

**Privacy Regulation Roundup – December 2023**

This Privacy Regulation Roundup summarizes the latest major global privacy regulatory developments, announcements, and changes. This report is updated monthly. For each relevant regulatory activity, you can find actionable Info-Tech analyst insights and links to useful Info-Tech research that can assist you with becoming compliant.

Contents

[Québec DPA Issues Guidelines for Obtaining Valid Consent 3](#_Toc152866955)

[Type: Announcement 3](#_Toc152866956)

[Announcement Date: October 31, 2023 3](#_Toc152866957)

[Colorado AG Publishes Shortlist of Opt-out Mechanisms 4](#_Toc152866958)

[Type: Regulation 4](#_Toc152866959)

[Announcement Date: October, 2023 4](#_Toc152866960)

[US Lawmakers draw on AI and Privacy Correlation for a Federal Privacy Legislation 6](#_Toc152866961)

[Type: Op-Ed 6](#_Toc152866962)

[Announcement Date: November 6, 2023 6](#_Toc152866963)

[German DPA AssessES Legal Aspect of Data Protection for AI Systems 7](#_Toc152866964)

[Type: Announcement 7](#_Toc152866965)

[Announcement Date: November 11, 2023 7](#_Toc152866966)

[China’s Pursuit of Data Sovereignty: Impact on International Audit Firms 8](#_Toc152866967)

[Type: Announcement 8](#_Toc152866968)

[Announcement Date: November 15, 2023 8](#_Toc152866969)

# Québec DPA Issues Guidelines for Obtaining Valid Consent

## Type: Announcement

## Announcement Date: October 31, 2023

**Summary:** The Commission d’accès à l’information du Québec, the provincial data protection authority, adopted the final version of its guidelines for organizations to obtain valid consent to process personal data. The Commission developed the document in the context of Law 25, which enhances the privacy obligations of organizations.

Law 25 was adopted by the Québec government on September 21, 2021. The final phase of the new legislation came into effect on September 22, 2023. The right to data portability will become effective in September 2024. Under the new law, organizations must obtain free and informed consent to process personal data, consent must be given for specific purposes, and it must be obtained using clear and simple language. Organizations must also seek express consent to use sensitive personal information.

The provisions include transparency requirements. Organizations must ensure individuals understand how they will use and communicate the information and possibly share it with third parties. They must also inform the individual why they collect the information and how and explain their rights of access, correction, and withdrawing of consent to use the information organizations collect.

**Analyst Perspective:** The revised guidelines are based on the principle of transparency and aim to give more rights to individuals who share personal information. Consent requirements must be met not only for customers and prospects but also for employees and job applicants. The details of the law are broadly consistent with existing privacy frameworks, including the GDPR. Organizations processing personal data should put in place a consent management strategy that identifies the business need to process personal data, specifies its intended purpose, and identifies requirements for consent management consistent with Law 25. These measures are part and parcel of a sound data privacy program, one that ensures consent from existing and future customers is valid, maintains the trust of stakeholders, and reduces the reputational risks that arise from poor management.

**Analyst:** [Michel Hebert](https://www.infotech.com/profiles/michel-hebert), Principal Research Director – Security & Privacy

**More Reading:**

* Source Material:
* [Quebec Bill 25, An Act to Modernize Privacy Legislation | Capital Hill Group](https://capitalhillgroup.ca/quebec-bill-25-an-act-to-modernize-privacy-legislation/)
* [Is your business ready for Quebec’s data protection legislation? | Copibec](https://www.copibec.ca/en/nouvelle/459/loi-25-et-protection-des-donnees-votre-entreprise-est-elle-prete-)
* [Data protection in Québec: Act 25 and consent | KPMG](https://kpmg.com/ca/en/home/insights/2023/05/data-protection-in-quebec-act-25-and-consent.html)
* [Guideline Document on Criteria for the Validity of Consent | Commission d’accès à l’information du Québec](https://www.cai.gouv.qc.ca/criteres-de-validite-du-consentement-la-commission-adopte-ses-lignes-directrices/)
* Related Info-Tech Research:
* [*Mature Your Privacy Operations*](https://www.infotech.com/research/ss/mature-your-privacy-operations)
* [*Build a Data Privacy Program*](https://www.infotech.com/research/ss/build-a-data-privacy-program)

# Colorado AG Publishes Shortlist of Opt-Out Mechanisms

## Type: Regulation

## Announcement Date: October 2023

**Summary:** The Colorado Privacy Act (CPA) has been in effect since July 2023 and companies subject to its provisions continue to face critical compliance obligations. Specifically, organizations that engage in targeted advertising or sell personal data must adhere to an impending CPA requirement, effective July 1, 2024. As mandated by Colorado Revised Statutes, controllers under the CPA must honor Colorado consumers’ requests to opt out of targeted advertising or the sale of personal data. These opt-out requests must be facilitated through a “user-selected universal opt-out mechanism” that conforms to technical specifications established by the Attorney General. CPA Rules 5.06 and 5.07 further elaborate on these technical specifications and minimum standards, designating the Attorney General’s office with maintaining a public registry of compliant mechanisms.

On November 21, 2023, the Colorado Attorney General released a Universal Opt-Out Shortlist, presenting three potential universal opt-out mechanisms for potential formal recognition; public feedback on each mechanism was solicited:

* 1. The Global Privacy Control
  2. The OptOutCode
  3. The Opt-Out Machine

The CPA empowers Colorado consumers with the right to opt out of the processing of their personal data for targeted advertising and the sale of their personal data. This opt-out mechanism empowers consumers to exercise control over the utilization of their personal information.

The CPA provides two modalities for consumers to exercise their opt-out rights:

* 1. Active method
  2. Passive method

The active method entails the consumer actively engaging with the controller’s designated opt-out mechanism, typically presented as a clear and conspicuous option. In contrast, the passive method involves the consumer employing a browser extension or using browser settings to transmit standardized opt-out signals to the controller’s website. These signals, recognized as universal opt-out mechanisms, inform the controller of the consumer’s preference to opt out of data processing for targeted advertising or data sales. For universal opt-out mechanisms to function effectively, controllers must configure their websites to detect and respond to these signals. The CPA Rules emphasize the purpose of universal opt-out mechanisms, which is to provide consumers with a straightforward and user-friendly means to automatically exercise their opt-out rights across multiple controllers without the need for individualized requests.

The CPA, in its current form, mandates controllers to offer an active opt-out mechanism and adhere to opt-out requests received through this channel. While the law permits controllers to recognize passive opt-out requests conveyed via universal opt-out mechanisms, it does not impose a legal obligation. If a controller decides to respond to passive opt-out requests, the onus falls on the controller to verify the authenticity of the opt-out signal against technical specifications and subsequently configure its website to adhere to the consumer's preference.

Starting July 1, 2024, businesses in Colorado will be required to honor opt-out requests made through universal opt-out mechanisms that have been approved by the Colorado AG. To make it easier for businesses to comply with this new requirement, the AG will publish a list of approved universal opt-out mechanisms by January 1, 2024. Businesses can start using these approved mechanisms as soon as they are available.

**Analyst Perspective:** Businesses covered by the Colorado Privacy Act should review their practices to make sure they can recognize and respond to these approved opt-out mechanisms. The Attorney General is currently evaluating different opt-out mechanisms to ensure they meet the requirements of the Colorado Privacy Act. A final list of approved opt-out mechanisms will be published by January 1, 2024, before the law goes into effect on July 1, 2024.

**Analyst:** [Carlos Rivera](https://www.infotech.com/profiles/carlos-rivera), Principal Advisory Director – Security, Privacy, Risk & Compliance

**More Reading:**

* Source Material:
  + [Universal Opt-Out Shortlist | Colorado Attorney General](https://coag.gov/uoom/)
  + [Colorado attorney general publishes viable opt-out mechanisms | IAPP](https://iapp.org/news/a/colorado-attorney-general-publishes-viable-opt-out-mechanisms/)
  + [Colorado Publishes Universal Opt-Out Mechanism Shortlist | CyberAdviser](https://www.cyberadviserblog.com/2023/11/colorado-publishes-universal-opt-out-mechanism-shortlist/)
  + [Colorado AG Publishes Shortlist of Universal Opt-Out Mechanisms | Alston & Bird Privacy, Cyber & Data Strategy Blog](https://www.alstonprivacy.com/colorado-ag-publishes-shortlist-of-universal-opt-out-mechanisms/)
* Related Info-Tech Research:
  + [*Build a Data Privacy Program*](https://www.infotech.com/research/ss/build-a-data-privacy-program)
  + [*Mature Your Privacy Operations*](https://www.infotech.com/research/ss/mature-your-privacy-operations)

# US Lawmakers Draw on AI and Privacy Correlation for a Federal Privacy Legislation

## Type: Op-Ed

## Announcement Date: November 6, 2023

**Summary:** Representatives in the United States House Committee on Energy and Commerce have urged Congress to pass new comprehensive privacy legislation for artificial intelligence (AI). This is to help address the risks of AI as it relates to consumer privacy protections. While many states have passed their own privacy regulations, in the past year alone, these individual state laws differ widely. While there has been some positive momentum regarding a comprehensive privacy approach, a federal law for nationwide privacy legislation has not been passed yet. Now, with the inclusion of AI becoming more prevalent in various industries and business environments across the world, US lawmakers are indicating that the time is right for such legislation. This would form a balanced and foundational approach to privacy and ensure that there are comprehensive protections for the collection, processing, transfer, and storage of consumer data.

US House Representatives Cathy McMorris Rodgers and Jay Obernolte jointly penned a recent opinion piece in Bloomberg Law regarding the need for a national data privacy and security standard. They urge that the time for the US Congress to act on such a comprehensive federal privacy legislation is now. Their concerns and sense of urgency relate to the various risks that the capabilities and prevalent use of AI could pose on the privacy of consumer data. Specifically, how AI could be used by cybercriminals to create threats on critical infrastructure, use deepfake capabilities of AI to scam consumers, or steal sensitive personal information to carry out a multitude of other cyber-related and AI-driven crimes. Their points emphasize that consumers today want to have more control over how their data is used by businesses. As companies integrate AI into their tools, workflows, and services, there is a pressing need to align on a federal level privacy legislation to ensure the privacy protections of consumers.

**Analyst Perspective:** Just this year alone, nine states have passed their own comprehensive privacy legislation for consumers and for companies doing business in their states. Without comprehensive national privacy legislation in place, many companies have had to keep up with these recent and rapid changes as they apply to the national privacy law landscape. Moreover, for companies doing business in multiple states, legal teams have had to stay up to date on the differences and intricacies within each of the various state laws. Notwithstanding the confusion for consumers who may do business in different states, their privacy protections and control over their specific data can vary widely. The idea for comprehensive US federal privacy legislation would help alleviate such confusion, make it clearer for consumers to have more control over and know how their data is used, regardless of the state they are doing business in. In essence, such clarity could have a positive effect, leading to more consumer confidence as to how their data is used. Likewise, for US businesses, a comprehensive federal law could have the benefits of clarity and consistency of applicability as it relates to federal guidelines for consumer privacy protection. All of which could help address and reduce security and privacy risks as it relates to the introduction of AI into business processes, services, and products for both the public and private sector.

**Analyst:** [Erik Avakian](https://www.infotech.com/profiles/erik-avakian), Technical Counselor, Security & Privacy

**More Reading:**

* Source Material:
* [US lawmakers double down on AI, privacy correlation | IAPP](https://iapp.org/news/a/us-lawmakers-double-down-on-ai-privacy-correlation/)
* [AI’s Rise Flags Need for Federal Privacy and Security Protection | Bloomberg Law](https://news.bloomberglaw.com/us-law-week/ais-rise-flags-need-for-federal-privacy-and-security-protection)
* Related Info-Tech Research:
* [*Build a Data Privacy Program*](https://www.infotech.com/research/ss/build-a-data-privacy-program)
* [*Comply With the California Consumer Privacy Act*](https://www.infotech.com/research/ss/comply-with-the-california-consumer-privacy-act)
* [*Comply With the California Privacy Rights Act*](https://www.infotech.com/research/ss/comply-with-the-california-privacy-rights-act)

# German DPA Assesses Legal Aspect of Data Protection for AI Systems

## Type: Announcement

## Announcement Date: November 11, 2023

**Summary:** On November 11, the Baden-Württemberg Commissioner for Data Protection and Freedom of Information released a paper outlining their views on the legal protections in place for the use of AI systems. The discussion paper was developed to assist responsible bodies in the Baden-Württemberg region explore the potential legal bases that data protection laws provide for the use of AI systems. The online paper, which has an option for individuals to share their own thoughts on the several topics discussed, allows organizations to reflect on the current state of the data protection for AI systems and the sentiments shared by citizens. The discussions in the paper cover a wide range of topics for data protection within AI systems, including the phases of collecting and processing data, deploying AI applications, and the usage of the results derived from the AI system. It also covers the responsibilities under new data protection laws and the legal implications for both public (authorities) and non-public (organizations) bodies. A checklist is provided for data controllers whose organization is interested in or is in the process of using an AI system, to review the legal aspects to ensure it aligns with the data protection requirements. The checklist is mapped to various GDPR articles including article 2 (material scope), 3 (territorial scope), 4 (definitions), and 5 (principles relating to processing of personal data), which ensures data controllers are implementing measures that comply with regulations. This paper will provide guidance on what important privacy implications organizations should explore, as more focused AI legislation is being drafted within the EU.

**Analyst Perspective:** The discussion paper produced by the Baden-Württemberg DPA presents the unique approach data commissioners are taking to assess the legal and privacy implications of AI technologies. As more organizations are looking to investing into this technology, both to streamline their business operations and better secure their infrastructure, measures should be in place to ensure the data collected from these AI systems are continuing to meet regulatory standards. This includes the usage of these AI systems in processing and storing the data as well as the usage of the results from the AI applications. Many data protection authorities (DPA) within the EU have begun drafting their own AI legislations, to ensure guidelines are in place for the responsible use of AI. However, having a discussion forum where individuals can voice their concerns on the privacy implications of AI would allow governing bodies and organizations to understand the most pressing issues potential consumers are worried about, which include having an influence on the development of their AI policies and regulations. Although this paper was produced by the DPA of one German state, we can anticipate other states within the nation and possibly other EU nations will follow suit to better explore the legal protections for data privacy in AI systems.

**Analyst:** [Ahmad Jowhar](https://www.infotech.com/profiles/ahmad-jowhar), Research Analyst – Security & Privacy

**More Reading:**

* Source Material:
* [Baden-wuerttemberg.datenschutz (1)](https://www.baden-wuerttemberg.datenschutz.de/diskussionspapier-rechtsgrundlagen-im-datenschutz-beim-einsatz-von-kuenstlicher-intelligenz/)
* [Baden-wuerttemberg.datenschutz (2)](https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki/#iv_datenschutzrechtliche_verantwortlichkeit)
* [German DPA explores legal grounds for data security in AI | IAPP](https://iapp.org/news/a/german-dpa-explores-legal-grounds-for-data-security-in-artificial-intelligence/)
* Related Info-Tech Research:
* [*Prepare to Privacy-Proof Your AI Technology*](https://www.infotech.com/research/ss/prepare-to-privacy-proof-your-ai-technology)
* [*Address Security and Privacy Risks for Generative AI*](https://www.infotech.com/research/ss/address-security-and-privacy-risks-for-generative-ai)

# China’s Pursuit of Data Sovereignty: Impact on International Audit Firms

## Type: Announcement

## Announcement Date: November 15, 2023

**Summary:** As part of China's broader efforts to strengthen data security and sovereignty, the Chinese finance ministry is proposing new measures to increase oversight of accounting and audit firms. This will involve conducting additional cybersecurity checks for industries related to national security such as finance, energy, telecommunications, transport, technology, and national defense. They will be expected to adopt comprehensive technical means including, but not limited to, network isolation, user authentication, access control, encryption, and intrusion detection. Additionally, relevant data must be stored within China.

The draft rules will apply to audit firms working with listed companies, non-listed state-owned financial institutions, and those conducting cross-border audit work. Interestingly, by default, the chief partner of an audit firm will be considered ultimately responsible for ensuring data security.

**Analyst Perspective:** The proposed measures indicate a desire for more stringent oversight and control over the data-sharing practices of audit firms, especially in sectors deemed critical for national security. This move will likely result in more stringent compliance requirements, increasing administrative burdens and costs for organizations operating in and with the auditing ecosystem, especially across multiple countries. Such organizations will need to allocate resources for cybersecurity assessments and control mechanisms, potentially affecting the efficiency and timelines of audits.

While this move to reduce reliance on global accounting firms supports the objective of digital and data sovereignty for China, international auditors should contemplate challenges in accessing the Chinese market and prepare to adapt their business operations accordingly. Non-compliance could lead to legal penalties and have an adverse impact on reputation for organizations. China, on the other hand, should strive to strike a balance between data security and economic openness, so that foreign investment and cross-border business activities are not stifled.

**Analyst:** [Safayat Moahamad](https://www.infotech.com/profiles/safayat-moahamad), Research Director – Security & Privacy

**More Reading:**

* **Source Material:**
* [China proposes cybersecurity check for auditors if national security involved | Reuters](https://www.reuters.com/technology/cybersecurity/china-drafts-measures-how-accounting-firms-should-manage-data-2023-11-13/)
* [[China’s national security push aims to put auditors in cross hairs when sensitive data is involved | SCMP](https://www.scmp.com/economy/china-economy/article/3241523/chinas-national-security-push-aims-put-auditors-cross-hairs-when-sensitive-data-involved)](https://www.delawarepublic.org/politics-government/2023-09-11/gov-carrney-signs-delaware-personal-data-privacy-act-effective-2025)
* [[China Plans New Checks For Auditors, Accounting Firms | Asia Financial](https://www.asiafinancial.com/china-plans-new-checks-for-auditors-accounting-firms)](https://www.covingtonblogs.com/2023/07/10/delaware-general-assembly-passes-personal-data-privacy-act/)
* **Related Info-Tech Research:**
* [*Build a Data Privacy Program*](https://www.infotech.com/research/ss/build-a-data-privacy-program)
* [[*Secure Your High-Risk Data*](https://www.infotech.com/research/ss/secure-your-high-risk-data)](https://www.infotech.com/research/ss/mature-your-privacy-operations)
* [*Secure Operations in High-Risk Jurisdictions*](https://www.infotech.com/research/ss/secure-operations-in-high-risk-jurisdictions)