Government of the District of Columbia
Office of the Chief Financial Officer

Glen Lee
Chief Financial Officer

MEMORANDUM

TO:	**The Honorable Phil Mendelson** **Chairman, Council of the District of Columbia**
FROM:	**Glen Lee** **Chief Financial Officer**
DATE:	**November 18, 2026**
SUBJECT:	**Fiscal Impact Statement – District of Columbia Government Data Privacy and Protection Act of 2026**
REFERENCE:	**Bill 26-670, Draft Committee Print as provided to the Office of Revenue Analysis on November 14, 2026**

Conclusion

Funds are not sufficient in the fiscal year 2027 through fiscal year 2030 budget and financial plan to implement the bill. The bill costs $584,000 in fiscal year 2027 and $2.8 million across the financial plan period.

Background

The bill:

- Establishes a Chief Data Privacy Officer (CDPO) in the Executive Office of the Mayor (EOM).
- Convenes a data privacy working group.
- Requires phased implementation standards for data privacy.
- Establishes comprehensive privacy protections governing the processing of covered individuals' personal data by District government agencies[1]. Under the bill, a covered individual is a natural person who currently resides in the District, who is currently employed in the District, 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

[1] The bill defines this to 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). The term does not include the District of Columbia Health Benefit Exchange Authority established by section 3 of the Health Benefit Exchange Authority Establishment Act of 2011, effective March 2, 2012 (D.C. Law 19-94; D.C. Official Code § 31-3171.02).

domicile or permanent residence. A parent, guardian, custodian, or other primary care giver may exercise the rights of a covered individual under the age of 18 to the extent authorized by applicable federal or District law.[2]

- Establishes requirements for service providers, authorized data recipients, and third parties processing personal data of covered individuals.
- Provides covered individuals with enforceable rights regarding their personal data and outlines exemptions.
- Creates oversight and enforcement mechanisms for data privacy.

The bill designates the CDPO in EOM as the District's primary advisor on data privacy, protection, and compliance matters. Within two years of taking office, the CDPO must conduct an audit of all publicly accessible District datasets and coordinate remediation of improperly disclosed information. Under the bill, the CDPO:

- Coordinates with the Office of the Chief Technology Officer (OCTO) on cybersecurity, data governance, privacy issues, and personal data breach investigations and notifications.
- Develops government-wide data privacy policies and procedures, including a publicly accessible Data Privacy Bill of Rights based on recommendations of the Data Privacy Working Group, which is established by the bill.
- Coordinates the development and review of agency-specific privacy policies, with privacy information posted on agency websites.
- Provides agencies with training, guidance, and best practices on data privacy requirements.
- Works with agency data privacy officers to oversee compliance and address agency data processing and privacy matters. The bill requires agencies to designate a data privacy officer ("privacy officer") to oversee agency compliance with the bill's provisions and coordinate with the CDPO on the agency's data privacy and practices. The privacy officer may be a new position or added to the duties of an existing filled position.
- Conducts periodic reviews of agency data practices and requires additional reporting from high-risk agencies or those with repeated compliance issues.
- Issues findings, recommendations, and directives to enforce compliance, including requiring agencies to modify practices, implement safeguards, or cease unlawful data processing, in coordination with OCTO and the Office of the Inspector General (OIG), when necessary.
- Ensures compliance with applicable federal and District data privacy laws and regulations.
- Assists agencies in resolving escalated complaints from covered individuals regarding personal data practices.
- Conducts or requires privacy impact assessments for applicable information technology systems and programs in partnership with OCTO.
- Participates in privacy audits conducted by the District Auditor and the OIG.
- Establishes, with OCTO, minimum anti-scraping standards[3] for agency portals containing personal data.

[2] Nothing in the bill shall be construed to alter or supersede the rights, limitations, or requirements applicable to a parent, guardian, custodian, other primary care giver or eligible students under the Family Educational Rights and Privacy Act of 1974, approved August 21, 1974 (88 Stat. 571; 20 U.S.C. § 1232g), and any regulations issued pursuant to this bill.

[3] **Data scraping** is a technique where a computer program extracts data from human-readable output coming from another program. https://en.wikipedia.org/wiki/Data_scraping

The bill also requires the CDPO to prepare a recurring District Data Privacy Progress Report ("progress report") for the Mayor and Council . The inaugural report is due within two years of the Data Privacy Working Group ("Working Group") report[4] or by November 15, 2031. The bill requires the progress report to include:

- Planned privacy education and training materials; recommendations on balancing transparency, privacy, and data protection.
- Proposed updates to privacy policies, governance structures, legislative or regulatory language, and implementation timelines.
- Results of agency privacy reviews and identified compliance issues.
- Recommendations for improving the District's artificial intelligence (AI) governance framework, including privacy and security risks, compliance, transparency, human oversight, industry standards, and protections for covered individuals.

The bill requires the CDPO to develop and maintain a government-wide artificial intelligence (AI) governance framework that addresses necessity, privacy risk, security, transparency, human oversight, and personal data protections. The CDPO must solicit public input and technical, legal, civil rights, privacy, and operational expertise before issuing AI standards. The AI framework should be reviewed and updated through the progress report. The bill charges the CDPO with approving or disapproving agency proposals to use personal data for the training, development, operation, or deployment of AI systems, in consultation with OCTO.

The bill requires the CDPO establish a Working Group composed of representatives from District agencies that handle large amounts of personal data; district agencies and government entities that use, or are considering using, data collection technologies; external stakeholders and experts with knowledge of information technology, data security, privacy, consumer protection, and government privacy practices; and civil liberties organizations. The bill authorizes the CDPO to convene additional meetings of the Working Group limited to agencies to discuss internal documents and sensitive sets of data or practices relating to the requirements of the bill. The bill limits what may be discussed only to topics that would present liabilities, exposure, or compromise other sensitive information. The bill requires the Working Group prepare a report and recommend strategies for creating and maintaining an effective District data privacy framework.[5]

The bill requires the Working Group report address implementation, including realistic timelines; rules governing the collection, use, retention, transfer, and AI-related processing of personal data; potential exemptions; expanded rights for covered individuals to access, correct, delete, de-identify, or challenge the use of their data; agency responsibilities and procedures for handling requests; the

[4] The Working Group hold its first meeting within 120 days of the CDPO's appointment; submit its findings and recommendations to the CDPO and the Council committee with jurisdiction within two years of the CDPO's appointment or by January 15, 2029; and transmit the report's findings via the CDPO to the Mayor and Council within 60 business days, or by March 16, 2029.

[5] The bill requires the Working Group to: develop appropriate frameworks for governing the processing activities described in the bill; identify the legitimate governmental functions served by the processing activities permitted under the bill, and the privacy implications of said activities; recommend strategies to empower covered individuals to protect and control their personal data; enable purposeful information use and sharing among agencies; account for differences in an agency's resources, capabilities, populations served, data types, and existing data privacy practices; and review statutory provisions related to governmental data privacy and records management to identify conflicts and gaps in data privacy law and standardize language.

content and transparency requirements of agency privacy notices and the District's Data Privacy Bill of Rights; and any additional recommendations identified by the Working Group and the CDPO to strengthen the District's data privacy framework.

The bill requires the Working Group hold its first meeting within 120 days of the CDPO's appointment; submit its findings and recommendations to the CDPO and the Council committee with jurisdiction within two years of the CDPO's appointment or by January 15, 2029; and transmit the report's findings via the CDPO to the Mayor and Council within 60 business days, or by March 16, 2029, which includes the Working Group's recommendations, an independent analysis outlining implementation next steps, and an explanation of any recommendations the CDPO does not support or proposes alternatives to, including the rationale for those positions.[6]

The bill phases in requirements for service providers, data recipients, and third parties by requiring the CDPO to develop and distribute standardized contract and data-sharing agreement language within 90 days of taking office, directing agencies to create agency-specific templates within 210 days of the CDPO taking office, and requiring agencies to incorporate those provisions into all new agreements and any existing agreements that are materially modified to expand their scope after the 210-day implementation deadline. Under the bill, agreements executed before the 210-day implementation deadline, and not subsequently modified, are exempt from the new requirements. The bill requires the CDPO, in consultation with the Working Group, to develop a phased implementation plan for the bill's remaining substantive provisions, giving agencies no more than two years after the Working Group report is submitted to understand the requirements; build the necessary technological, operational, and administrative capabilities; update existing data-sharing agreements and policies; and establish processes for responding to individuals' requests and complaints. The CDPO must then formally set and publish implementation dates for these requirements in the District of Columbia Register and on the CDPO's website.[7]

The bill subjects agency duties to the bill's phased implementation schedule. Under the bill, agencies that process personal data must establish and maintain administrative, technical, and physical security safeguards consistent with the National Institute of Standards and Technology Cybersecurity Framework or an equivalent standard; designate a qualified privacy officer, appointed by the agency's Director, to oversee compliance and coordinate with the CDPO; and maintain a clear and accessible website privacy page describing the agency's privacy practices, individuals' rights and how to exercise them, a link to the District's Data Privacy Bill of Rights, and any additional requirements established by the CDPO and recommended by the Working Group. The bill restricts agencies from denying services, benefits, or otherwise discriminating against individuals for

[6] Nothing in this section of the bill shall be construed to require the publication of information that reveals a data security vulnerability of the District government. To the extent the findings and recommendations of the Working Group could be used to identify and exploit data security vulnerabilities of the District government if made public, the bill requires CDPO omit such findings and recommendations from any public reports but must communicate them through an in-person briefing or other secure method to the Mayor and the Council committee of jurisdiction.

[7] No requirement under this bill is to be construed to apply retroactively to processing, disclosures, contracts, or data-sharing agreements completed before the applicable implementation dates established by the CDPO, except where necessary to prevent an ongoing violation of the bill's provisions.

exercising their privacy rights[8]; prohibits the sale or improper acquisition of personal data[9]; requires the prompt reporting of security breaches[10]; and restricts disclosures of personal data to federal entities unless legally authorized or required[11]. The bill also limits agencies' transfer of personal data to a service provider, authorized data recipient, or third party pursuant to a written contract that includes the requirements set forth under sections 7, 8, and 9, and subject to the recommendations of the Working Group and standards established by the CDPO. It restricts agencies' processing of personal data to the minimum amount necessary to accomplish a specified purpose permitted under this act, requires that agencies adhere to data minimization principles, and limits how agencies may process personal data they receive from a third party.

The bill authorizes agencies to transfer personal data to service providers, authorized recipients, or third parties only for fraud prevention, security, identity verification, or responding to fraud, identity theft, security incidents, or illegal activity, and only when:

- The data shared is limited to what is reasonably necessary.
- The data is not sold or transferred to data brokers or used for another entity's independent commercial purposes.
- The data is not used for marketing, profiling, or other secondary purposes.
- The data is deleted or de-identified once the fraud-prevention or security purpose has been fulfilled.

The bill specifies that the exception does not allow bulk publication of personal data or the creation or enhancement of commercial profiles using personal data. Agencies must also comply with any additional privacy and data governance duties established by the CDPO or recommended by the Working Group.

The bill establishes requirements for a service provider, which are subject to the phased implementation standards. The bill defines a service provider as person or entity that processes personal data on behalf of an agency pursuant to a contract that limits the processing of personal data to specified purposes and solely as necessary to provide goods and services to the agency. Under the bill, any contract between a District agency and a service provider must clearly define how the service provider may process data on the agency's behalf. The service provider may only process data as instructed by the agency and only as necessary to deliver the contracted services. The contract must require the service provider to:

- Restrict data access to authorized personnel who need it to perform approved functions.
- Maintain appropriate security safeguards to protect personal data.

[8] However, an agency may refuse a service or benefit if exercising a privacy right prevents the agency from obtaining information legally required to determine eligibility or provide the service.

[9] Agencies cannot sell, lease, license, rent, or otherwise provide personal data to outside entities in exchange for money for the recipient's independent commercial use or for purposes not authorized by the bill. Agencies also cannot buy personal data from data brokers or third parties to obtain information that they would be prohibited from collecting directly from the individual or through another legally authorized process.

[10] Agencies must notify OCTO within 24 hours of discovering a security incident involving District data. Agencies must submit a preliminary incident report within 30 days and a final report within 60 days describing affected data, remediation efforts, and prevention measures. For incidents involving personal or sensitive data, they also must notify the CDPO within 24 hours and provide the same reporting timeline in coordination with OCTO.

[11] Agencies cannot voluntarily share personal data with federal agencies upon request. Disclosures are only permitted when required by law, court order, subpoena, warrant, other legally binding process, or when necessary to administer a federally authorized or required program.

- Demonstrate compliance by providing records and information requested by the agency regarding data access, processing, and security practices.
- Delete or return personal data when services end or the data is no longer needed, unless retention is legally required.
- Prohibit data sales and advertising uses, including selling personal data or using it for marketing or commercial solicitation.
- Hold subcontractors to the same standards pursuant to the service provider's contract with the agency and notify the agency before granting them access to personal data. Limit processing to authorized purposes and minimize access to personal data by employees and third parties, whenever feasible.
- Restrict sensitive data processing to what is necessary for contracted services and expressly authorized by the agency, with no unnecessary retention.
- Obtain prior written approval from both the agency and the CDPO before using personal or sensitive data in any AI system.
- Prohibit the use of agency personal data to train, develop, fine-tune, operate, or deploy AI models, unless such use is directly related to the contracted service and explicitly authorized in the contract.

The bill requires service providers to notify the agency of any data breach or security incident involving agency data within 24 hours of discovery. In instances where a federal, state, or local government entity outside the District requests personal or sensitive data, the bill restricts the service provider from disclosing the data unless the request is supported by a warrant, subpoena, court order, or other legally binding legal process. Service providers must review the validity of the request to ensure it is lawful, and narrowly tailored; notify the originating agency within 24 hours of receiving the request, unless prohibited by law; provide at least 48 hours' notice before complying with the request, unless legally prohibited; and disclose only the minimum amount of data necessary to satisfy the request. The bill prohibits service providers from voluntarily sharing personal data with non-District government entities unless the contract specifically identifies the need for the transfer, identifies the recipients, specifies the categories of data to be disclosed, and is consistent with District law. Under the bill, a service provider's failure to comply constitutes a material breach of contract and may result in contract termination and/or debarment from future contracts awards.

The bill establishes requirements of an authorized data recipient, which are subject to the phased implementation standards. The bill defines an authorized data recipient as a person or entity that processes personal data from a District agency pursuant to a written data-sharing agreement for a specific and authorized research, evaluation, public-interest, community-service, or governmental function[12]. An authorized data recipient does not use or disclose personal data for any purpose other than specified in the written data-sharing agreement and authorized by law. Under the bill, any authorized data recipient that receives personal data from a District agency must sign a written data-sharing agreement and comply with privacy and data protection requirements. The agreement must require the authorized data recipient to:

- Restrict access to personal data only to authorized individuals who need it for the approved purpose.
- Maintain appropriate safeguards to protect the data based on its sensitivity.

[12] An authorized data recipient may be a nonprofit organization, research organization, educational institution, community-based organization, or other entity conducting research, analysis, evaluation, or other work in furtherance of a governmental function or public-interest purpose.

- Delete or return the data when the authorized purpose is complete, unless retention is legally required or permitted.
- Prohibit the sale of personal data.
- Not share data with third parties without the agency's written consent or other authorization in the data-sharing agreement.
- Use the data only for the approved purpose, such as research, evaluation, analysis, public-interest, community-service, or another specifically authorized use.
- Limit processing of sensitive data to situations where it is necessary for the authorized purpose, with the agreement specifically identifying the categories of sensitive data and why they are needed.
- Restrict AI use by prohibiting the use of agency personal data to train, develop, or fine-tune AI models or systems; and requiring prior written approval from both the agency and the CDPO before personal data can be entered into any AI system.

The bill requires authorized data recipients to notify the agency within 24 hours of discovering any data breach or security incident involving agency data. In instances where a government entity outside the District requests personal data, the bill restricts the authorized data recipient from disclosing the data unless the request is supported by a warrant, subpoena, court order, or other legally binding legal process. Service providers must notify the originating agency within 24 hours of receiving the requestand provide at least 48 hours' notice before complying with the request. The bill prohibits authorized data recipients from voluntarily sharing personal or sensitive data with non-District government entities unless the data-sharing agreement specifically identifies the need for the transfer, identifies the recipients, and specifies the categories of data to be disclosed.

The bill establishes requirements of a third party, which are subject to the phased implementation standards. The bill defines a third party to mean an external entity distinct from District government that processes personal data from or on behalf of a District government agency, including data brokers and national research firms, but excluding service providers, authorized data recipients, and entities or persons whose access to the personal data is expressly required or authorized by District law. Under the bill, any contract between a District agency and a third party must clearly govern how the third party may process agency data. The contract must specify the purpose, scope, duration, categories of personal data involved, and the rights and responsibilities of both parties. TThe contract must require the third party to:

- Restrict access to personal data to authorized individuals and ensure anyone handling data is bound by confidentiality obligations.
- Use data only for authorized purposes specified in the contract, data-sharing agreement, or otherwise authorized by the agency.
- Maintain appropriate safeguards to protect data.
- Demonstrate compliance by providing records and information regarding data access, processing, and security upon the agency's request.
- Delete or return data when it is no longer needed for the authorized purpose.
- Prohibit commercial use of the data, including selling data, using it for advertising, solicitation, or unrelated purposes.
- Restrict onward disclosure to other entities, subcontractors, or third parties unless necessary for the authorized purpose, governed by a written contract imposing equivalent obligations, and disclosed to the agency in the contract.
- Obtain prior approval from both the agency and the CDPO before entering data into any AI system.

- Prohibit the use of agency data to train, fine-tune, develop, operate, or deploy AI models or systems, with a written commitment to this restriction.

The bill restricts agencies from transferring sensitive data to third parties unless the disclosure is specifically authorized by law, required by court order, necessary to address a health or safety emergency , or permitted under statutory exemption. Like with service providers, third parties must review the validity of the request to ensure it is lawful, within the requesting entity's authority, and narrowly tailored; notify the originating agency within 24 hours of receiving the request; provide at least 48 hours' notice before complying with the request; and disclose only the minimum amount of data necessary to satisfy the request. The bill prohibits third parties from voluntarily sharing data with non-District government entities unless the contract specifically identifies the need for the transfer, identifies the recipients, and specifies the categories of data to be disclosed. Under the bill, a third party's failure to comply constitutes a material breach of contract and may result in contract termination and/or debarment.

The bill establishes rights for covered individuals, which are subject to the phased implementation standards that the bill requires the CDPO to develop in consultation with the Working Group. These implementation standards must include sufficient time for agencies to implement compliance (but not longer than two years from submission of the Working Group report). Subject to the phased implementation,a covered individual will have the right to:

- Once within any 12-month period, review how the agency processes their data.
- Once within any 6-month period, request correction or amendment of data that the covered individual demonstrates is inaccurate .[13]
- Once within any 12-month period, file a complaint regarding the agency's processing of their data, following procedures established by the CDPO and the Working Group.
- Receive notice about data collection at or before the time data is collected from them, in a manner prescribed by the CDPO and the Working Group.

The bill generally does not allow individuals to sue or obtain private remedies for violations. However, within 90 days of the phased 2-year implementation deadline of the Working Group report, a covered individual may bring a civil action against an agency for violations that occur on or after that date and causes the individual measurable harm. Under the bill, a lawsuit may seek damages, and/or judicial relief to stop, prevent, or remedy the violation. Before filing suit, the individual must provide the agency with a written description of the alleged violation and requested relief; file a complaint with the CDPO; and allow the agency 120 days to investigate and, if appropriate, resolve the issue. The bill authorizes the agency to resolve the matter by correcting the practice, providing the requested relief, or reaching an agreement with the individual.

The bill exempts certain information[14] from its requirements. The bill restricts federal entities from obtaining or using data held by a District agency unless it is necessary to carry out an existing

[13] Agencies may direct individuals to the entity responsible for maintaining or correcting the data when appropriate. Agencies are not required to change records maintained by another entity; alter records they are legally required to maintain; or modify records simply because the individual disagrees with the event, finding, or determination documented in the record.

[14] The information includes: protected health information under the Health Insurance Portability and Accountability Act ; data regulated under Family Educational Rights and Privacy Act ; emergency contact information; information necessary to administer benefits for another person related to the covered individual; information processed by Fire and Emergency Medical Services Department when needed to respond to emergencies; information processed by the Metropolitan Police Department or other public

government function authorized by law, regulation, or other binding authority; or access is required by federal law.

Federal entities remain subject to certain requirements of the bill unless federal law expressly preempts the requirement or the information falls within a specific exemption under the bill. When a District agency processes data that is subject to another federal privacy law, the data is exempt only to the extent necessary to avoid a conflict with federal law. The bill specifies that agencies cannot avoid compliance with the bill's provisions simply because federal privacy laws also apply. An agency is not exempt from the bill because it participates in a federal program or receives federal funding and any exemption applies only to the portions of processing or disclosure that must comply with federal requirements.

The bill authorizes OIG to oversee agency compliance with the data privacy law and recommend corrective actions when violations occur. The bill authorizes the OIG to independently audit, inspect, and investigate agencies for compliance, at its own discretion or at the Mayor's request. The bill authorizes the OIG to consider:

- The severity and nature of the violation;
- The number of people affected;
- The sensitivity of the data involved;
- The risk or occurrence of harm;
- Whether the violation was recurring;
- The duration of the violation; and
- The agency's efforts to prevent or correct the issue.

The OIG may require agencies to change data practices; implement safeguards; cease unlawful data processing; improve training; or take other measures to prevent future violations. Further, under the bill, the OIG may recommend that:

- Agencies with violations undergo annual operational audits of their privacy practices;
- Agencies enter into compliance agreements with the CDPO that specify corrective actions ; and
- Agencies provide remediation plans and submit to monitoring as needed.

Agencies subject to corrective actions must complete them by the deadlines recommended by the OIG and enforced by the CDPO, unless the CDPO grants an extension due to the complexity or nature of the required action.

safety agencies for emergency purposes, provided processing is limited to what is necessary, and the agency does not provide a covered individual's personal information to federal immigration authorities.

Financial Plan Impact

Funds are not sufficient in the fiscal year 2027 through fiscal year 2030 budget and financial plan to implement the bill. The bill costs $584,000 in fiscal year 2027 and $2.8 million across the financial plan period.

B26-670 - District of Columbia Government Data Privacy and Protection Act of 2026 Total Costs ($ in thousands)					
	FY 2027	FY 2028	FY 2029	FY 2030	**TOTAL**
Executive Office of the Mayor					
Salary[a]	$156	$212	$217	$221	$806
Fringe[b]	$24	$43	$44	$45	$155
Workstation, Technology, Equipment, Supplies, Licenses, Software[c]	$50	$5	$5	$5	$65
Metropolitan Police Department					
Salary[d]	$139	$190	$193	$197	$720
Fringe[e]	$25	$37	$38	$39	$139
Office of Tax and Revenue					
Salary[f]	$153	$208	$212	$216	$788
Fringe[g]	$37	$50	$51	$52	$190
TOTAL	$584	$744	$760	$775	$2,863

Table Notes:

(a) Salary for one E5, Midpoint Executive Service (DX) CDPO. Assumes annual 2.0 percent growth. Fiscal Year 2027 accounts for nine months of costs.
(b) Fringe rate of 20.2 percent. Assumes annual 2.35 percent growth. Fiscal Year 2027 accounts for nine months of costs.
(c) Includes one-time costs of $45,000 in fiscal year 2027.
(d) Salary for one Grade 15, Step 5 Legal Services (LS) Data Privacy Officer. Assumes annual 2.0 percent growth. Fiscal Year 2027 accounts for nine months of costs.
(e) Fringe rate of 19.5 percent. Assumes annual 2.35 percent growth. Fiscal Year 2027 accounts for nine months of costs.
(f) Salary for one Grade 16, Step 5 Data Privacy Officer. Assumes annual 2.0 percent growth. Fiscal Year 2027 accounts for nine months of costs.
(g) Fringe rate of 24 percent. Assumes annual 2.35 percent growth. Fiscal Year 2027 accounts for nine months of costs.

Executive Office of the Mayor

The bill requires the appointment of a CDPO within EOM as the District's primary advisor on data privacyThis position costs $180,000 in fiscal year 2027 and $961,000 over the financial plan period. EOM also requires $50,000 in fiscal year 2027 and $65,000 over the financial plan period for supplies including workstation, technology, equipment, licensing, software, and associated materials.

Metropolitan Police Department

Within 210 days, the bill requires the CDPO to direct agencies to create agency-specific templates and incorporate those provisions into all new agreements and any existing agreements that are materially modified to expand their scope after the 210-day implementation deadline. The bill provides an exemption for Metropolitan Police Department (MPD) related to emergencies. The bill requires MPD to modify its Records Management System (RMS) to support additional data management and review processes . The cost to the system is indeterminate, but will be considered and factored in during the period of time the Working Group develops its report. The bill will require personnel to evaluate whether specific investigative activities meet the statutory criteria for an exemption and whether information sharing is permitted under those criteria. Because investigations often involve the collection, review, and analysis of information before its relevance can be fully determined, compliance with these requirements will necessitate additional documentation, review, and oversight activities.

MPD anticipates increased administrative and operational workload associated with applying the new standards, monitoring compliance, determining future costs associated with modifications to its RMS, and implementing necessary system changes. MPD requires a Data Privacy Officer to support these responsibilities and ensure consistent application of the requirements across the agency. This position costs $164,000 in fiscal year 2027 and $858,000 over the financial plan period.

Office of Tax and Revenue

The bill does not provide an exemption for the Office of Tax and Revenue (OTR). The Recorder of Deeds is part of OTR and serves as the official repository for all land records, deeds, mortgages, liens, and similar public instruments in the District. These records are saved and made available for the public to view online. OTR's real property tax database also provides online access to real property information. The database permits a user to obtain property value, assessment roll, and other information for more than 200,000 parcels. Lastly, if a property owner is delinquent on their real property taxes or fees,the District seeks to collect the funds through the annual tax sale . This includes publication in local newspapers before the tax sale .

The bill requires OTR modify both the Recorder of Deeds database and the real property tax database. The cost to the system is indeterminate, but will be considered and factored in during the period of time the Working Group develops its report. OTR will require personnel to process any redactions for covered individuals and an estimate of the volume of covered individuals who may avail themselves to the removal of their information is indeterminate. Because the implementation falls outside of the financial plan period, the anticipated costs are not enumerated in this analysis. OTR requires a Data Privacy Officer to review OTR's current systems and databases, establish and maintain data privacy controls, coordinate compliance activities across OTR , develop a framework for redaction requests, monitor ongoing data protection , and determine how public access will be maintained . This position costs $190,000 in fiscal year 2027 and $978,000 over the financial plan period.

Office of the Attorney General

A private cause of action allows an individual or private entity to file a civil lawsuit to enforce a right, seek damages, or obtain an injunction. When a private individual or non-government entity files a civil lawsuit against the District, the Office of the Attorney General's (OAG) Civil Litigation Division (CLD) represents the District. Within 90 days of the two-year phased implementation deadline or

January 15, 2031, a covered individual can bring a civil action against an agency for data privacy violations. In 2025, OAG's CLD defended the District in over 900 cases. The volume of covered individuals who may avail themselves of the private right of action under the bill is indeterminate. The cost to defend the District is likewise indeterminate, but will be considered and factored in during the period of time the Working Group develops its report. OAG will require personnel for any increase in litigation volume. Because the implementation falls outside of the financial plan period, the anticipated costs are not enumerated in this analysis.