iapp

AMERICAN PRIVACY RIGHTS ACT

cheat sheet

Overview of the discussion draft published 21 May 2024.

Scope

Covered entities, either alone or jointly with others, determine the purposes and means of processing covered data.

Includes:
- Businesses subject to the U.S. Federal Trade Commission's authority.
- Common carriers.
- Nonprofits.

Excludes small businesses if all of the following apply:
- They have less than USD40 million in annual revenue, adjusted for inflation.
- They process covered data of less than 200,000 individuals, with exceptions.
- They do not earn revenue from the transfer of covered data to third parties, with exceptions including targeted advertising.

Service providers process covered data on behalf of, and at the direction of, a covered entity or another service provider.

Selected Definitions

Covered algorithm means a computational process that is used to substantially assist or replace discretionary human decision-making using covered data to provide outputs that are not predetermined in order to make a consequential decision.

Covered data includes information that identifies or is linked or reasonably linkable to an individual, including in combination with other information and excluding deidentified data.

Individual means a natural person residing in the U.S.

Sensitive data is defined broadly to include data related to government identifiers; health; biometrics; genetics; financial accounts and payments; precise geolocation; log-in credentials; private communications; revealed sexual behavior; calendar or address book data, phone logs, photos and recordings for private use; intimate imagery; video viewing activity; race, ethnicity, national origin, religion or sex; online activities over time and across third-party websites; and information about a minor under the age of 17.

Third party means any entity that receives covered data from another entity, except service providers. All "covered entity" requirements apply to third parties, except sensitive data, 39(b).

Additional obligations

Large data holders, whether covered entities or service providers, must also:
- Publish privacy policies from the past 10 years.
- Publish annual transparency reports about consumer requests.
- Provide annual CEO-signed certifications of compliance controls to the FTC.
- Empower a privacy officer and a security officer with mandated reporting lines.
- Conduct biennial audits and privacy impact assessments.
- When AI is used to make a consequential decision, either conduct an independent audit or submit annual internal impact assessments to the National Telecommunications and Information Administration.

Data brokers, a type of covered entity, must also:
- Provide special notices to consumers and register on the FTC-managed registry.
- Honor "Do Not Collect" and "Delete My Data" requests via the centralized mechanism established by the FTC. Once established, the private right of action applies to this obligation.
- Not rely on the "bona fide loyalty program" exception to the prohibition on retaliation.

Covered high-impact social media companies must also:
- Treat individuals' activities on their platforms as sensitive data, even if it is not "over time and across websites or services."
- Treat any ads selected based on data collected "over time" as targeted advertising, including first-party data "but not based on a profile created about the individual."
- Not rely on the "bona fide loyalty program" exception to the prohibition on retaliation.

Effective date: 180 days after enactment, unless otherwise indicated.

Enforcement: Enforceable by the FTC, state attorneys general, the chief consumer protection officer of a state, or an authorized officer or office of the state.

Private right of action: Individuals have a private right of action to enforce various provisions and can seek damages, injunctive relief, declaratory relief, and reasonable legal and litigation costs.

Relationship to other laws: State privacy law provisions "covered by" the provisions of APRA are preempted, with enumerated exceptions. Existing sectoral federal privacy laws, such as the Gramm-Leach-Bliley Act, are preserved.

Key obligations

	Covered entities	Service providers	Subject to PRA

Section 102: Data minimization
Generally, processing of personal data is prohibited unless:
• Necessary, proportionate and limited to provide or maintain either:
  • A specific product or service requested by the individual.
  • An anticipated nonadvertising communication to the individual.
• For one of the 16 listed permitted purposes.
	✓	✓	✗

• Sensitive data also requires opt-in consent for transfer.	✓	✓	✓
• Biometric and genetic information also require opt-in consent for collection or processing, unless for one of nine permitted purposes.	✓	✓	✓
Section 103: Privacy by Design Mandatory reasonable policies, practices and procedures must "mitigate privacy risks and implement reasonable internal training and safeguards.	✓	✓	✗
Section 104: Transparency Privacy policies must list prescribed information, including categories of third parties and names of any data broker transfers.	✓	✓	✓
Material changes require prenotification and means of opting out.	✓	✗	✓
Section 105: Individual control over covered data Consumer rights include access, correction, deletion and portability, with a 30- to 45-day deadline.	✓	✗	✓
Section 106: Opt-out rights and universal mechanism Individuals have rights to opt out of covered data transfers and targeted advertising.	✓	✗	✓
Signals must be respected once centralized opt-out mechanisms are established.	✓	✗	✓
Section 107: Interference with consumer rights Dark patterns are prohibited if they interfere with notice, consent or choice.	✓	✗	✓
Conditioning the exercise of rights on misleading or fraudulent statements is prohibited.	✓	✗	✓
Section 108: Prohibition on denial of service and waiver of rights Retaliation through service or pricing for exercising consumer rights is prohibited, except for bona fide loyalty programs.	✓	✗	✓
Section 109: Data security and protection of covered data Reasonable data security practices, including regular training, are required.	✓	✓	✓ for breach only
Section 110: Executive responsibility At least one privacy and data security officer is required.	✓	✓	✗
Section 111: Service providers and third parties Contracts and reasonable due diligence are required before selecting a service provider or transferring to a third party.	✓	✓	✓
Service providers must adhere to the instructions of covered entities and implement reasonable safeguards.	✗	✓	✗
Section 113: Civil rights and algorithms Processing covered data in a way that discriminates on the basis of race, color, religion, national origin, sex or disability is prohibited with exceptions, including for testing to prevent discrimination.	✓	✓	✓
Knowingly developing an algorithm designed to make a consequential decision requires a design evaluation prior to deployment. If not conducted by an independent auditor, the design evaluation must be shared with the NTIA.	✓	✓	✗
Section 114: Consequential decision opt out Using a covered algorithm to make or facilitate a consequential decision requires notice and an opportunity to opt for a human decision instead.	✓	✗	✓

Updated June 2024.

iapp.org