S. 3

To establish a robust Data Protection Agency and comprehensive regulations to safeguard personal data and protect individuals' privacy rights in the United States.

IN THE SENATE
July 18, 2023

Mr. Charest-Harris (for himself,) introduced the following bill, on behalf of the Rosen Administration, as authored by President Rosen and Senator Charest-Harris;

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

A BILL

1. SECTION 1. SHORT TITLE

1.1. This Act shall be cited as the "Data Protection Act" or the “DPA” for short.

2. SECTION 2. PERSONAL DATA

2.1. For the purposes of this Act, the term "Personal Data" shall mean any information that pertains to an identified or identifiable natural person, including, but not limited to, personal identifiers such as name, address, social security number, biometric data, genetic data, health data, racial or ethnic origin, religious or philosophical beliefs, political opinions, and sexual orientation.

3. SEC. 3. COLLECTION AND CONSENT OF PERSONAL DATA

3.1. Non-Federal Entities— Any entity not of a federal nature, inclusive of private corporations, shall be required to obtain explicit consent from individuals prior to the collection of their Personal Data, except in circumstances where such collection is necessitated by federal agencies in accordance with their legal obligations.

3.2. Service Refusal— Non-federal entities may refuse service that is contingent upon the collection of Personal Data without consent, provided that the necessity of such data collection for the provision of the service can be demonstrated in a court of law.

3.3. Federal Entities— Federal entities are exempted from the requirement of obtaining consent for the collection of Personal Data when such collection is necessary for the provision of a service. However, such entities must inform the individual of the collection and specify the Personal Data being collected.

3.3.1. A copy of this information shall be forwarded to the Data Protection Agency.

4. SEC. 4. ESTABLISHMENT OF THE DATA PROTECTION AGENCY

4.1. Establishment and Structure— The Data Protection Agency (DPA) is hereby established as an independent agency under the authority of the Department of Justice.

4.1.1. The DPA shall be headed by a General Director, appointed by

the President with the advice and consent of the Senate.

4.2. Powers and Responsibilities— The DPA shall have the power and responsibility to enforce and implement the provisions of this Act, conduct investigations, issue regulations, provide guidance to ensure compliance with this Act, impose fines, penalties, and sanctions for violations of this Act, promote public awareness and education regarding data protection and privacy rights, and cooperate and coordinate with federal agencies, state authorities, and international organizations to facilitate the enforcement of data protection laws.

5. SEC. 5. FUNDING

5.1. The sum of $5,000,000,000.00 is hereby authorized and appropriated from the general budget to establish the Data Protection Agency. The budget of the Data Protection Agency shall be part of the general budget and subject to annual or monthly appropriations.

6. SEC. 6. FINES

6.1. Any person or organization found to be in violation of this Act may be subject to fines, penalties, or sanctions as determined by the DPA. The DPA shall establish a graduated system of fines based on the nature, gravity, and duration of the violation. Gross violations of this Act may result in criminal prosecution, punishable by imprisonment, in addition to fines and penalties.

7. SEC. 7. ENFORCEMENT

7.1. Cooperation with Law Enforcement— The DPA shall collaborate and share information with law enforcement agencies to assist in the investigation and prosecution of criminal offenses related to personal data protection, as defined by Sec. 9 of this Act.

7.1.1. The DPA shall establish procedures to ensure the confidentiality and secure handling of shared information.

7.2. Judicial Review— Any person or organization aggrieved by a decision of the DPA may seek judicial review in a court of competent jurisdiction.

7.2.1. Such a court of competent jurisdiction shall have the power to review the decision and provide appropriate remedies, including injunctions, to enforce compliance with this Act.

8. SEC. 8. WITHDRAWAL OF CONSENT

8.1. Right to Withdraw Consent— Individuals shall have the right to withdraw their consent for the collection, storage, and processing of their Personal Data at any time, unless such data collection is necessary for compliance with legal obligations imposed on federal agencies.

8.2. Process for Withdrawal of Consent— Non-federal entities shall provide individuals with a clear and accessible mechanism to withdraw their consent for the collection, storage, and processing of Personal Data. The process for withdrawal of consent shall be simple, free of charge, and readily available to individuals. Non-federal entities shall not impose any undue obstacles or conditions on the exercise of this right. Upon receipt of a withdrawal of consent, non-federal entities shall promptly cease the collection, storage, and processing of the individual's Personal Data, except to the extent required by applicable laws or legitimate overriding interests.

8.3. Effect of Withdrawal of Consent— Upon the withdrawal of consent, non-federal entities shall no longer have the legal basis to collect, store, or process the Personal Data of the individual who has withdrawn their consent. Non-federal entities shall take reasonable measures to ensure that the withdrawn consent is duly implemented, and any Personal Data collected based on the previous consent shall be promptly deleted or anonymized, unless retention is required by law.

8.4. Non-Discrimination— Non-federal entities shall not discriminate against individuals who exercise their right to withdraw consent. Such entities shall not deny access to services, products, or benefits, or impose any unfair conditions or disadvantages based on the withdrawal of consent, except where the collection of Personal Data is vital to the provision of the service, as determined in accordance with Section 3.2.

8.5. Communication of Withdrawal of Consent— Non-federal entities shall inform individuals about their right to withdraw consent and provide clear instructions on how to exercise this right. This information shall be readily available through privacy notices, websites, or other appropriate means. The Data Protection Agency shall promote public awareness of the right to withdraw consent and provide guidelines to non-federal entities on complying with the obligations outlined in this

section.

9. SEC. 9. COLLECTION OF PERSONAL DATA IN CRIMINAL INVESTIGATIONS

9.1. Personal Data in Criminal Investigations— In the context of a criminal investigation, federal agencies may collect Personal Data without explicit consent from individuals, provided that such collection is necessary and proportionate to the investigation and is carried out in accordance with applicable laws and regulations. Personal Data collected in criminal investigations shall be limited to what is necessary for the purpose of the investigation and shall be handled with utmost care to ensure the protection of privacy rights.

9.2. Process for Collection of Personal Data in Criminal Investigations— Federal agencies conducting criminal investigations shall adhere to the following process for the collection of Personal Data—

9.2.1. JUSTIFICATION.— Federal agencies shall justify the necessity and proportionality of collecting personal data in relation to the criminal investigation.

9.2.2. LEGAL BASIS.— Personal data collection shall be based on a clear legal basis, such as a court-issued warrant, subpoena, or other authorized legal instruments.

9.2.3. MINIMIZATION.— Personal data collection shall be limited to what is necessary and relevant to the criminal investigation, avoiding the collection of excessive or unrelated information.

9.2.4. TRANSPARENCY.— Federal agencies shall, to the extent permitted by law, provide individuals subject to data collection with clear and accessible information about the purpose, scope, and duration of the data collection.

9.2.5. SECURITY.— Personal data collected in criminal investigations shall be handled and stored securely, ensuring appropriate measures are in place to prevent unauthorized access, use, or disclosure.

9.2.6. RETENTION AND DISPOSAL.— Personal data collected in criminal investigations shall be retained only for as long as necessary for the purpose of the investigation, and shall be disposed of in a secure manner once no longer needed, unless retention is required by law.

9.2.7. ACCOUNTABILITY.— Federal agencies shall maintain proper records of the personal data collected in criminal investigations and be accountable for their actions in accordance with applicable laws, regulations, and internal policies.

9.3. The Data Protection Agency shall oversee and ensure compliance with the process outlined in this section, conducting periodic audits and investigations to safeguard individuals' privacy rights in the context of criminal investigations.

10. SEC. 10. EFFECTIVE DATE

10.1. Effective Date— This Act shall take effect 90 days after its enactment.

10.2. Applicability— The provisions of this Act shall apply prospectively to the collection, storage, and processing of personal data from the effective date onward.

10.3. Existing Data— Existing data held by non-federal organizations shall be subject to the provisions of this Act within one year of the effective date.

10.4. Federal Compliance— Federal agencies and departments shall comply with the provisions of this Act immediately upon its effective date.

10.5. Operation Date— The Data Protection Agency shall be operational within one year of the effective date.