Brianne K. Nadeau
Councilmember, Ward 1

Statement of Introduction
DC Government Data Privacy and Protection Act of 2026

April 24, 2026

Today, along with Councilmembers Christina Henderson, Janeese Lewis George, and Zachary Parker, I am introducing the "District of Columbia Data Privacy and Protection Act of 2026". This legislation establishes comprehensive privacy protections governing the collection, use, sale, and disclosure of individuals' personal data by District government agencies and third parties and provides individuals with rights over their personal data. The bill establishes a Chief Privacy Officer (CPO) within the Office of the Chief Technology Officer (OCTO) to oversee compliance and implementation across agencies.

Data privacy laws for government are essential to safeguarding residents' personal information and preventing misuse by unauthorized actors. Public-sector databases have increasingly become targets for cybercriminals, who seek to exploit sensitive information for financial gain, identity theft, or unauthorized access to government systems.[1] For example, the 2023 breach of the District of Columbia Board of Elections exposed voter registration data after attackers gained access to internal systems.[2]

The Committee on Public Works & Operations learned through oversight of OCTO that the Department of Motor Vehicles had sold user data to LexisNexis.[3] This sale occurred without clear, informed consent from residents, and without prior approval from OCTO about what information, if any, could be securely sold. Any sale of data should be transparent and performed with clear guidelines and limitations for both the agency and the third party.

When handled responsibly and securely, data is a powerful tool for improving government services, serving as an aid to agencies in identifying disparities in service delivery, evaluating program effectiveness, and promoting community advocacy.[4] This legislation establishes clear rules and rights to safeguard individuals' data, promoting responsible data usage so that our government can continue to utilize data-informed service delivery for District residents and visitors.

---

[1] Data Security Laws | State Government
[2] Update: D.C. Elections Board Says Hack Impacted Less Than 4,000 Voters | DCist
[3] Testimony of Shauna Dillavou, Brightlines, at the FY24 Performance Oversight Hearing for the Office of the Chief Technology Officer
[4] Building Trust in Data Requires Building Trust with Communities | DQC

Councilmember Christina Henderson

Councilmember Brianne K. Nadeau

Councilmember Zachary Parker

Councilmember Janeese Lewis George

A BILL

IN THE COUNCIL OF THE DISTRICT OF COLUMBIA

To establish comprehensive privacy protections governing the collection, use, and disclosure of covered individuals' personal data by District government agencies, to establish requirements for third party's handling personal data of covered individuals, to provide covered individuals with enforceable rights regarding their personal data, and to establish a Chief Privacy Officer in the Office of the Chief Technology Officer.

BE IT ENACTED BY THE COUNCIL OF THE DISTRICT OF COLUMBIA, That this act may be cited as the "District of Columbia Government Data Privacy and Protection Act of 2026".

Sec 2. Definitions.

For the purposes of this act, the term:

(1) "Affirmative consent" means a clear affirmative act signifying a covered individual's freely given, specific, informed, and unambiguous agreement to the processing of personal data for a purpose that is not required by law or necessary to provide a government service requested by the individual.

(2) “Agency” shall include agencies and independent agencies as defined in section 1, paragraphs (1) and (13) of the District of Columbia Government Comprehensive Merit Personnel Act of 1978, effective March 3, 1979 (D.C. Law 2-139, D.C. Official Code § 1–603.01).

(3) “Authenticate” means to use reasonable means to determine that a request to exercise any of the rights afforded under this act is being made by, or on behalf of, the covered individual who is entitled to exercise such rights with respect to the personal data at issue.

(4) “Collect” and “collecting” mean gathering, obtaining, receiving, accessing, or otherwise acquiring personal data of covered individuals by an agency.

(5) “Covered individual” means an individual or natural person who currently resides in the District of Columbia, is currently employed in the District of Columbia, or who accesses, uses, or otherwise interacts with District services, programs, systems, or benefits provided by a District agency, regardless of the individual’s place of domicile or permanent residence.

(6) “Personal data” means any information that is linked to an identified or identifiable covered individual. “Personal data” does not include de-identified or aggregated data, or publicly available information.

(7) “Process” or “processing” means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the use, storage, disclosure, analysis, deletion or modification of personal data.

(8) “Sale of personal data” means the exchange of personal data for monetary or other consideration by an agency to a third party.

(9) “Sensitive data” means personal data that includes:

(A) Racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, status as pregnant, sex life, sexual orientation, gender identity, union membership, income level or indebtedness, or citizenship or immigration status;

(B) Health data or medical information;

(C) Genetic or biometric data;

(D) Personal data of a covered individual that is under the age of 18; and,

(E) A government-issued identifier, including a Social Security number, passport number or driver's license number, that is not required by law to be displayed in public.

(10) “Third party” means any non-governmental entity, external entity, or person that receives, collects, stores, processes, accesses, or transfers personal data from, on behalf of, or at the direction of a District government agency.

(11) “Transfer” means to disclose, release, disseminate, make available, license, rent, or share personal data to a third party orally, in writing, electronically, or by any other means.

Sec 3. Duties of agencies.

(a) An agency that processes personal data shall:

(1) Limit the collection, processing, and transfer of personal data to what is reasonably necessary to provide or maintain:

(A) A specific product or service requested by the covered individual to whom the data pertains including routine administrative, operational, or service-provision activities necessary to deliver the government service requested by the covered individual; or

(B) A communication by the agency to the covered individual that is reasonably anticipated within the context of the relationship between the agency and the covered individual.

(2) Not collect, process, or transfer sensitive data concerning a covered individual except when such collection, processing, or transfer is strictly necessary to provide or maintain a specific product or service requested by the covered individual to whom the sensitive data pertains.

(3) Not sell sensitive data of any covered individual.

(4) Not sell personal data of any covered individual without obtaining the covered individual's affirmative, informed consent.

(5) Not transfer personal data concerning a covered individual to a third party without obtaining the covered individual's affirmative consent.

(6) Establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data.

(7) Provide a mechanism for a covered individual to revoke the covered individual's affirmative consent and cease to process the data as soon as practicable, but not later than 45 days after the receipt of such request.

(8) Direct to a clear, accessible privacy notice, as established by the Chief Privacy Officer ("CPO"), regarding data practices and rights of covered individuals that includes:

(A) How a covered individual may exercise their rights, including how a covered individual may appeal an agency decision;

(B) The categories of personal data collected and processed by the agency, including a separate list of categories of sensitive data collected and processed by the agency;

(C) The purpose for collecting and processing each category of personal data;

(D) The categories of personal data that the government agency transfers to third parties, if any, and the purposes for those transfers;

(E) The length of time the agency retains each category of personal data; and,

(F) Information on how a covered individual may exercise the right to opt out of such sales or processing.

(9) Not deny services or benefits to a covered individual for exercising rights under this act.

(b) Agencies may only share personal data with third parties if:

(1) The sharing is necessary for a governmental purpose;

(2) The personal data does not include sensitive data, unless required by law; and,

(3) The third party agrees to comply with equivalent or greater privacy protections, including:

(A) The ability of the agency to request that the third party delete or return all personal data to the agency as requested, unless retention of the personal data is required by law;

(B) Providing to the agency all information in its possession necessary to demonstrate the third party's compliance with the obligations of this section;

(C) Only processing and transferring the data it receives from the agency to the extent necessary to provide a service requested by the agency; and

(D) Detailing the type of data subject to processing and the duration of the processing and data retention.

(4) The sharing is documented and subject to audit.

(c) Nothing in this section shall be construed to restrict an agency's ability to:

(1) Comply with District laws and regulations;

(2) Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal or other governmental authorities, except as prohibited by District law;

(3) Provide a product or service specifically requested by the covered individual;

(4) Assist another agency with any of the obligations under this act;

(5) Collect or process personal data to accomplish the agencies' mission and core functions; and,

(6) Ensure the data security and integrity of personal data as required by this act, protect against spam, or protect and maintain networks and systems, including through diagnostics, debugging, and repairs.

Sec 4. Requirements of third parties.

(a) A contract between an agency and a third party shall govern the third party's data processing procedures with respect to processing performed on behalf of the agency. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The third party shall adhere to the instructions of the agency and only process and transfer the data it receives from the agency to the extent necessary

to provide a service requested by the agency, as set out in the contract. The contract shall also require that the third party:

(1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

(2) At the agency's direction, delete or return all personal data to the agency as requested at the end of the provision of services, unless retention of the personal data is required by law;

(3) Upon the reasonable request of the agency, make available to the agency all information in its possession necessary to demonstrate the third parties compliance with the obligations under this act;

(4) After providing the agency an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the third party with respect to the personal data; and,

(5) Be prohibited from combining personal data that the third party receives from or on behalf of an agency with personal data that the third party receives from or on behalf of another person or collects from the interaction of the third party with an individual.

(b) A third party shall establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue.

(c) Any third party that receives personal data from an agency shall, upon receiving a request for such data from any federal, state, or local government entity:

(1) Review the legal validity of the request, including whether it is lawfully issued, within the authority of the requesting entity, and narrowly tailored to the data sought; and,

(2) Challenge the request in a court of competent jurisdiction where the third party has a reasonable basis to believe that the request is overbroad, not supported by sufficient legal process, or inconsistent with applicable law or contractual obligations.

(d)(1) A third party shall not disclose personal data in response to a government request unless the request is accompanied by a warrant, subpoena, court order, or another form of legally binding process recognized under applicable law.

(2) The third party shall promptly notify the originating agency of any government request for data, unless legally prohibited. Where not prohibited by law, the third party shall make reasonable efforts to notify affected individuals prior to disclosure.

(3) If disclosure is required, the third party shall disclose only the minimum amount of data necessary to comply with the request, take reasonable steps to narrow or modify the request, and seek protective orders or confidentiality agreements where appropriate.

(e) A third party may not voluntarily provide personal data to any government entity absent a legally binding request or express authorization from the originating agency and consistency with District law.

(f) Third parties shall maintain records of all government requests received and provide periodic reports to the agency, including the number of requests, the type of legal process used, and whether requests were challenged.

(g) All agency contracts involving the transfer of personal data shall require compliance with this section as a material term of the agreement.

(h) Failure to comply with this section shall constitute a material breach of contract and may result in termination, damages, and debarment from future District contracts.

Sec 5. Rights of covered individuals

(a) Covered individuals shall have the right to:

(1) Confirm whether or not an agency is collecting or processing the covered individual's personal data and obtain:

(A) Categories of data collected;

(B) Purpose of processing; and,

(C) Categories of recipients;

(2) Obtain a copy of the personal data collected or processed;

(3) Correct inaccuracies in the covered individual's personal data;

(4) Delete personal data provided by, or obtained about, the covered individual, unless the data is required by law to be retained; and,

(5) Obtain from an agency a list of specific third parties, other than natural persons, to which the agency has transferred or sold:

(A) The covered individual's personal data; or,

(B) Any personal data.

(6) Opt-out of the transfer or sale of personal data for purposes not required by law or necessary to provide a government service.

(b) (1) Agencies shall respond to verified requests within sixty days after receipt of the request.

(2) The agency shall inform the covered individual within forty-five days after receipt of the request of any justification for declining to provide the requested information and provide instructions for how to appeal the decision.

(c) A covered individual may exercise rights under this section by a secure and reliable means established by CPO and described to the covered individual in the agency's privacy notice.

(d) Information provided in response to a covered individuals' request shall be provided by an agency once per covered individual during any four-month period.

(e) Nothing in this section shall be construed to provide a basis for a private right of action or any other remedy, claim, or cause of action for any violation of this act. The CPO and the Office of the Attorney General for the District of Columbia ("OAG") shall have authority to investigate and enforce this act.

Sec 6. Chief Privacy Officer.

(a) There is established within the Office of the Chief Technology Officer ("OCTO") a Chief Privacy Officer ("CPO") that shall be appointed by the Chief Technology Officer ("CTO"). The CPO shall be a member in good standing with the DC Bar.

(b) The CPO shall:

(1) Be directly responsible for coordinating the related responsibilities of cybersecurity, data governance, and privacy.

(2) Develop and implement written policies and procedures to ensure the privacy and security of covered individuals' personal data;

(3) Ensure compliance with applicable federal and state laws and regulations relating to data privacy;

(4) Issue written findings, recommendations, or directives to an agency to ensure compliance with this act, including requiring the agency to modify its practices, implement safeguards, or cease unlawful data processing activities, and may coordinate with OAG to ensure compliance;

(5) Conduct or require privacy impact assessments for applicable information technology systems or programs;

(6) Establish government-wide standards for the collection, use, retention, and disclosure of covered individuals' personal data and sensitive data;

(7) Coordinate with the Chief Data Officer, Chief Information Officer, or equivalent positions, regarding the investigation and notification of breaches of personal data;

(8) Provide training and guidance to agencies regarding data privacy requirements and best practices;

(9) Conduct periodic reviews of agency practices relating to the handling of personal data;

(10) Receive and resolve complaints;

(11) Receive and resolve disputes among agencies related to data privacy in writing;

(12) Participate in audits related to data privacy conducted by the District of Columbia Auditor and the Office of the Inspector General;

(13) Provide an annual report to the CTO to publish in August of every year beginning after the effective date of this act, and

(14) Advise the CTO on matters relating to privacy and data protection.

(d) The CPO shall, in partnership with agencies:

(1) Develop a process by which covered individuals may appeal data request decisions made by agencies; and,

(2) Develop a data privacy bill of rights, accessible to covered individuals on the CPO's webpage, and directly linked on webpages of agencies that collect or process personal data of covered individuals.

Sec 7. Enforcement

(a) The OAG may issue written findings, recommendations, or directives to an agency to ensure compliance with this act, including requiring the agency to modify its practices, implement safeguards, or cease unlawful data processing activities.

(b) The OAG may require an agency to enter into a compliance agreement that includes specific corrective actions, timelines for implementation, and ongoing monitoring or reporting obligations.

(c) An agency found to be in violation of this act may be subject to appropriate administrative remedies under District law, including required remediation, changes to data practices, training requirements, or other corrective measures designed to ensure future compliance.

(d) The OAG may require periodic reporting from agencies regarding their data practices, risk assessments, data sharing activities, and compliance with this act.

(e) In determining the appropriate remedy or corrective action, the OAG may consider the nature and seriousness of the violation, the number of individuals affected, the sensitivity of the data, the risk of harm, whether the violation was part of a pattern or practice, and whether the violation resulted from human or technical error.

(f) Nothing in this section shall be construed to limit any authority of the OAG under District law or to impair the application of any other law governing the conduct of District agencies.

Sec 8. Applicability

(a) This act shall apply upon the date of inclusion of its fiscal effect in an approved budget and financial plan.

(b) The Chief Financial Officer shall certify the date of the inclusion of the fiscal effect in an approved budget and financial plan, and provide notice to the Budget Director of the Council of the certification.

(c)(1) The Budget Director shall cause the notice of the certification to be published in the District of Columbia Register.

(2) The date of publication of the notice of the certification shall not affect the applicability of this act.

Sec. 9. Fiscal impact statement.

The Council adopts the fiscal impact statement in the committee report as the fiscal impact statement required by section 4a of the General Legislative Procedures Act of 1975, approved October 16, 2006 (120 Stat. 2038; D.C. Official Code § 1-301.47a).

Sec. 10. Effective date.

This act shall take effect following approval by the Mayor (or in the event of veto by the Mayor, action by the Council to override the veto) and a 30-day period of congressional review as provided in section 602(c)(1) of the District of Columbia Home Rule Act, approved December 24, 1973 (87 Stat. 813; D.C. Official Code § 1-206.02(c)(1)).