



Procedures on Personal Records and Geolocation Data

State Government Article, Section 10-1702(c)

Effective Date: July 1, 2026

Table of Contents

Table of Contents	1
Purpose	2
Definitions	2
Scope	3
Roles and Responsibilities	3
Standards	3
Develop Agency-Level Procedures (PT-1)	4
Establish Authority to Process (PT-2)	4
Define Processing Purposes (PT-3)	4
Obtain Consent (PT-4)	5
Privacy Notice and Required Disclosures Prior to Collecting or Sharing PI/PII (PT-5)	5
System of Records Notice (PT-6)	5
Address Specific Categories of PII/PI (PT-7)	5
Meet Computer Matching Requirements (PT-8)	6
Prohibit Agency Sale of Person Information (PT-9)	6
Data Use Agreements and Third Party Processors (PT-10)	6
Not a Contract	6
Three-Year Review Process	6
Appendices	7
Appendix A: Privacy Threshold Analysis (PTA)	7
Appendix B: Criminal Injuries Compensation Board Privacy Policy	9

Purpose

Pursuant to § 10–1702 of the State Government Article, this **Procedures on Personal Records and Geolocation Data** provides guidelines to prevent the sale and redisclosure of data on behalf of the protected individuals. It also includes technical and operational specifications to process Personal Information (PI) / Personally Identifiable Information (PII) responsibly, maintain transparency, and comply with privacy regulations.

The Governor’s Office of Crime Prevention and Policy (Office) developed this **Procedures on Personal Records and Geolocation Data** with the use of the *National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5 Moderate Baseline* and State-specific organizationally defined parameters. It also follows the State’s *Privacy and Security Policy* which is accessible on the Department of Information Technology’s (DoIT’s) website at: <https://www.maryland.gov/privacy-and-security-policy>.

Definitions

Please refer to the following definition, including those specified under § 10–1702 of the State Government Article and § 4–501 of the General Provisions Article.

- **Personal Information (PI)** means an individual’s first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:
 - a Social Security number;
 - an individual tax identification number;
 - a passport number or other other identification number issued by the government;
 - a driver’s license number, state identification card number, or other individual identification number issued by a unit;
 - a financial or other account number, a credit card number, or a debit card number; that, in combination with any required security code, access code, or password, would permit access to an individual’s account;
 - a username or email address in combination with a password or security question; and answer that permits access to an individual’s email account;
 - genetic and health related data including mental health, substance use disorder, and disability; or
 - sensitive data as defined in § 14–4701 of the Commercial Law Article.
- **Personally Identifiable Information (PII)** refers to any data that can be used to identify a specific individual. This includes information that can directly identify a person or can be used in combination with other data to identify someone.

Scope

This **Procedures on Personal Records and Geolocation Data** applies to:

- All agency personnel, full-time employees, and temporary staff within the Office; and
- All information technology (IT) systems, applications, databases and physical environments that process, store, or transmit PI/PII.

Roles and Responsibilities

Responsibility	Responsible Parties
PT-1 Develop Agency Level Procedures	Chief Privacy Officer Chief Data Officer
PT-2 Authority to Process PII	Chief Privacy Officer
PT-3 Define Processing Purposes	Chief Privacy Officer Data Owners Procurement Officer
PT-4 Consent	Chief Privacy Officer Data Owners
PT-5 Privacy Notice and Required Disclosures Prior to Collecting or Sharing PI/PII	Chief Privacy Officer Data Owners
PT-6 Systems of Record Notice	Chief Privacy Officer
PT-7 Address Specific Categories of PII/PI	Data Owners
PT-8 Meet Computer Matching Requirements	n/a
PT-9 Prohibit Agency Sale of Personal Information	Chief Privacy Officer Data Owners Procurement Officer
PT-10 Data Use Agreements and Third Party Processors	Procurement Officer

Standards

DoIT has identified the standards below which help to establish a baseline of privacy and transparency practices that the Office must implement to comply with State cybersecurity and privacy policies and the protection of PI/PII.

Develop Agency-Level Procedures (PT-1)

In alignment with this Standard, the Office is required to develop and document agency-level privacy protection and transparency procedures and share them with agency personnel with IT security responsibilities. All procedures must be reviewed and if necessary, updated based on changes and risk at least every three years. This **Procedures on Personal Records and Geolocation Data** identifies all procedures to address the purpose, scope, roles and responsibilities, and guidelines, as mandated.

Establish Authority to Process (PT-2)

The Director of the Research, Analysis, and Evaluation serves as the Office's Chief Privacy Officer and permits the processing of PI/PII, and ensures that it is processed only as explicitly authorized. If you have any questions, please contact:

Jeffrey Zuback
Director of Research, Analysis, and Evaluation
Jeffrey.Zuback@Maryland.gov

Prior to the development or modification of any IT systems, applications, databases, and physical environments that process, store, or transmit PI/PII, the Agency Privacy Officer will:

- Complete a Privacy Threshold Analysis (see [Appendix A](#));
- Conduct a Privacy Impact Assessment to ensure the proper privacy controls are in place;
- Identify the exact legislative mandate authorizing the data;
- Log the approved system into the Office's Agency PII Data Inventory.

Define Processing Purposes (PT-3)

The Office collects PI/PII data for two primary purposes:

1. To compensate crime victims.
2. To ensure compliance with the four core protections under the federal Office of Juvenile Justice Delinquency and Prevention Act of 2018.¹

The Office does not collect geolocation data.

¹ Governor's Office of Crime Prevention and Policy. *Juvenile Justice and Delinquency Prevention Act*. <https://gocpp.maryland.gov/juvenile-justice-and-delinquency-prevention-act-2/>

The Data Owners are those individuals in the office that manage the databases that contain PI/PII. They will ensure that PI/PII may be used only for purposes originally disclosed unless otherwise authorized by law and ensure only those staff with a need to know are provided authorized access. Any changes to these existing data systems with PI/PII or the procurement of additional IT systems, applications, databases and physical environments that process, store, or transmit PI/PII are authorized through the Office's Procurement Officer.

Obtain Consent (PT-4)

The Chief Privacy Officer will work directly with the Data Owners to ensure that the IT systems, applications, databases and physical environments that process, store, or transmit PI/PII enable individuals to provide consent for the processing of their information prior to data collection including the purpose, legal authority, and intended use of their personal information.

See [Appendix B](#) for an example of a privacy notice/informed consent notice within one of the Office's data systems that contains PI/PII.

Privacy Notice and Required Disclosures Prior to Collecting or Sharing PI/PII (PT-5)

For more information regarding privacy and security policy, please visit:
<https://www.maryland.gov/privacy-and-security-policy>.

System of Records Notice (PT-6)

The Office follows the Fair Information Privacy Practices (FIPPs) guidance which serves as a foundational framework for privacy and data protection.² Originally developed in the 1970s and widely adopted across government and industry, it provides guidance on how organizations should collect, use, and manage personal information responsibly. The Office also complies with Executive Order 01.01.2021.10 regarding Maryland Data Privacy.³

Address Specific Categories of PII/PI (PT-7)

This standard refers to the processing and collection of Social Security Numbers (SSNs). The Office collects SSNs for just one database. The collection of SSNs shall only be used to verify billing invoicing and for the finance department to process payments.

² U.S Department of Homeland Security. (2011). *The Fair Information Practice Principles at Work*.
<https://www.dhs.gov/sites/default/files/2024-01/Governing%20Privacy%20Policy%20-%20FIPPs%20Factsheet.pdf>

³ Code of Maryland Regulations. *Executive Order 01.01.2021.10 Maryland Data Privacy*.
<https://regs.maryland.gov/us/md/exec/comar/01.01.2021.10>

Meet Computer Matching Requirements (PT-8)

This standard refers to matching PII across agencies, such as the Social Security Administration, the Department of Homeland Security, and the Department of Health and Human Services. This section is not applicable to the Office.

Prohibit Agency Sale of Person Information (PT-9)

The State does not sell PI/PII under any circumstances. The Office's Chief Privacy Officer will work with the Procurement Director to ensure that any contract/agreement entered into with a contractor or other third party explicitly disallows the sale of personal information that has been collected by the Office and strictly restrict third parties authorized to process PI/PII from the sale/reselling, licensing, renting, monetizing, or otherwise deriving commercial values from the data.

Data Use Agreements and Third Party Processors (PT-10)

The Procurement Officer ensures that the most recent Office of State Procurement Attachment Y: Data Use Agreement⁴ is executed as part of any contract involving third-party processing of PI/PII.

Not a Contract

This **Procedures on Personal Records and Geolocation Data** does not constitute or create an express or implied contract. It is not intended to, and does not, create contractual obligations with respect to any matter it covers.

Three-Year Review Process

To ensure this **Procedures on Personal Records and Geolocation Data** remains current with IT changes, the Office will review all procedures every three years, to include the purpose, scope, roles and responsibilities, and guidelines. It will also incorporate an active risk assessment evaluating changes in the Office's IT infrastructure, emerging privacy threats, and changes to upstream State standards. All updates will be tracked and fully synchronized with overarching standards before re-authorization.

⁴ Office of State Procurement. *Attachment Y. Data Use Agreement*.

<https://procurement.maryland.gov/wp-content/uploads/sites/12/2024/08/Attachment-Y.-Data-Usage-Agreement.pdf>

Appendices

Appendix A: Privacy Threshold Analysis (PTA)

[Agency Name] — Preliminary Privacy Assessment

Purpose: This form is used to determine whether a new or significantly modified information technology system, project, or data-sharing agreement involves the collection, storage, or maintenance of **Personally Identifiable Information (PII)** and whether a full **Privacy Impact Assessment (PIA)** is required.

Instructions: The Data Owner should complete this form and submit it to the **Agency Privacy Officer** prior to procuring software or beginning system development.

SECTION 1: GENERAL SYSTEM & PROJECT INFORMATION

- **1.1 Project / System Name:** _____
- **1.2 Data Owner:** _____
- **1.3 Division / Program Office:** _____
- **1.4 Brief Description of the Project and its Business Purpose:** _____

SECTION 2: DATA CHARACTERISTICS & COLLECTION

2.1 Does this system collect, maintain, use, or disseminate information about individuals?

- ☐ **Yes** (*Proceed to question 2.2*)
- ☐ **No** (*Skip to Section 4*)

2.2 Check all categories of data that will be collected, maintained, or processed by this system:

Standard PII

- ☐ Full Name
- ☐ Mailing/Home Address
- ☐ Email Address (Personal or Work)
- ☐ Phone Number
- ☐ Date of Birth
- ☐ Employment / Education History
- ☐ IP Address / Device Identifiers

Sensitive / Protected PII

- ☐ Social Security Number (SSN) / Taxpayer ID
- ☐ Driver's License / State ID Number

- ☐ Financial Account / Credit Card Numbers
- ☐ Medical / Health Records (Protected Health Information)
- ☐ Criminal History / Background Check Data
- ☐ Biometric Identifiers (Fingerprints, Facial Recognition)
- ☐ Geolocation / GPS Tracking Data

2.3 Whose information is being collected? (Check all that apply)

- ☐ State Employees / Contractors
- ☐ Members of the General Public / State Residents
- ☐ Businesses / Vendors
- ☐ Vulnerable Populations (e.g., Minors, Incarcerated Individuals, Foster Youth)

SECTION 3: SYSTEM ARCHITECTURE & DATA SHARING

3.1 Where will the data be hosted/stored?

- ☐ On-Premise State Agency Data Center
- ☐ Third-Party Cloud Vendor (e.g., AWS, Azure, Salesforce, SaaS provider)
- ☐ Other: _____

3.2 Will data be shared with, or accessed by, entities outside of this Agency?

- ☐ No
- ☐ Yes, with other State/Federal Agencies (List agencies: _____)
- ☐ Yes, with private vendors or contractors (List vendors: _____)

3.3 Does the system use any of the following technologies? (Check all that apply)

- ☐ Artificial Intelligence (AI) or Automated Decision-Making algorithms
- ☐ Video, audio, or drone surveillance
- ☐ Public-facing web portals or mobile applications

SECTION 4: SIGNATURE AND PRIVACY OFFICE DETERMINATION

Submitted By: *Data Owner*



FOR PRIVACY OFFICE USE ONLY

Privacy Reviewer: _____ Date Reviewed: _____

Final Determination:

- ☐ **Option A: No Further Privacy Action Required.** The system does not collect or maintain PII, or the privacy risks are negligible.
- ☐ **Option B: Full Privacy Impact Assessment (PIA) Required.** The system processes PII or sensitive data; project team must complete a formal PIA before deployment.

Privacy Officer Comments: _____

Appendix B: Criminal Injuries Compensation Board Privacy Policy

Below is an example of a privacy notice/informed consent notice within one of the Office's data systems that contains PI/PII.

Privacy Policy

This Privacy Policy describes Our policies and procedures on the collection, use and disclosure of Your information when You use the Service and tells You about Your privacy rights and how the law protects You.

We use Your Personal data to provide and improve the Service. By using the Service, You agree to the collection and use of information in accordance with this Privacy Policy.

Interpretation and Definitions

Interpretation

The words of which the initial letter is capitalized have meanings defined under the following conditions.

The following definitions shall have the same meaning regardless of whether they appear in singular or in plural.

Definitions

For the purposes of this Privacy Policy:

- **You** means the individual accessing or using the Service, or the company, or other legal entity on behalf of which such individual is accessing or using the Service, as applicable.
- **Company** (referred to as either "the Company", "We", "Us" or "Our" in this Agreement) refers to CCVC INC, PO Box 631159, Highlands Ranch, CO 80163.
- **Affiliate** means an entity that controls, is controlled by or is under common control with a party, where "control" means ownership of 50% or more of the shares, equity interest or other securities entitled to vote for election of directors or other managing authority.
- **Account** means a unique account created for You to access our Service or parts of our Service.
- **Website** refers to the source web site from where this policy was referenced
- **Service** refers to the Website.
- **Country** refers to: Colorado, United States
- **Service Provider** means any natural or legal person who processes the data on behalf of the Company. It refers to third-party companies or individuals employed by the Company

to facilitate the Service, to provide the Service on behalf of the Company, to perform services related to the Service or to assist the Company in analyzing how the Service is used.

- **Third-party Social Media** Service refers to any website or any social network website through which a User can log in or create an account to use the Service.
- **Personal Data** is any information that relates to an identified or identifiable individual.
- **Cookies** are small files that are placed on Your computer, mobile device or any other device by a website, containing the details of Your browsing history on that website among its many uses.
- **Device** means any device that can access the Service such as a computer, a cellphone or a digital tablet.
- **Usage Data** refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, the duration of a page visit).

Collecting and Using Your Personal Data

Types of Data Collected

Personal Data

While using Our Service, We may ask You to provide Us with certain personally identifiable information that can be used to contact or identify You. Personally identifiable information may include, but is not limited to:

- Email address
- First name and last name
- Phone number
- Address, State, Province, ZIP/Postal code, City
- Usage Data

Usage Data

Usage Data is collected automatically when using the Service.

Usage Data may include information such as Your Device's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that You visit, the time and date of Your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When You access the Service by or through a mobile device, We may collect certain information automatically, including, but not limited to, the type of mobile device You use, Your mobile

device unique ID, the IP address of Your mobile device, Your mobile operating system, the type of mobile Internet browser You use, unique device identifiers and other diagnostic data.

We may also collect information that Your browser sends whenever You visit our Service or when You access the Service by or through a mobile device.

Tracking Technologies and Cookies

We use Cookies and similar tracking technologies to track the activity on Our Service and store certain information. Tracking technologies used are beacons, tags, and scripts to collect and track information and to improve and analyze Our Service.

You can instruct Your browser to refuse all Cookies or to indicate when a Cookie is being sent. However, if You do not accept Cookies, You may not be able to use some parts of our Service.

Cookies can be “Persistent” or “Session” Cookies. Persistent Cookies remain on your personal computer or mobile device when You go offline, while Session Cookies are deleted as soon as You close your web browser. Learn more about cookies in the [“What Are Cookies”](#) article.

- **Necessary / Essential Cookies**

- Type: Session Cookies
- Administered by: Us
- Purpose: These Cookies are essential to provide You with services available through the Website and to enable You to use some of its features. They help to authenticate users and prevent fraudulent use of user accounts. Without these Cookies, the services that You have asked for cannot be provided, and We only use these Cookies to provide You with those services.

- **Cookies Policy / Notice Acceptance Cookies**

- Type: Persistent Cookies
- Administered by: Us
- Purpose: These Cookies identify if users have accepted the use of cookies on the Website.

- **Functionality Cookies**

- Type: Persistent Cookies
- Administered by: Us
- Purpose: These Cookies allow us to remember choices You make when You use the Website, such as remembering your login details or language preference. The purpose of these Cookies is to provide You with a more personal experience and to avoid You having to re-enter your preferences every time You use the Website.

For more information about the cookies we use and your choices regarding cookies, please visit our Cookies Policy.

Use of Your Personal Data

We may use Personal Data for the following purposes:

- **To provide and maintain our Service**, including to monitor the usage of our Service.
- **To manage Your Account:** to manage Your registration as a user of the Service. The Personal Data You provide can give You access to different functionalities of the Service that are available to You as a registered user.
- **For the performance of a contract:** the development, compliance and undertaking of the purchase contract for the products, items or services You have purchased or of any other contract with Us through the Service.
- **To contact You:** To contact You by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products or contracted services, including the security updates, when necessary or reasonable for their implementation.
- **To provide You** with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless You have opted not to receive such information.
- **To manage Your requests:** To attend and manage Your requests to Us.

We may share your personal information in the following situations:

- **With Service Providers:** We may share Your personal information with Service Providers to monitor and analyze the use of our Service, to contact You.
- **For Business transfers:** We may share or transfer Your personal information in connection with, or during negotiations of, any merger, sale of Company assets, financing, or acquisition of all or a portion of our business to another company.
- **With Affiliates:** We may share Your information with Our affiliates, in which case we will require those affiliates to honor this Privacy Policy. Affiliates include Our parent company and any other subsidiaries, joint venture partners or other companies that We control or that are under common control with Us.
- **With Business partners:** We may share Your information with Our business partners to offer You certain products, services or promotions.
- **With other users:** when You share personal information or otherwise interact in the public areas with other users, such information may be viewed by all users and may be publicly distributed outside. If You interact with other users or register through a Third-Party Social Media Service, Your contacts on the Third-Party Social Media Service

may see Your name, profile, pictures and description of Your activity. Similarly, other users will be able to view descriptions of Your activity, communicate with You and view Your profile.

Retention of Your Personal Data

The Company will retain Your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy. We will retain and use Your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

The Company will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer time periods.

Transfer of Your Personal Data

Your information, including Personal Data, is processed at the Company's operating offices and in any other places where the parties involved in the processing are located. It means that this information may be transferred to — and maintained on — computers located outside of Your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from Your jurisdiction.

Your consent to this Privacy Policy followed by Your submission of such information represents Your agreement to that transfer.

The Company will take all steps reasonably necessary to ensure that Your data is treated securely and in accordance with this Privacy Policy and no transfer of Your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of Your data and other personal information.

Disclosure of Your Personal Data

Business Transactions

If the Company is involved in a merger, acquisition or asset sale, Your Personal Data may be transferred. We will provide notice before Your Personal Data is transferred and becomes subject to a different Privacy Policy.

Law enforcement

Under certain circumstances, the Company may be required to disclose Your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

Other legal requirements

The Company may disclose Your Personal Data in the good faith belief that such action is necessary to:

- Comply with a legal obligation
- Protect and defend the rights or property of the Company
- Prevent or investigate possible wrongdoing in connection with the Service
- Protect the personal safety of Users of the Service or the public
- Protect against legal liability

Security of Your Personal Data

The security of Your Personal Data is important to Us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While We strive to use commercially acceptable means to protect Your Personal Data, We cannot guarantee its absolute security.

Links to Other Websites

Our Service may contain links to other websites that are not operated by Us. If You click on a third party link, You will be directed to that third party's site. We strongly advise You to review the Privacy Policy of every site You visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

Changes to this Privacy Policy

We may update our Privacy Policy from time to time. We will notify You of any changes by posting the new Privacy Policy on this page.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

Contact Us

If you have any questions, comments, complaints or requests regarding this Privacy Policy, or our processing of your information, you can contact us at support@ccvc.org