



Standard Operating Procedure

Privacy Procedures for Prohibition of the Sale of Personal Information in Contracts and Discouragement of the Resale or Rediscovery of Personal Record Information

Division: Legal and Legislative Division

Policy Area: Data Privacy, Contracting, Records Management,
Public Information, and Law Enforcement Information Sharing

Policy Drafter: Thomas R. Akas, Esq., Director, Legal and
Legislative Division

Approving Officer: Jeffrey A. Kelly, Executive Director

Effective Date:

Policy No. 1.01

Pages: 8

Revision date: 7/1/2026

Purpose: To establish internal procedures for the Alcohol, Tobacco, and Cannabis Commission (“ATCC”) to protect personal records, personal information, personally identifiable information, geolocation data, and other sensitive information collected, maintained, provided, or made available by the ATCC.

This policy is intended to comply with Md. Code Ann., State Gov’t § 10-1702, which requires governmental entities, in consultation with the Department of Information Technology (“DoIT”), to develop and publish procedures to prevent the sale and redisclosure of personal records and geolocation data in a way that harms the privacy of Maryland residents.

This policy directs ATCC employees on contract terms, vendor access, public records responses, data minimization, internal data sharing, incident reporting, and appropriate law enforcement information sharing.

Responsible Staff: The Director of the Legal and Legislative Division, the Procurement Officer, the Public Information Act Representative or Records Custodian, the Section Manager for the Regulatory and Research Section within the Licensing, Research, and Trade Practices Division, the Special Projects Manager of the Licensing, Research, and Trade Practices Division, the Section Manager of the Finance, Administration, and Accountability Division, the Human Resources Officer, the Director of the Field Enforcement Division, Field Enforcement Division law enforcement officers, program managers, and any ATCC employee who collects, maintains, reviews, discloses, or provides access to personal records or geolocation data.

For purposes of this policy:

- The Section Manager for the Regulatory and Research Section within the Licensing, Research, and Trade Practices Division shall serve as the Agency Data Owner.
- The Special Projects Manager of the Regulatory, Licensing, Research, and Trade Practices Division shall serve as the Information Technology and Data Security Personnel.
- The Section Manager of the Finance, Administration, and Accountability Division shall serve as the Contract Monitor.

- The Procurement Officer shall ensure that applicable procurement documents, contracts, amendments, renewals, memoranda of understanding, and data use agreements contain appropriate privacy terms.
- The Legal and Legislative Division shall provide guidance regarding privacy, redisclosure, contract terms, Public Information Act requests, law enforcement information sharing, and statutory compliance. This Division shall also submit the finalized SOP to the General Assembly.
- The Director of the Field Enforcement Division shall supervise law enforcement information sharing conducted by Field Enforcement Division officers in connection with criminal investigations.
- The Executive Director shall designate a serve as the agency's Privacy Officer to oversee compliance with data protection protocols and coordinate with the Department of Information Technology and the Office of the Attorney General, pursuant to Md. Code Ann., State Fin. & Proc. § 3.5-319.

Staff Monitor:

Compliance with these procedures will be monitored by the Executive Director, the Director of the Legal and Legislative Division, the Director of the Field Enforcement Division, and the staff identified above.

Policy:

The ATCC shall protect personal records and geolocation data from sale, resale, redisclosure, monetization, data brokerage, profiling, targeted advertising, or other secondary commercial use.

The ATCC shall not knowingly enter into or administer a contract that permits a contractor, vendor, subcontractor, consultant, processor, or other third party to sell, resell, license, rent, monetize, or otherwise commercially exploit personal records or geolocation data provided or made available by the ATCC.

The ATCC shall limit the collection, use, disclosure, and sharing of personal record information to authorized agency purposes. Employees shall use privacy-protective practices, including minimization, redaction, aggregation, deidentification, access controls, and legal review when appropriate.

This policy does not prohibit authorized ATCC law enforcement officers from sharing personal records, personally identifiable information, geolocation data, investigative information, intelligence, reports, records, evidence, or other sensitive information with federal, State, or local law enforcement agencies when the sharing is for a legitimate law enforcement purpose, including the investigation, enforcement, prosecution, or prevention of criminal violations related to the alcohol, tobacco, or cannabis laws of the State.

Nothing in this policy authorizes the ATCC to withhold records that must be disclosed under the Maryland Public Information Act or other applicable law.

1. Definitions

- a) **Personal Record:** A public record that names or, with reasonable certainty, otherwise identifies an individual by an identifying factor, including an address, description, fingerprint or voice print, number, or picture, as provided in Md. Code Ann., Gen. Prov. § 4-501.
- b) **Personal Information / Personally Identifiable Information / PI / PII:** Information that identifies, describes, relates to, or can reasonably be linked to a specific individual, including “Personal Information” as defined by Md. Code Ann. State Gov’t § 10-1301(c). This includes addresses, telephone numbers, email addresses, dates of birth, Social Security Numbers, Individual Taxpayer Identification Numbers (“ITINs”), passport numbers, or other U.S. government-issued identification numbers, photographs, usernames or email addresses in combination with a password or security question and answer that permits access to an individual’s e-mail account, genetic and health-related data (including mental health, substance use disorder, and disability), **Sensitive Data** (as defined in Section 1.g) licensing information, complaint information, witness information, investigation information, enforcement information, financial information, or similar identifying information.
- c) **Geolocation Data:** Information that identifies or may reasonably be used to infer an individual’s physical location, including information derived from a device, address, coordinates, inspection record, complaint record, licensing record, enforcement record, or other source.
- d) **Law Enforcement Information Sharing:** The disclosure of personal records, PII, geolocation data, investigative information, reports, evidence, intelligence, or other sensitive information by authorized ATCC law enforcement officers to federal, State, or local law enforcement agencies for a legitimate criminal investigative, enforcement, prosecution, officer-safety, or public-safety purpose.
- e) **Redisclosure:** Any disclosure, transfer, publication, sale, resale, sharing, licensing, release, access, or transmission of ATCC-provided personal records or geolocation data by a recipient to another person or entity. Redisclosure does not include authorized law enforcement information sharing conducted in accordance with this SOP.
- f) **Secondary Commercial Market:** Any commercial use involving personal records or geolocation data beyond the original governmental purpose for which the information was collected, maintained, or disclosed, including data brokerage, profiling, marketing lists, advertising products, analytics products, or artificial intelligence training sets.
- g) **Sensitive Data:** As defined by Md. Code Ann., Com. Law § 14-4701, is personal data that includes Genetic or biometric data; personal data of a consumer that the controller knows or has reason to know is a child, precise geolocation data, or that reveals any of the following: (i) Racial or ethnic origin, (ii) Religious beliefs, (iii) Consumer health data, (iv) Sex life, (v) Sexual orientation, (vi) Status as transgender or nonbinary, (vii) National origin; or (viii) Citizenship or immigration status.

2. Collection and Authorized Use of Personal Information

- a) ATCC employees may collect personal information only when it is appropriate, relevant, and limited to the minimum amount necessary to accomplish a legitimate government purpose, including licensing, permitting, enforcement, compliance, inspections,

investigations, adjudications, public communications, employee administration, law enforcement activity, or other official agency duties.

- b) Before collecting personal information, the responsible ATCC employee or unit shall determine the agency purpose for collection, whether the information is necessary, whether less sensitive information would satisfy the same purpose, who will have access, how long the information must be retained, and whether the information may later be provided to a contractor, vendor, public records requester, law enforcement partner, or other third party.
- c) ATCC employees shall not collect personal information solely because it may be useful later. Collection shall be tied to a specific legitimate government purpose, including a legitimate law enforcement function where applicable.
- d) Where practical, ATCC employees shall collect only necessary fields, limit access to employees with a work-related need, use aggregate or deidentified information when feasible, and avoid unnecessary duplication of personal records.
- e) The Agency Data Owner shall assist program staff in identifying covered data sets and determining whether personal information should be minimized, aggregated, deidentified, or otherwise restricted before disclosure. The Agency Data Owner shall not interfere with lawful law enforcement information sharing conducted by authorized Field Enforcement Division officers for criminal investigative purposes.
- f) **Public Privacy Notice:** In accordance with Department of Information Technology transparency standards, the ATCC shall publish and maintain a clear, easy-to-understand Privacy Notice on its public-facing website. The Privacy Notice shall inform the public about the legal authority for collecting personal information, the specific purposes for which the information will be processed, and the agency's data protection practices. Where feasible, the ATCC shall provide specific notification to individuals prior to the collection or sharing of their personal information detailing the legitimate government purpose for collection, any consequences for refusing to provide the information, the individual's right to inspect or correct the records, whether the information is generally available for public inspection, and whether it will be shared with other entities.
- g) **Retention and Deletion:** Personal information shall not be retained for longer than is reasonably necessary to fulfill the legitimate government purpose for which it was collected. In accordance with the ATCC's official records retention schedule or as allowed by law, personal information shall be securely deleted or de-identified when no longer needed.
- h) **Licensing Exemption Applicability:** Pursuant to Md. Code Ann., Gen. Prov. § 4-501(c)(5)(v), information contained in application or renewal materials relating to ATCC licensing is exempt from the requirement to provide point-of-collection privacy notices. However, all licensing materials remain strictly subject to the data minimization, retention, and secure deletion requirements outlined in this section.

3. Contract Prohibition on Sale, Resale, and Commercial Use

- a) All ATCC contracts, agreements, memoranda of understanding, data use agreements, purchase orders, renewals, amendments, and vendor arrangements that involve access to personal records, personal information, geolocation data, licensing data, enforcement data, complaint data, or other sensitive ATCC information shall prohibit the contractor, vendor, subcontractor, or third party from:

- i. selling, reselling, licensing, renting, transferring, monetizing, or otherwise commercially exploiting ATCC-provided personal records or geolocation data;
- ii. using ATCC-provided personal records or geolocation data to create, enhance, or sell a commercial data product;
- iii. using ATCC-provided personal records or geolocation data for targeted advertising, behavioral advertising, profiling, lead generation, marketing lists, data brokerage, artificial intelligence training, or similar commercial purposes;
- iv. redisclosing ATCC-provided personal records or geolocation data to another person or entity except as expressly authorized by the contract, required by law, approved in writing by the ATCC, or necessary to support an authorized law enforcement purpose;
- v. combining ATCC-provided personal records or geolocation data with outside data sets to identify, track, profile, target, or commercially exploit an individual;
- vi. retaining ATCC-provided personal records or geolocation data longer than authorized by the contract or applicable retention requirement; and
- vii. using ATCC-provided personal records or geolocation data for any purpose other than the specific purpose authorized by the ATCC.

To enforce these prohibitions, any such contracts must utilize the Office of State Procurement Attachment Y: Data Use Agreement, or ensure that the contract entered into contains privacy preserving measures that are no less restrictive.

- b) The Procurement Officer, in consultation with the Legal and Legislative Division, shall ensure that applicable contracts include privacy, data use, no-sale, no-resale, no-commercial-use, and redisclosure limitation terms before execution.
- c) Contract terms shall require vendors and contractors to flow down the same privacy restrictions to subcontractors, agents, processors, consultants, and any other person or entity with access to ATCC-provided data.
- d) The Section Manager of the Finance, Administration, and Accountability Division shall monitor applicable contracts for compliance and report suspected violations to the Procurement Officer and the Legal and Legislative Division.
- e) A contractor's unauthorized sale, resale, monetization, redisclosure, or secondary commercial use of ATCC-provided personal records or geolocation data may result in contract remedies, termination, suspension of data access, referral for legal action, or other corrective action.

4. Vendor Review and Data Use Agreements

- a) Before ATCC provides personal records or geolocation data to a vendor, contractor, consultant, processor, or other third party, the responsible program unit, Procurement Officer, Contract Monitor, Agency Data Owner, and Information Technology and Data Security Personnel shall determine, as applicable, whether the recipient needs the information, whether the amount of data is limited to the minimum necessary, whether the recipient has appropriate privacy and security safeguards consistent with the NIST Privacy Framework V1, NIST SP 800-53 V5, and NIST SP 800-207 Zero Trust Architecture, and whether the Office of State Procurement Attachment Y: Data Use

Agreement or similar written instrument containing no less restrictive measures is required.

- b) The Special Projects Manager of the Licensing, Research, and Trade Practices Division shall assist with review of system access, data transmission methods, technical restrictions, and data security controls when a vendor or third party will receive or access ATCC data.
- c) The Procurement Officer shall maintain a record of contracts and data use agreements that include privacy, no-sale, no-resale, and redisclosure limitation provisions.
- d) This section does not apply to routine law enforcement information sharing by authorized Field Enforcement Division officers with federal, State, or local law enforcement agencies, provided the sharing is for a legitimate criminal investigative, enforcement, prosecution, officer-safety, or public-safety purpose.

5. Public Information Act Requests and Disclosure of Personal Records

- a) ATCC shall continue to comply with the Maryland Public Information Act and other applicable disclosure laws.
- b) When responding to a request for records that may contain personal information, the Records Custodian, Public Information Act Representative, or designee shall review the records to determine whether disclosure may create a risk of sale, resale, redisclosure, commercial exploitation, identity-based harm, privacy harm, or use for a purpose unrelated to the reason the information was collected.
- c) Where legally permitted, ATCC shall use privacy-protective disclosure methods, including redaction, aggregation, deidentification, field-level minimization, exclusion of geolocation data not required to be disclosed, and legal review for requests involving bulk data, licensing lists, complaint data, enforcement data, geolocation data, or records that could support a secondary commercial market.
- d) The Agency Data Owner shall assist the Records Custodian or Public Information Act Representative, when requested, in identifying whether requested data may be aggregated, deidentified, or minimized before disclosure.
- e) ATCC employees shall not deny access to an entire record solely because it contains personal information if the record can be lawfully disclosed with appropriate redactions or privacy-protective disclosure methods.
- f) Records that are part of an active criminal investigation, intelligence matter, enforcement operation, referral to a law enforcement agency, or other protected law enforcement record shall be reviewed by the Legal and Legislative Division and, where appropriate, the Field Enforcement Division before release.
- g) When minimizing, redacting, or deidentifying personal records or geolocation data pursuant to this policy, the Records Custodian or Public Information Act Representative shall formally document the field-level minimization in the written response to the requester. To establish the legal and operational justification for the protection of this data against secondary commercial use, the response shall explicitly cite **Md. Code Ann., State Gov't § 10-1702** and the **Department of Information Technology (DoIT) Standard MD-STD-315-PT-02**.

6. Internal Data Sharing, Sensitive Data, Law Enforcement Sharing, and Incident Reporting

- a) ATCC employees shall access, use, and share personal records only for official agency business and only to the extent necessary to perform assigned duties.
- b) Employees may not download, copy, export, transmit, upload, or disclose personal records for a non-agency purpose; use personal records for personal, political, commercial, or unofficial purposes; upload personal records into unauthorized software, websites, artificial intelligence tools, cloud storage, personal accounts, or external platforms; maintain shadow databases; or assist any person or entity in obtaining ATCC data for resale, redistribution, commercial marketing, profiling, or data brokerage.
- c) Law enforcement officers of the Field Enforcement Division are authorized to share data, including personal records, personally identifiable information, geolocation data, investigative information, intelligence, reports, records, photographs, video, documents, and other sensitive information, with federal, State, and local law enforcement agencies for the purpose of conducting criminal investigations into violations related to the alcohol, tobacco, and cannabis laws of the State. Such sharing shall be limited to a legitimate law enforcement purpose and shall be conducted consistent with applicable law, agency procedures, investigative need, officer safety, and public safety. However, in accordance with Chapter 718 of the Acts of 2025 (The Maryland Values Act), ATCC employees and law enforcement officers shall not disclose personal records or sensitive data (including citizenship or immigration status) to federal authorities for the purpose of civil immigration enforcement unless presented with a valid warrant issued by a federal or State court.
- d) Field Enforcement Division officers may share sensitive information with law enforcement partners when necessary to investigate suspected criminal activity, coordinate enforcement operations, identify suspects or witnesses, locate evidence, verify licensure or compliance status, support prosecution, respond to officer-safety concerns, or prevent ongoing violations of alcohol, tobacco, or cannabis laws.
- e) ATCC shall treat geolocation data, biometric data, government identification numbers, dates of birth, home addresses, personal contact information, complaint information, enforcement information, witness information, and other sensitive data with heightened care. Geolocation data and Sensitive data shall not be collected or disclosed unless necessary for an authorized agency function, including a legitimate law enforcement function.
- f) Employees who are unsure whether information may be shared shall consult their supervisor, the Records Custodian, the Procurement Officer, the Agency Data Owner, the Information Technology and Data Security Personnel, the Field Enforcement Division, or the Legal and Legislative Division before disclosure. Field Enforcement Division officers may consult supervisory law enforcement personnel when immediate operational needs require prompt information sharing.
- g) Any ATCC employee who becomes aware of a suspected or actual unauthorized sale, resale, redisclosure, commercial use, misuse, loss, or improper access to personal records or geolocation data shall promptly report the matter to the employee's supervisor and the Legal and Legislative Division.
- h) The Legal and Legislative Division shall notify, as appropriate, the Agency Data Owner, the Information Technology and Data Security Personnel, the Procurement Officer, the

Contract Monitor, the Director of the Field Enforcement Division, and the Executive Director. ATCC may take corrective action, including suspension of access, vendor remediation, contract enforcement, employee counseling, disciplinary action, contract termination, referral to appropriate authorities, or other steps necessary to protect privacy.

7. Training, Review, and Recordkeeping

- a) ATCC shall provide appropriate internal guidance or training to employees whose duties involve collection, disclosure, procurement, contracting, information technology, records management, licensing, enforcement, investigations, Public Information Act responses, or law enforcement information sharing.
- b) This policy shall be reviewed at least once every three years, or sooner if required by law, Department of Information Technology guidance, agency operations, audit findings, contract issues, law enforcement information-sharing needs, or changes in privacy standards.
- c) ATCC shall maintain records of contracts containing privacy and data use restrictions, data use agreements, vendor privacy reviews, contract monitoring concerns, PIA responses involving significant personal record minimization or redaction issues, reported suspected unauthorized sale or redisclosure incidents, and updates to this policy.
- d) Investigative records, law enforcement referrals, intelligence records, and criminal enforcement records shall be maintained in accordance with applicable records retention requirements, law enforcement procedures, litigation holds, court orders, and agency preservation obligations.

8. References

- Md. Code Ann., State Gov't § 10-1702.
Md. Code Ann., Gen. Provisions § 4-501.
- Md. Code Ann., Com. Law § 14-4701.
Maryland Public Information Act, Md. Code Ann., Gen. Provisions §§ 4-101 et seq.
Chapter 718 of the Acts of 2025, House Bill 1222.
- Chapter 435 of the Acts of 2026, House Bill 264.
Applicable State privacy, cybersecurity, procurement, records retention, law enforcement, and Department of Information Technology standards.