American Data Privacy and Protection Act (Text, Summary)

This Chart is from the Bill as Amended with provisions post July 20, 2022

Individual Rights		
Sec. 103	**Covered Data and Entities**	• ADPPA applies to any entity that processes Covered Data and is subject to the Federal Trade Commission Act (FTC Act) • Categories of covered entities: nonprofits, common carriers, and entities such as large data holders that meet certain thresholds and service providers that use data on behalf of other entities (including covered entities, government entities, and other service providers) • Covered data: Expands previously identified categories of information considered sensitive in nature, now includes information that identifies an individual's online activities and information on one's race, color, ethnicity, religion, or union membership. • Data minimization: companies would only be allowed to collect/make use of user data if is necessary for one of *17 permitted purposes*, including authenticating users, preventing fraud, and completing transactions. Collection and use outside of these purposes would be prohibited.
Sec. 204	**Private Right of Action**	• Creates a delayed private right of action 2 years post-enactment. • Injured individuals, or classes of individuals, would be able to sue covered entities in federal court for damages, injunctions, litigation costs, and attorneys' fees. Notification of FTC and state attorney general prior to suit is required. • Before bringing a suit for injunctive relief or a suit against a small- or medium-size business, individuals would be required to give the violator an opportunity to address the violation. • Pre-dispute arbitration agreements or joint-action waivers with individuals under the age of 18 are unenforceable in disputes arising under the ADPPA.
Sec. 207	**Civil Rights and Algorithms**	• Prohibits most covered entities from using covered data in a way that discriminates on the basis of protected characteristics (such as race, gender, or sexual orientation). • Requires large data holders to conduct algorithm impact assessments. These assessments would need to describe the entity's steps to mitigate potential harms resulting from its algorithms, among other requirements. • Large data holders are required to submit these assessments to the FTC and make them available to Congress on request.
Sec. 205	**Youth Protections**	• Targeted advertising is prohibited with respect to such minors and data transfers to third parties require consent. • Approved purposes for data of minors: may collect, process, or transfer covered data of an individual the covered entity or service provider knows is under the age of 18 solely in order to submit information relating to child victimization to law enforcement or to a non-profit, national resource center and clearinghouse congressionally designated to provide assistance to victims, families, child-serving professionals, and the general public on missing and exploited children issues

		• Places stringent requirements on processing data from, targeting advertisements to, and sharing data from minors who are under the age of 17, so entities interacting with covered data from children under 16 would have significant risk calculations.
Secs. 201-204	**Consumer Control and Consent**	• Continuation of prior consumer data rights, namely: access, deletion; correction; right to export covered data; right to opt-out of covered transfers; and right to opt-out of targeted advertising • On the point of verification, a covered entity is not permitted to exercise an individual rights in whole or in part, if they cannot reasonably verify the individual whom the data belongs to, or the authorized person • Consent requests must include a description of each processing purpose for which consent is sought.
Business Obligations		
Sec. 208	**Data Security**	Additional permissible purposes for the collecting, processing, or transfer of covered data: • Data previously collected by a service provider at the direction of a government entity, or a service provided to a government entity by a covered entity, and only insofar as authorized statute, to prevent, detect, protect against, or respond to a public safety incident. • Non-advertisement communications, if reasonably anticipated by the individual within the context of their interactions with the covered entity • A covered entity may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate.
Sec. 209(c), 304	**Small and Medium – size Businesses**	• Relieves small- and medium-size businesses from complying with several requirements; for instance, these businesses may respond to a consumer's request to correct their data by deleting the data, rather than correcting it. • Large data holders must comply with a request within 45 days of verification, whereas covered entities that are not large data holders or do not fall under the small business protections will have 60 days to respond, covered entities that fall under the small business protections will have 90 days to respond.
Sec. 206	**Third-party Collecting Entities**	• These entities would have to comply with FTC auditing regulations and, if they collect data above the threshold number of individuals or devices, FTC registration is required. Mandates a clear and readily accessible notice on the website or mobile application of the third-party collecting entity (if the third-party collecting entity maintains such a website or mobile application) that notifies individuals that the entity is a third- party collecting entity using specific language, including a link to the website, and is accessible by individuals with disabilities
Sec. 202	**Transparency**	• Requires covered entities to disclose, among other things, the type of data they collect, what they use it for, how long they retain it, and whether they make the data accessible to the People's Republic of China, Russia, Iran, or North Korea.
Sec. 101-104	**Duties of Loyalty**	• Prohibits covered entities from collecting, using, or transferring covered data beyond what is *reasonably necessary and proportionate* to provide a service requested by the individual, unless the collection, use, or disclosure would fall under one of seventeen permissible purposes.

		• It also would create special protections for certain types of sensitive covered data, defined as sixteen different categories of data. • Affirmative & express consent from the consumer is required before transferring their sensitive covered data to a third party unless a specific exception applies.
Enforcement		
Sec. 404b	**Preemption**	• In general, no State or political subdivision of a State may adopt, maintain, enforce, prescribe, or continue in effect any law, regulation, rule, standard, requirement, or other provision having the force and effect of law of any State, or political subdivision of a State, covered by the provisions of HR 8152, or a rule, regulation, or requirement promulgated under HR 8152 • While certain state laws or provisions thereof are specifically identified in HR 8152 as not being pre-empted ('BIPA') and the data breach-based private right of action under the CCPA/ ('CPRA') other descriptors are so broad that they could put numerous State laws back in play.
Secs. 401-403	**Enforcement**	• Enforcement to begin 2 years post enactment. • Exception: private right of action will not apply to claims against covered entities that have less than $25 million per year in revenue, or covered entities that collect, process, or transfer the covered data of fewer than 50,000 individuals, and derive less than 50% of their revenue from transferring covered data. • It would be enforceable by the FTC and by state attorneys general in civil actions.

Key Definitions:

Covered Data / Sensitive Data	-Information that identifies or is linked or reasonably linkable to individuals (Sec.2(8)(A) ADPPA)but excludes (i) de-identified data, (ii) employee data, and (iii) publicly available information (as well as inferences made from such information). -Sensitive covered data also includes a government-issued identifier, such as a Social Security number, passport number that is not required by law to be displayed in public, information identifying the sexual orientation, online activities over time or across third-party websites information that describes or reveals the past, present, or future physical health, and biometric and genetic information etc.
Covered Entities	-Any entity or person that collects, processes, or transfers covered data subject to appropriate data regulations within the United States
Third-Party Collecting Entities	-Entities whose main source of revenue comes from processing or transferring data that they do not directly collect from consumers (e.g., data brokers)
Large Data Holder	-Covered entities that have a gross annual revenue of at least USD 250 million and they collect, process, or transfer the covered data of more than five million individuals
Impact Assessment	-All organizations that meet the criteria for being a large data holder must conduct a privacy impact assessment which is reasonable & appropriate in scope concerning the nature and volume of data collected, processed, and transferred; Results of the assessment must be documented in written form and maintained until the following assessment. -The assessment must be approved by the relevant privacy officer of the organization.
Biometric Information	-Any covered data generated from the measurement, observation, tracking, collecting, or processing of an individual's biological, physical, or physiological characteristics such as fingerprints, voice, iris, or retina imagery scans, facial or hand imagery, gait, or any other identifying physical movements.
Affirmative Express Consent	- Individual's freely given, specific, informed, and unambiguous authorization for an actor practice that is clearly communicated in response to a specific request from a covered entity. -Said request must be provided in a stand-alone disclosure and meet comprehensive transparency requirements (Sec.2(1)(B)ADPPA).
Employee Data	- Information relating to a job applicant collected by a covered entity acting as a prospective employer, information processed by an employer relating to an employee who is acting in a professional capacity for the employer, and emergency contact information collected by an employer that relates to an employee of that employer.
De-Identified Data	- Information that does not identify and is not linked or reasonably linkable to a distinct individual or a device, regardless of whether the information is aggregated, and if the covered entity or service provider takes reasonable technical measures to ensure information cannot be used, at any time, to re-identify any individual; publicly commits to process and transfer info in a solely de-identified form
First Party Advertising	- Advertising or marketing conducted by a first party either through direct communications with a user such as direct mail, email, or text message communications, or advertising or marketing conducted entirely within the first-party context, such as in a physical location operated by the first party, or on a web site or app operated by the first party
Targeted Advertising	- Presenting to an individual or device identified by a unique identifier, or groups of individuals or devices identified by unique identifiers, an online advertisement that is selected based on known or predicted preferences, characteristics, or interests associated with the individual or a device identified by a unique identifier
Publicly Available Information	- Any information that a covered entity or service provider has a reasonable basis to believe has been lawfully made available to the general public from Federal, State, or local government records; media, a website or online service made available to all members of the public

Service Provider	-Person or entity that collects, processes, transfers, or receives covered data on behalf of, and at the direction of, a covered entity or a Federal, State, Tribal, territorial, or local government entity
Widely Distributed Media	-Information that is available to the public, including information from a telephone book or online directory, a television, internet, or radio program, the news media, or an internet site that is available to the general public on an unrestricted basis, but does not include an obscene visual depiction