Contents

Introduction

A concern for privacy is sweeping the globe. To address it, many countries around the world and states within the U.S. have enacted laws designed to protect the privacy of their constituents. While these laws often differ in scope, they share a common purpose – to grant people more power over and transparency into how their personal information is collected, processed and shared. Organizations that fail to comply with these laws are held accountable by governmental authorities via judicial action, the imposition of fines and penalties and, in many cases, by enabling citizens to bring private rights of action against organizations that fail to comply with the laws or to honor the rights granted to them under the law.

In this eBook, the Covestic Governance, Risk and Compliance team outlines these privacy rights, provides an at-a-glance look at recently passed U.S. privacy laws and explains how Covestic can help leverage your investment in ServiceNow to ensure your organization achieves and remains continually compliant with these laws.

Ten Rights Commonly Granted by Domestic and International Privacy Laws

While privacy laws differ in scope and jurisdiction, most share a common objective – to give their citizens greater control over their personal data. They do this by granting them specific rights. Here is a synopsis of the top 10 privacy rights frequently enacted in the various privacy laws.

1

Right to Be Informed

Individuals have the ***right to know whether*** their data is being collected, retained and shared.

2

Right to Access

Individuals have the ***right to know what*** data is being collected, how it is being used and with whom, if anyone, it is being shared.

3

Right to Rectification

Individuals have the ***right to correct*** inaccuracies, complete incomplete information and update outdated information to ensure retained data is current, correct and complete.

4

Right to Deletion

Individuals have the ***right to have their data deleted***. This right is also known as the 'right to erasure' and the 'right to be forgotten.'

5

Right to Restriction

Individuals have the ***right to limit processing*** of some or all their personal information permanently or temporarily without requesting their data be deleted.

6

Right to Data Portability

Individuals have the ***right to obtain a portable copy*** of their data, typically for free and in a format that is human-readable as well as machine-portable.

Ten Rights Commonly Granted by Domestic and International Privacy Laws (Cont'd)

7 Right to Opt-Out

Individuals have the ***right to say "No"*** to the selling of their personal information to third parties.

8 Right to Non-Discrimination

Individuals have the ***right to equal treatment*** (and to not be 'penalized') when they exercise a right (e.g., opting out).

9 Right to Sue

Individuals have the ***right to seek civil damages*** (via private or class actions) against covered businesses for violation of a statute (e.g., a data-breach resulting from adequately protecting their data).

10 Right to Non-automated Decision Making

Individuals have the ***right to human input*** in decisions about them (e.g., credit approval) to ensure decisions are not based solely on automated processes.

Understanding these rights, as well as their intent, is essential to designing and building a compliance program that not only honors your customers' rights, but also demonstrates your organization's commitment to protecting their privacy.

Three International Privacy Laws

Countries around the world have enacted their own privacy laws. Here are three you need to be aware of if you are doing business in these major international markets – the European Union (EU), South America and Japan.

European Union

The General Data Protection Regulation (GDPR) led the way in international privacy protection and is undoubtedly the toughest privacy law in the world. It applies to any organization located anywhere that processes the personal data of citizens of the EU. It grants all the rights discussed above and imposes extremely stiff fines — as high as 4% of an organization's gross annual revenue or $20 Million Euros – for non-compliance. Since the law went into effect, the European courts have vigorously enforced the law, levying millions of dollars in fines.

> **Did you know that Europe's highest court recent struck down the EU-US Privacy Shield Framework?** Read more in our blog →

South America

The Lei Geral de Proteçao de Dados (LGPD) is Brazil's general data protection regulation. It is nearly identical to the GDPR in terms of scope, jurisdiction and penalties and provides for fines up to 50 million BRL (approximately $10 Million USD) for violations.

Japan

Japan's Act on Protection of Personal Information (APPI) applies to both foreign and domestic companies that process the data of Japanese citizens. While similar to the GDPR, it differs enough that Japan and the EU has entered into a reciprocity agreement where companies from each country are deemed to have established privacy protections that adequately meet the requirements of the other country. Data subjects in either country can seek recourse for violation of their rights by the business in the other country.

South Korea, Thailand and many other countries have similar laws so if you sell products or services in these countries, you need to make sure you are intimately familiar with their privacy protection laws.

Three U.S. Privacy Laws

The United States does not yet have a comprehensive privacy law like other countries. Instead, privacy is protected by federal sectoral laws, such as the Fair Credit Reporting Act for consumer credit information, the Health Insurance Portability and Accountability Act (HIPAA) for patient medical-related information, and the Gramm-Leach-Bliley Act (GLBA) for financial information. For consumers, privacy protection falls to the individual states.

In 2018, California led the way in consumer privacy legislation, passing the California Consumer Privacy Act (CCPA). Two other states – Nevada and Maine – were quick to follow, while dozens of other states have similar bills working their way

The California Consumer Privacy Act (CCPA)

The CCPA went into effect on January 1 of this year and became enforceable on July 1, 2020. It grants California residents the right to know what information a company has collected on them, the right to request that their personal data be deleted and the right to "say no" to the selling/sharing of their personal information (aka, the right to "opt-out"). The law applies to most businesses that sell services or products to California residents, regardless of where the business is located. It also grants citizens the right to sue in the event of a data breach. The CCPA is the most stringent consumer privacy law in the United States and is replete with requirements.

> Check out our on-demand webinar to learn how you can leverage your investment in ServiceNow to meet the requirements of the CCPA. Watch the recording →

The Nevada Online Privacy Law (SB220)

The Nevada Privacy Law, enacted in May 2019, requires businesses to offer consumers an opportunity to opt-out of the selling of their personal information. It does not grant them the right to know what data has been collected or the right to request that their data be deleted. The Nevada law also defines "selling" and "personal information" much more narrowly than the CCPA. If your organization is doing business in Nevada and it is already CCPA compliant, it may already be SB220 compliant since most of the requirements of the Nevada law can also be found in the CCPA.

Three U.S. Privacy Laws (Cont'd)

The Maine Act to Protect the Privacy of Online Consumer Information (LD946)

Signed into law in June 2019, the Maine privacy law prohibits internet providers from using, selling, distributing or allowing access to a customer's personal information without the express consent of the customer. This requirement to obtain the consumer's permission beforehand is much more stringent than the CCPA. It puts the burden of obtaining consent on the business that collects and uses the data rather than on the consumer. The Maine law also defines a 'customer' as well as 'personal information' much more narrowly than the CCPA. Perhaps the biggest difference is that the Maine law is only applicable to broadband service providers operating within the state. However, if your business is covered by the Maine law, be aware that failures to comply carry harsh penalties – up to up to $500,000 or 5% of annual revenues maximum for willful non-compliance.

If your organization does business in any of these states, you need to ensure that your organization has the proper safeguards in place to ensure compliance with their laws. But, to future-proof and fortify your privacy program, you also need to keep an eye on the bills that are still working their way through their respective state legislatures. Below are some of the states that are still processing or considering privacy legislation:

- Arizona HB2729
- Connecticut RB1108
- Hawaii HCR225
- Illinois HB5603, Consumer Privacy Act
- Louisiana HR249
- Maryland HB784, Online Consumer Protection Act
- Massachusetts S120
- Minnesota HF3936, Minnesota Consumer Data Privacy Act
- Nebraska LB746, Nebraska Consumer Data Privacy Act
- New Hampshire HB1680
- New Jersey A3255
- New York S5642, Privacy Act
- North Dakota HB1485
- South Carolina
- Texas HB4390
- Washington State SB6281

How ServiceNow Can Accelerate Your Time to Compliance

ServiceNow provides a robust set of tightly integrated capabilities that can be used to rapidly implement a highly-efficient and effective privacy compliance program. Here's a look at a few areas of the platform that can help you meet various privacy law requirements:

ServiceNow Customer Service Management (CSM):

The CSM application can be leveraged to enable consumers to exercise their rights. The application is designed from the ground up to support external customers, allowing them to submit 'cases' – via a CSM portal – that can be routed for resolution to the appropriate customer service agent

Learn More →

ServiceNow Security Operations Management (SOM):

The SOM suite of applications provides a structured response engine that uses intelligent workflows, automation and a deep connection with IT to quickly identify and resolve incidents. The security incident response application pulls data from your existing security tools, coordinates it with threat data pulled from industry databases and trusted security circles to prioritize incidents based on impact.

Learn More →

ServiceNow Governance, Risk and Compliance (GRC):

The GRC ServiceNow Policy & Compliance Management application provides a centralized process for creating and managing policies, standards and internal control procedures that are cross-mapped to external regulations and best practices. In addition, the capabilities provided by the GRC Vendor Risk Management application can be leveraged to ensure your vendors and any third-parties with whom you share consumer information have processes in place to respond to opt-out and delete requests from your consumers.

Learn More →

ServiceNow Orchestration:

The ServiceNow Orchestration module extends the workflow engine to processes outside of a ServiceNow instance. It allows you to automate tasks that run on remote services, servers, applications and hardware.

How Covestic Can Accelerate Your Time to Value

At Covestic, our Governance, Risk, and Compliance (GRC) team is well-versed in consumer privacy and data protection requirements. Whether your organization needs to comply with CCPA, GDPR, or any of the myriad of other privacy regulations, we have both the regulatory compliance expertise and deep ServiceNow platform experience needed to ensure your compliance program is not only effective but also highly-efficient and scalable. With Covestic on your team, we can help you:

- Translate legal requirements into ServiceNow implementation requirements (stories).
- Understand how best to leverage your instance of ServiceNow to implement those stories.
- Minimize your time to compliance and time to value.
- Ensure your solution is effective, efficient and scalable.
- Minimize the ongoing cost of compliance and the day-to-day burden of compliance on your staff.

Contact our team to learn more about how we can help you leverage your investment in ServiceNow to achieve your privacy regulatory compliance goals.

CONTACT US →

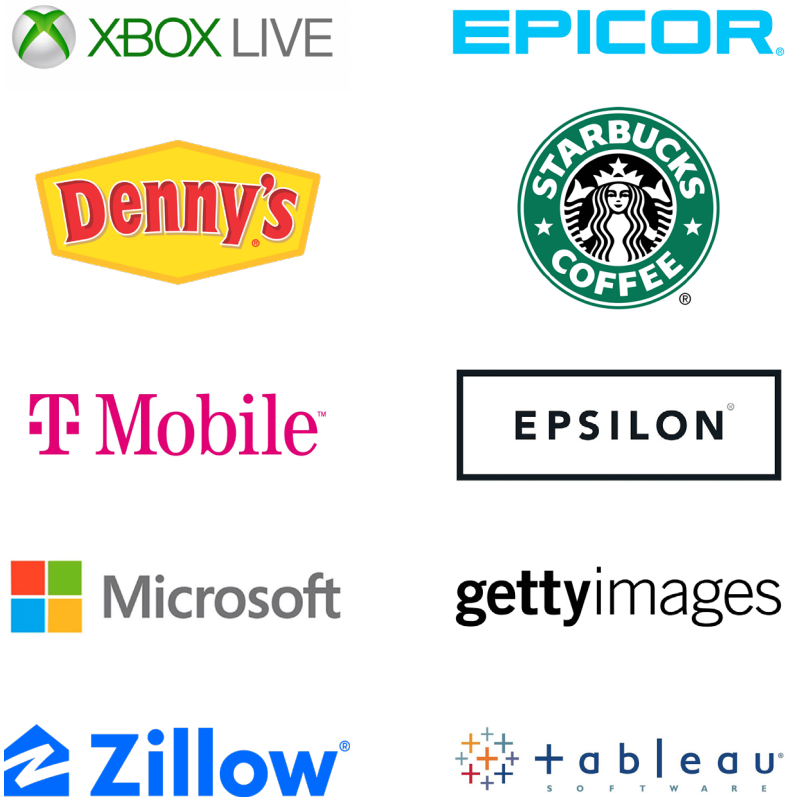
About Covestic

We deliver practical IT services and solutions that optimize the value technology brings to business.

Covestic is a world-class consulting practice that implements technology solutions to help clients realize greater value from their technology investments, so they can rapidly scale and grow their business, provide superior customer experiences and trust that their valuable data and technology assets are protected and secure.

- ServiceNow Consulting
- IT Operations Managed Services
- Staffing & Project Delivery

Our Clients



Contact Covestic

5555 Lakeview Drive Suite 100

Kirkland, WA 98003

E: info@covestic.com

T: 425.803.9889

W: www.covestic.com