The Data Protection Act of 2021 by Senator Gillibrand

Section-by-Section

Section 1: SHORT TITLE; TABLE OF CONTENTS

The title of the bill is the "Data Protection Act of 2021"

Section 2: DEFINITIONS [only select definitions are included here]

- **"Automated decision system"** means a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision, or facilitates human decision making,
- "**Data Aggregator"** refers to any person who collects, uses, or shares, in or affecting interstate commerce, an amount of personal data that is not de minimus, as well as entities related to that person by common ownership or corporate control. It does not include an individual who collects, uses, or shares personal data solely for non-commercial reasons.
- **"Federal Privacy Law"** means the provisions of this title and all subsequent law created by this Agency, including other specified laws, such as the Children's Online Privacy Protection Act and the Fair Credit Reporting Act.
- **"High-Risk Data Practice"** is an action by a data aggregator that involves:
    - the use of an automated decision system;
    - the processing of data in a manner that reveals an individual's protected class, familial status, lawful source of income, financial status such as the individual's income or assets), veteran status, criminal convictions or arrests, citizenship, past, present, or future physical or mental health or condition, psychological states, or any other factor used as a proxy for identifying any of these characteristics;
    - a systematic processing of publicly accessible data on a large scale;
    - processing involving the use of new technologies, or combinations of technologies, that causes or materially contributes to privacy harm;
    - decisions about an individual's access to a product, service, opportunity, or benefit which is based to any extent on automated decision system processing;
    - any profiling of individuals on a large scale;
    - any processing of biometric information for the purpose of uniquely identifying an individual, with the exception of one-to-one biometric matching;
    - combining, comparing, or matching personal data obtained from multiple sources;
    - processing which involves an individual's precise geolocation;
    - the use of personal data of children and teens under 17 or other vulnerable individuals such as the elderly, people with disabilities, and other groups known

to be susceptible for exploitation for marketing purposes, profiling, or automated processing; or

- consumer scoring or other business practices that pertain to the eligibility of an individual, and related terms, rights, benefits, and privileges, for employment (including hiring, firing, promotion, demotion, and compensation), credit, insurance, housing, education, professional certification, or the provision of health care and related services.

- **"High-Risk Data Practice Impact Assessments "** means a study conducted after deployment of a high-risk data practice that includes, at a minimum—
  - an evaluation of a high-risk data practice's accuracy, disparate impacts on the basis of protected class, and privacy harms;
  - an evaluation of the effectiveness of measures taken to minimize risks as outlined in any prior high-risk data practice risk assessments; and
  - recommended measures to further minimize risks to accuracy, disparate impacts on the basis of protected class, and privacy harms.
- **"High-Risk Data Practice Risk Assessment"** means a study evaluating a high-risk data practice and the high-risk data practice's development process, including the design and training data of the high-risk data practice, if applicable, for likelihood and severity of risks to accuracy, bias, discrimination, and privacy harms that includes, at a minimum—

(A) a detailed description of the high-risk data practice, including—

(i) its design and methodologies;

(ii) training data characteristics;

(iii) data; and

(iv) purpose;

(B) an assessment of the relative benefits and costs of the high-risk data practice in light of its purpose, potential unintended consequences, and taking into account relevant factors, including—

(i) data minimization practices;

(ii) the duration and methods for which personal data and the results of the high-risk data practice are stored;

(iii) what information about the high-risk data practice is available to individuals;

(iv) the extent to which individuals have access to the results of the high-risk data practice and may correct or object to its results; and

(v) the recipients of the results of the high-risk data practice;

(C) an assessment of the risks of privacy harm posed by the high-risk data practice and the risks that the high-risk data practice may result in or contribute to inaccurate, biased, or discriminatory decisions impacting individuals or groups of individuals;

(D) the decision to accept, reject, or mitigate and minimize risks and the measures a data aggregator will employ including to minimize the risks described in subparagraph(C), including technological and physical safeguards.

- **"Personal Data"** means electronic data that, alone or in combination with other data—
    - identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual, household, or device; or
    - could be used to determine that an individual or household is part of a protected class.
- **"Precise geolocation"** means any data that is derived from a device and that is used or intended to be used to locate an individual within a geographic area that is equal to or less than the area of a circle with a radius of one thousand, eight hundred and fifty (1,850) feet.
- **"Privacy Harm"** means an adverse consequence, or a potential adverse consequence, to an individual, a group of individuals, or society caused, in whole or in part, by the collection, use, or sharing of personal data. (examples listed in the bill)
- **"Process"** means to perform an operation or set of operations on personal data, either manually or by automated means, including collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, sorting, classifying, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.
- **"Profile"** means the use of an automated decision system to process data (including personal data and other data) to derive, infer, predict or evaluate information about an individual or group, such as the processing of data to analyze or predict an individual's identity, attributes, interests or behavior.

Section 3: ESTABLISHMENT OF THE DATA PROTECTION AGENCY

- Establishes the United States Data Protection Agency as an independent agency in the Executive Branch, which shall regulate high-risk data practices and the collection, use, and sharing of personal data.
- The Director is appointed by the President and confirmed by the Senate. The Director will have knowledge and expertise in technology, protection of personal data, civil rights and liberties, law, and social sciences.
- The Director shall appoint their Deputy Director who will serve as acting Director in the event of the Director's death, resignation, sickness, or absence.
- The Director will have a term of 5 years.
- The President may remove the Director at will, as required by *Seila Law v. CFPB*.

Section 4: EXECUTIVE AND ADMINISTRATIVE POWERS

- The Agency has independence and has the authority to carry out its duties under this Act. This authority is largely vested with the Director.

Section 5: ADMINISTRATION

- The Agency shall:
    - Employ attorneys, compliance examiners, compliance supervision analysts, economists, technologists, data scientists, designers, ethicists, privacy experts, statisticians, and other employees as may be deemed necessary.
    - Establish an ombud as a liaison for affected persons.
- Allows an agency-specific personnel structure modeled on the CFPB's authorizations in order to attract technologists and engineers who could earn several times more than the GS schedule allows.
- Creates three specific functional units within the DPA:
    1. **Office of Civil Rights**. The Agency's Office of Civil Rights will:
        - provide oversight and enforcement of federal privacy laws to ensure that the collection, use, and sharing of personal data is fair, equitable, and non-discriminatory in treatment and effect;
        - develop, establish, and promote data processing practices that affirmatively further equal opportunity to and expand access to housing, employment, credit, insurance, education, healthcare, and other aspects of interstate commerce;
        - work with civil rights advocates, privacy organizations, and data aggregators on the promotion of compliance with the civil rights compliance under federal privacy laws;
        - liaise with communities and consumers impacted by practices regulated by this Act and the Agency;
        - provide annual reports to Congress on the efforts of the Agency to fulfill its civil rights mandate.
    2. **Research.** The Agency's Research Unit shall research, analyze, assess, and report on:
        - the collection and use of personal data, including automated decision systems;
        - the collection and processing of personal data by government agencies, including contracts between government agencies and data aggregators; and
        - unfair, deceptive, or discriminatory outcomes that result or are likely to result from the use of automated decision systems, including disparate treatment or disparate impact on the basis of protected class or proxies for protected class.

3. **Collecting and Tracking Complaints.** The Director shall establish a unit, the functions of which shall include identifying and facilitating the development of best practices for consumers to file a complaint, and establishing a single toll-free telephone number, a publicly available website, and a publicly available database, or utilizing an existing publicly available database, to facilitate the centralized collection of, monitoring of, and response to complaints regarding the collection, use, and sharing of personal data.

Section 6: COORDINATION

- The Agency shall coordinate with other Federal agencies and State regulators to promote consistent regulatory treatment of personal data.

Section 7: REPORTS AND INFORMATION

- The Director shall submit semi-annual reports to the President and Congress, and shall appear before Congress at semi-annual hearings regarding the reports. The reports shall be made public on the Agency website.

Section 8: FUNDING; PENALTIES AND FINES

- Authorizes the Agency to set and collect an assessment, fee, or other charge from data aggregators with annual gross revenues over $25M or who annually collect, use, or share, the personal data of 50,000 or more individuals. Such amounts are deposited into the Data Protection Agency Fund.
    - The Data Protection Agency Fund is available to pay the expenses of the Agency in carrying out its duties and responsibilities.
    - Funds obtained by or transferred to the Agency Fund may not be construed to be Government funds or appropriated monies, and are not subject to apportionment.
- Establishes the "Data Protection Civil Penalty Fund." If the Agency obtains a civil penalty against any person in any action under Federal laws, the Agency shall deposit the penalty into the Civil Penalty Fund.
    - Amounts in the Civil Penalty Fund are available to the Agency for payments to the victims of activities for which penalties have been imposed under federal privacy laws.
    - To the extent that individuals cannot be located or such redress, payments or compensation, or other monetary relief are otherwise not practicable or economically viable, the Agency may use such funds for the purpose of consumer or business education relating to data protection or for technological research.
        - The Agency may also utilize a cy-pres approach to distribute funds in order to advance data protection and privacy in the U.S. The Agency may identify recipients, including charitable and civil society organizations,

whose interests reasonable approximate those of the victims of the activities for which civil penalties have been imposed and distribute funds from the Civil Penalty Fund to those recipients.

Section 9: PURPOSE, OBJECTIVES, AND FUNCTIONS OF THE AGENCY

- **Purpose:** The purpose of the Agency is to protect individuals' privacy; prevent and remediate privacy harms; prevent, remediate, and reduce discrimination on the basis of protected class through the processing of personal information, including both differential treatment on the basis of a protected class and disparate impact on a protected class; prevent, remediate, and reduce processing of personal information that has the effect of depriving equal opportunity on the basis of protected class; and limit the collection, use, and sharing of personal data.
- **Objectives**: The Agency is authorized to exercise its authorities under this Act for the following purposes:
    - Protect individuals from violations of this Act, other Federal privacy laws, or rules and orders issued under this Act;
    - Promote and affirmatively further equal opportunity in all aspects of economic life as it relates to fair and non-discriminatory processing of personal information;
    - Oversee the use of high-risk data practices;
    - Promote the minimization of collection of personal data for commercial purposes;
    - Prevent and remediate privacy harms; and
    - Ensure that Federal privacy law is enforced consistently and in order to protect individuals' privacy.
- **Functions**: Agency will provide leadership and coordination to all Federal departments and agencies to enforce all Federal statutes, Executive Orders, regulations, and policies that involve privacy or data protection. The Agency will maximize effort, promote efficiency, and eliminate conflict, competition, duplication, and inconsistency among the operations, functions, and jurisdictions of relevant Federal department and agencies.
    - The Agency will also provide leadership, guidance, education, and appropriate assistance to private sector businesses, organizations, and individuals regarding privacy and data protection rights and standards.
    - The Agency will require and oversee ex-ante high-risk data practice risk assessments and ex-post high-risk data practice impact evaluations to advance fair and just data practices.
    - The Agency will protect individuals and groups of individuals from privacy harms.
    - The Agency will examine the social, ethical, economic, and civil rights impacts of data collection and processing practices and propose remedies.

- The Agency will protect civil rights, combat unlawful discrimination, and affirmatively further equal opportunity as they relate to the processing of personal information.
- The Agency will ensure that high-risk data privacy practices are fair, just, non-deceptive, and do not discriminate against a protected class.
- The Agency will collect, research, and respond to complaints.
- The Agency will develop model privacy and data protection standards, guidelines, and policies for use by the private sector.
- The Agency will enforce other privacy statutes and rules as authorized by Congress.

Section 10: RULEMAKING AUTHORITY

- The Agency shall prescribe rules and issue orders and guidance in order for it to effectively carry out the purposes of Federal privacy laws.
- The Agency shall issue such regulations the Administrative Procedure Act identifying:
  - high-risk data practices in connection with the collection, use, or sharing of personal data, which may include requirements for the purpose of auditing, preventing, or restricting such acts or practices;
  - acts or practices in connection with the collection, use, or sharing of personal data that causes or are likely to cause privacy harm to individuals or groups of individuals, which may include requirements for the purpose of preventing or restricting such acts or practices;
  - unlawful, unfair, deceptive, abusive, or discriminatory acts or practices in connection with the collection, use, or sharing of personal data, which may include requirements for the purpose of preventing or restricting such acts or practices, for the purpose of preventing disparate impacts on the basis of a protected class, or for the purpose of affirmatively furthering equal opportunity;
  - rights that data aggregators must provide to individuals, including the right to access and correct, limit the processing of, and request deletion of the individual's personal data; and
  - obligations on data aggregators, including transparency about business practices, data collection limitations, processing and disclosure limitations, purpose specification and legal basis for processing requirements, accountability requirements, confidentiality and security requirements, and data accuracy requirements.
- In creating rules the Agency shall consider potential benefits and costs to individuals or groups of individuals. The Agency shall consult with civil society groups and the public. The Agency may apply a rule to a subcategory of data aggregators.

- The Agency will monitor for risks to individuals or groups of individuals in the collection, disclosure, processing, and misuse of data.

Section 11: SUPERVISION OF DATA AGGREGATORS

- The Agency may require reports and conduct examinations of a periodic basis of large data aggregators (defined as data aggregators with gross annual revenues that exceed $25M and/or annually collects, uses, or shares the personal data of 50,000 or more individuals, households, or devices)
    - The Agency can ask for reports from these entities to ensure they are complying with Federal privacy laws, their internal compliance systems, detecting/assessing risks these practices have to consumers, and requiring and overseeing high-risk data practice risk assessments and high-risk data practice impact evaluations.
- The Agency must maintain a publicly accessible list of data aggregators that collect, use, or share personal data of more than 10,000 persons or households, and the permissible purposes for which the data aggregators purport to collect personal data
- **Merger review:** The Agency must conduct a review and submit to the FTC and DOJ a report on the privacy and data protection implications of any merger involving a large data aggregator, or any merger that proposes the transfer of personal data of 50,000 or more individuals.

Section 12: PROHIBITED ACTS

- It is unlawful for:
    - any data aggregator or service provider to commit any act or omission in violation of this Act, Federal privacy law, or any rule or order issued by the Agency under this Act;
    - any data aggregator or service provider to commit any unlawful, unfair, deceptive, abusive, or discriminatory acts or practices in connection with the collection, processing, or sharing of personal data;
    - any data aggregator or service provider to fail or refuse: to permit access to or copying of records, to establish or maintain records, or to make reports or provide information to the Agency;
    - any person to knowingly or recklessly provide substantial assistance to a data aggregator or service provider in violation of this Act or Federal privacy law, or any rule or order issued thereunder; or
    - any person to re-identify, or attempt to re-identify, an individual, household, or device from anonymized data, unless such person is conducting authorized testing to prove personal data has been anonymized.

Section 13: ENFORCEMENT POWERS

- The Agency may conduct investigations, subpoena for testimony or documents, and issue civil investigative demands, and must treat investigation documents confidentially.
- The Agency may conduct hearings and adjudication proceedings to ensure or enforce compliance of this Act. The Agency may issue cease-and-desist orders, and temporary cease and-desist orders if continued actions during a proceeding may result in insolvency of an affected person or prejudice individual interest.
- The Agency may engage in joint investigations, including on matters relating to protection of individuals' civil rights.
- The Agency may commence a civil action to impose a civil penalty or to seek all appropriate legal and equitable relief, including permanent or temporary injunction.
    - The Attorney General will be notified about any civil cases and there will be coordination between the Agency and the Attorney General to ensure consistency in litigation. The investigations of the Agency will not impede any parallel investigations undertaken by the Attorney General.
    - There is a 5 year statute of limitations from the date of discovery of the violation.
- **Relief available:**
    - The Agency is able to grant appropriate relief to victims of violations of Federal privacy law. This includes, but is not limited to: reformation of contracts, refund of money, restitution, disgorgement, and civil money penalties.
    - Penalty Amounts:
        - **First tier:** For any violation of a law, rule, or final order or condition imposed in writing by the Agency, a civil penalty may not exceed $5,000 for each day the violation continues;
        - **Second tier:** any person that recklessly engages in Federal privacy law violations, daily penalties will not exceed $25,000.
        - **Third tier:** any person who knowingly violates Federal privacy law will not receive a daily fine higher than $1,000,000.
    - When determining the penalty for civil complaints, the Agency will take into account the size of financial resources and good faith of the person charged, the gravity of the violation/if they failed to pay, the severity of risk/loss faced by individuals affected by violation, and if there is a history of violations. The Agency may alter or compromise any penalty that has already been assessed.
    - Civil penalties cannot be issued unless the person has had an opportunity for a hearing and the court rules in favor of the Agency.
    - The Agency, State Attorney General, or any State regulator may recover costs that are associated with prosecution.
- If the Agency discovers that any person, domestic or foreign, has violated Federal criminal law, the information will be given to the Attorney General of the United States.

Section 14: TRANSFERS OF FUNCTIONS

- The authority of the Federal Trade Commission under Federal privacy law will be transferred to the Agency, but no Federal Trade Commission employee will be forced to move to the Agency.
- This title shall not be construed as limiting or affecting the authority of the Federal Trade Commission (including its authority with respect to large data aggregators) under the Federal Trade Commission Act, other than the authority under a Federal privacy law.
- This title shall not be construed as limiting or affecting the authority of the Consumer Financial Protection Bureau.

Section 15: AUTHORIZATION OF APPROPRIATIONS

- There are authorized to be appropriated to the Agency such sums as necessary.

Section 16: PRESERVATION OF STATE LAW

- This Act does not preempt existing state law.
- Any State Attorney General can bring civil action against a person that lives under their jurisdiction and is found in violation of this act. This Act cannot be construed as altering any State laws or limiting their authority.

Section 17: INSPECTOR GENERAL

- Amends the Inspector General Act of 1978 to create an Office of the Inspector General within the Data Protection Agency.