iapp

AMERICAN PRIVACY RIGHTS ACT

cheat sheet

Overview of the discussion draft published 7 April 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.
- 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.

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

Selected Definitions

Covered algorithm means a computational process that makes a decision or facilitates human decision-making by using covered data.

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

Individuals 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; information about a minor under the age of 17; and other data the FTC defines as sensitive covered data by regulation.

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.
- Submit impact assessments to the FTC when AI poses a consequential risk of harm,

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" requests via the centralized opt-out 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 advertising "over time" on the platform as targeted advertising, with exceptions.
- Not rely on the "bona fide loyalty program" exception to the prohibition on retaliation.

Effective date: 180 days after enactment.

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: Nonsectoral state privacy laws are preempted but existing sectoral federal privacy laws, such as the Gramm-Leach-Bliley Act, are preserved.

Key obligations

	Covered entities	Service providers	Subject to PRA

Section 3: 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 communication to the individual.
• For one of the 15 listed permitted purposes.
	✓	✓	✗

• Sensitive data requires opt-in consent for transfer.	✓	✓	✓
• Biometric and genetic information require opt-in consent for collection or transfer.	✓	✓	✓
Section 4: Transparency Privacy policies must list prescribed information, including categories of third parties and names of any data broker transfers.	✓	✓	✓
Material changes require pre-notification and means of opting out.	✓	✗	✓
Section 5: Individual control over covered data Consumer rights include access, correction, deletion and portability.	✓	✗	✓
Section 6: Opt-out rights and centralized mechanism The right to opt out of covered data transfers and targeted advertising is included.	✓	✗	✓
Signals must be respected once centralized opt-out mechanisms are established.	✓	✗	✓
Section 7: 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 8: Prohibition on denial of service and waiver of rights Retaliation for exercising consumer rights is prohibited.	✓	✗	✓
Section 9: Data security and protection of covered data Reasonable data security practices, including regular training, are required.	✓	✓	✓ for breach only
Section 10: Executive responsibility A privacy or data security officer is required.	✓	✓	✗
Section 11: Service providers and third parties Reasonable due diligence is required for selecting a service provider and transferring to a third party.	✓	✗	✓
Service providers must adhere to the instructions of covered entities and implement reasonable safeguards.	✗	✓	✗
Section 13: 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.	✓	✓	✓
Annual algorithm impact assessments for large data holders are required if there is a "consequential risk of harm" to defined groups or outcomes, including minors, major life events and disparate impacts.	✓ if applicable	✓ if applicable	✗
Section 14: Consequential decision opt out An entity that uses a covered algorithm to make or facilitate a consequential decision, further defined by future FTC rules, must provide notice and an opportunity to opt out.	Applies to "entities"	Applies to "entities"	✓

Published April 2024.

iapp.org