

**Privacy Regulation Roundup – November 2023**

This Privacy Regulation Roundup summarizes the latest major global privacy regulatory developments, announcements, and changes. This report is updated on a monthly basis. 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

[EU-APAC Privacy Regulation Roundup – EU and Japan Finalize Data Transfer Agreement 3](#_Toc151046441)

[Type: Announcement 3](#_Toc151046442)

[Announcement Date: October 28th, 2023 3](#_Toc151046443)

[US Regulation Roundup – President Biden's Plan to Advance the Agency's use of AI 4](#_Toc151046444)

[Type: Regulation 4](#_Toc151046445)

[Announcement Date: October 30, 2023 4](#_Toc151046446)

[Canada Privacy Regulation Round Up – Bill C-27 Lingers Due to Concerns 6](#_Toc151046447)

[Type: Regulation 6](#_Toc151046448)

[Announcement Date: TBD 6](#_Toc151046449)

[US Privacy Regulation Round Up – Delaware Became the Thirteenth US State to Adopt a Comprehensive Privacy Law 7](#_Toc151046450)

[Type: Regulation 7](#_Toc151046451)

[Announcement Date: September 11, 2023 7](#_Toc151046452)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# EU-APAC Privacy Regulation Roundup – EU and Japan Finalize Data Transfer Agreement

## Type: Announcement

## Announcement Date: October 28, 2023

**Summary:** On October 28th, the EU and Japan announced a landmark deal that will allow doing business online across both countries easier and more cost efficient. This agreement would be included in the EU-Japan Economic Partnership Agreement (EPA), which provides details on the common approaches both countries should implement when dealing with digital trade. The trade also aims at strengthening the digital protectionism and arbitrary restrictions that previously hindered the digital trade. This agreement will enable the handling of data without the administrative or storage requirements. Furthermore, the removal of data localization requirements would remove a costly obstacle that affected European and Japanese businesses. This removal would ensure that companies are not required to physically store their data locally, which will reduce complexities as businesses will not have to build and maintain their own data storage facilities and will reduce any potential data privacy threats. Many sectors would benefit from this agreement, including financial services, transportation, and machinery. This agreement took one year to be formalized, as the EU and Japan began the negotiation talks to include cross-border data flows in their EPA back in October 2022. This also follows new approaches of digital trade being included in the EU’s agreements with its trading partners, as it finalized similar agreements with New Zealand and the UK. Furthermore, other countries in the APAC region have begun negotiating a partnership agreement with the EU, as similar negotiations are taking place with South Korea and Singapore.

**Analyst Perspective:** The new data transfer agreement will not only strengthen the economic ties between the two countries, but it also depicts a growing trend in nations including digital trade as part of their economic partnership agreement. With the GDPR being recognized as a forefront in consumer data protection, organizations from different countries are ensuring their data privacy programs and practices comply with the EU’s regulations. Having this agreement formalized between countries is one step to ensure the importance of personal protection and privacy of consumer data is being recognized by nations who wish to further their economic ties through cross-border data flows. Furthermore, the data market, which is a marketplace where digital data is exchanged as products or services have had a positive impact to a country’s economy. With the data economy representing 2.6% and 1.2% of the EU’s and Japan’s GDP respectively, we can expect to see more nations formalizing data transfer agreements as we continue to head toward a more digitized world.

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

**More Reading:**

* Source Material:
* [European Commission](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5378)
* [Japantimes](https://www.japantimes.co.jp/news/2023/10/28/japan/politics/eu-japan-data-flow-agreement/)
* [iapp](https://iapp.org/news/a/eu-japan-finalize-economic-partnership-agreement/)
* Related Info-Tech Research:
* *Mature Your Privacy Operations*
* *Build a Data Privacy Program*

# US Regulation Roundup – President Biden's Plan to Advance the Agency's Use of AI

## Type: Regulation

## Announcement Date: October 30, 2023

**Summary:** The Executive Office of the President, Office of Management and Budget (OMB) has released a memorandum for the heads of executive departments and agencies to advance the use of artificial intelligence by focusing on three core tenets. The memorandum directs agencies to strengthen AI governance, advance responsible AI innovation, and manage risks from the use of AI, particularly those affecting the safety and rights of the public.

* **Strengthening AI Governance**
* Agencies must designate a Chief AI Officer (CAIO) within 60 days of the issuance of the memorandum.
* CAIOs will be responsible for implementing the memorandum and coordinating implementation with other agencies.
* Agencies must convene a senior-level AI governance body to coordinate and oversee AI issues.
* Agencies must submit compliance plans to OMB, including plans to update any existing internal AI principles and guidelines.
* Agencies must annually submit an inventory of their AI use cases to OMB, including information on safety-impacting and rights-impacting AI.
* **Advancing Responsible AI Innovation**
* CFO Act agencies must develop an enterprise AI strategy.
* Agencies are encouraged to reduce barriers to the responsible use of AI, such as barriers related to IT infrastructure, data, cybersecurity, workforce, and generative AI.
* **Managing Risks From the Use of AI**
* Agencies must follow minimum practices when using rights-impacting and safety-impacting AI.
* Agencies must enumerate specific categories of AI that are presumed to impact rights and safety.
* Agencies must establish a series of recommendations for managing AI risks in the context of Federal procurement.

The memorandum does not apply to AI used as a component of a national security system.

**Analyst Perspective:** The memorandum is a welcome step in ensuring that the Federal Government uses artificial intelligence (AI) responsibly and ethically. By strengthening AI governance, advancing responsible AI innovation, and managing risks from the use of AI, the memorandum aims to protect the safety and rights of the public. Designating a Chief AI Officer (CAIO) is a significant step toward strengthening AI governance in the Federal Government. CAIOs will be responsible for implementing the memorandum and coordinating implementation with other agencies, which will help to ensure that there is a unified approach to AI governance across the government.

The requirement for agencies to follow minimum practices when using rights-impacting and safety-impacting AI is essential and will help to mitigate the risks of AI being used in ways that could harm or discriminate against individuals. The requirement to convene a senior-level AI governance body is also important. This body will provide oversight and guidance on AI issues and help to ensure that AI is used in a way that is consistent with the government.

Finally, the requirement for CFO Act agencies to develop an enterprise AI strategy is a good way to encourage agencies to think strategically about how they can use AI to improve their operations and deliver better services to the public. The encouragement for agencies to reduce barriers to the responsible use of AI could include addressing issues such as IT infrastructure, data, cybersecurity, workforce, and generative AI's values and objectives.

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

**More Reading:**

* Source Material:
* [Proposed Memorandum for the Heads of Executive Departments and Agencies (ai.gov)](https://ai.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-Public-Comment.pdf)
* [OMB Releases Implementation Guidance Following President Biden’s Executive Order on Artificial Intelligence | OMB | The White House](https://www.whitehouse.gov/omb/briefing-room/2023/11/01/omb-releases-implementation-guidance-following-president-bidens-executive-order-on-artificial-intelligence/)
* [AI.gov: Making AI Work for the American People](https://ai.gov/)
* Related Info-Tech Research:
* [*AI Governance*](https://www.infotech.com/research/ss/ai-governance)
* [*Build Your Generative AI Roadmap*](https://www.infotech.com/research/ss/build-your-generative-ai-roadmap)
* [*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)

# Canada Privacy Regulation Round Up – Bill C-27 Lingers Due to Concerns

## Type: Regulation

## Announcement Date: TBD

**Summary:** Bill C-27 was introduced approximately a year ago. It aims to address privacy and generative artificial intelligence (GenAI) concerns in Canada. As of today, it is still in the review process. The delay in enacting the bill stems from two major concerns – first, the effectiveness of the privacy provisions, and second, the inadequacy of the GenAI guardrails. Over the next several months, Canadians will see hearings scheduled for the bill, but the enactment date will remain uncertain.

**Analyst Perspective:** Generative AI (GenAI) is a technology that carries immense potential on one hand but introduces significant privacy concerns on the other. Having regulations to govern the use of the technology, especially from a privacy perspective, is a must.

In addition to the existing challenges in enacting a regulation, GenAI is a new technology with a complex, significant impact and unknown elements compared to existing technologies. It is not to say that the Government should shy away from regulating. On the contrary, the Government should commit additional resources and effort to ensure that the regulation promotes innovation, and at the same time, protects the privacy of its constituents and citizens.

**Analyst:** [Hendra T. Hendrawan](https://www.infotech.com/profiles/hendra-hendrawan), Technical Counselor, Security & Privacy

**More Reading:**

* Source Material:
* [Letter from the Chair of the Standing Committee on Industry and Technology, House of Common, Minister of Innovation, Science and Industry](https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12600809/12600809/MinisterOfInnovationScienceAndIndustry-2023-10-03-e.pdf)
* [Why Industry Minister Champagne Broke the Bill C-27 Hearings on Privacy and AI Regulation in Only 12 Minutes.](https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12600809/12600809/MinisterOfInnovationScienceAndIndustry-2023-10-03-e.pdf%22%EF%B7%9FHYPERLINK%20%22Why%20Industry%20Minister%20Champagne%20Broke%20the%20Bill%20C-27%20Hearings%20on%20Privacy%20and%20AI%20Regulation%20in%20Only%2012%20Minutes%20-%20Michael%20Geist)
* Related Info-Tech Research:
* [*Build Your Generative AI Roadmap*](https://www.infotech.com/research/ss/build-your-generative-ai-roadmap)
* [*Build a Data Privacy Program*](https://www.infotech.com/research/ss/build-a-data-privacy-program)
* [*Privacy by Design for Digital Marketing*](https://www.infotech.com/research/ss/privacy-by-design-for-digital-marketing)
* [*Mature Your Privacy Operations*](https://www.infotech.com/research/ss/mature-your-privacy-operations)

# US Privacy Regulation Round Up – Delaware Became the Thirteenth US State to Adopt a Comprehensive Privacy Law

## Type: Regulation

## Announcement Date: September 11, 2023

**Summary:** Delaware recently joined 12 other states by passing the Delaware Personal Data Privacy Act (DPDPA), a comprehensive data privacy law effective from January 1, 2025. This legislation provides consumers with fundamental data rights, akin to other state laws, including the right to access, delete, and correct personal data. However, it also introduces distinctions from other state privacy laws:

* **Broader Applicability:** Unlike many other laws, the DPDPA lacks a revenue threshold, encompassing a wider array of businesses. Entities processing the personal data of 35,000 or more consumers or 10,000 or more consumers with over 20% gross revenue from personal data sales fall under its scope.
* **Sensitive Data:** The DPDPA expands the definition of "sensitive data" requiring consumer opt-in consent, potentially encompassing more types of information.
* **Opt-Out Compliance:** Controllers must adhere to opt-out preference signals, utilizing various platforms or technologies, ensuring consumers have control over the use of their data.
* **Age Restrictions:** The DPDPA restricts processing the data of consumers aged 13 to 18 for targeted advertising or sales without explicit consent. This age range differs from other state laws, typically covering those aged 13 to 16.

While the DPDPA aligns with familiar consumer data rights, businesses need to adapt to its unique features. The absence of a private right of action means enforcement falls under the Delaware Department of Justice, with penalties reaching $10,500 per violation. Companies operating in Delaware or targeting its residents should assess and update their data privacy practices to comply with the nuances of this new legislation.

**Analyst Perspective:** The Delaware Personal Data Privacy Act (DPDPA) introduces several unique provisions that businesses need to be aware of. Its broader applicability means that more businesses, including smaller ones, may fall under its scope. The expanded definition of “sensitive data” and the requirement for businesses to adhere to opt-out preferences will necessitate changes in data collection and handling practices. Additionally, the unique age restrictions may require businesses to implement robust age verification processes.

The enforcement of the DPDPA by the Delaware Department of Justice, with penalties reaching $10,500 per violation, underscores the importance of compliance. Businesses, especially those operating in Delaware or targeting its residents, should begin reviewing and updating their data privacy practices and notices well ahead of the January 1, 2025, effective date to avoid potential penalties. The enactment of the DPDPA represents a significant development in the US privacy landscape, and proper privacy compliance should be a top priority for businesses.

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

**More Reading:**

* **Source Material:**
* [Gov. Carney Signs Delaware Personal Data Privacy Act, effective 2025](https://www.delawarepublic.org/politics-government/2023-09-11/gov-carrney-signs-delaware-personal-data-privacy-act-effective-2025)
* [Delaware General Assembly Passes Personal Data Privacy Act](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)
* [*Mature Your Privacy Operations*](https://www.infotech.com/research/ss/mature-your-privacy-operations)