Attachment Y. Data Use Agreement

DATA USE AGREEMENT BETWEEN [NAME OF AGENCY] AND _____

This Data Use Agreement (this "Agreement") is made between the Maryland [NAME OF AGENCY], a unit of the State of Maryland Executive branch of government (the "State"), and _____ (the "Processor") (each a "Party" and collectively, the "Parties").

WHEREAS, the State and Processor are Parties to [Identify the Contract] dated _____ __, ____ pursuant to which Processor provides the services described therein [or perhaps briefly describe here the services it provides] (the "Underlying Contract") and, in the performance thereof, receives from the State certain Personally Identifiable Information about one or more individuals necessary to the performance of the Underlying Contract ("Authorized Purpose");

WHEREAS, pursuant to and consistent with the Underlying Contract, the Authorized Purpose may include the collection, use, disclosure, analysis, deletion, or modification of PII;

WHEREAS, the Protection of Information by Government Agencies (PIGA) provisions in Title 10, Subtitle 13 of the State Government Article, Annotated Code of Maryland, were enacted to protect personal information from unauthorized access, use, modification, or disclosure, and requires (1) "a unit that collects Personal Information [herein called "Personally Identifiable Information"] of an individual to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information collected and the nature of the unit and its operations"; and (2) "a unit that uses a nonaffiliated third party [such as the Processor] as a service provider to perform services for the unit and discloses personal information about an individual under a written contract or agreement with the third party [to] require by written contract or agreement that the third party implement and maintain reasonable security procedures and practices that: (i) are appropriate to the nature of the personal information disclosed to the nonaffiliated third party; and (ii) are reasonably designed to help protect the personal information from unauthorized access, use, modification, disclosure, or destruction";

WHEREAS, the Parties desire to enter into this Agreement for the purposes of ensuring the confidentiality, privacy, and security of data provided to or accessed by Processor or exchanged between the Parties under and in connection with the Underlying Contract and in compliance with the PIGA and any other applicable State or federal privacy laws.

NOW THEREFORE, for and in consideration of the mutual promises and of other good and valuable consideration herein contained, the Parties, intending to be legally bound, hereby agree as follows:

A. Definitions

1. **Confidentiality** means the protection of data from unauthorized access, use, and disclosure, including means for protecting personal privacy and proprietary information.

2. **Data subject** means any individual person whose Personally Identifiable Information is provided to or accessed by Processor or exchanged between the Parties in connection with services provided by Processor under the Underlying Contract.

3. **Entity** means a person or organization possessing separate and distinct legal rights.

4. **Personally Identifiable Information** (PII) means

a. 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:

   i) A Social Security number, an Individual Taxpayer Identification number, a passport number, or other identification number issued by the federal government;
   ii) A driver's license number or state identification card number;
   iii) 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; or

b. Username or email address in combination with a password or security question and answer that permits access to an individual's email account.

5. **Privacy** means the right of an Entity to maintain control over and confidentiality of information about itself.

6. **Reasonable security measures** means data security procedures and practices developed, in good faith, and set forth in a written information security policy that are (i) appropriate to the nature of the Personally Identifiable Information disclosed to the Processor; and (ii) are reasonably designed to protect the Personally Identifiable Information from unauthorized access, use, modification, disclosure, or destruction.

7. **Breach** of the Security of a System means the unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of Personally Identifiable Information maintained by the Processor.

B. Permitted Uses and Disclosure of Personal Information

1. The Processor may only use or disclose PII as necessary to the Authorized Purpose and must limit uses and disclosures to the minimum extent necessary in the performance thereof.

2. If the Processor is requested or required by law or by any governmental body to disclose any Personal Information, the Processor shall, to the extent legally permissible, provide prompt written notice to the State as provided for herein of any such request or requirement so that the State may seek a protective order or other appropriate remedy and/or waive compliance with the provisions of this Agreement. In the absence of such protective order or waiver, the Processor may disclose only such portion of the PII as is legally required or requested.

3. The Processor may not sell the PII of any Entity or otherwise directly or indirectly receive remuneration in exchange, thereof. For the avoidance of doubt, this provision shall not preclude Processor from receiving payment for the provision of services set forth in the Underlying Contract.

4. The Processor may not use or disclose the PII of any Entity for the purposes of marketing a product or service unless necessary to perform the services set forth in the Underlying Contract or required by law.

For the purposes of this provision, "marketing" shall mean a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

C. Processor Duties Relative to PII

1. The Processor shall use reasonable security measures to protect the privacy of PII including, but not limited to the following:

   a. Limit disclosure of the information and details relating to a PII loss only to those with a need to know and who are bound by confidentiality obligations at least as restrictive as those set forth in this Agreement.

   b. Safeguard PII always, regardless of whether the Processor's employee, contractor, or agent is at their regular duty station.

   c. Train individuals to whom access to PII is granted about privacy, IT Security, and confidentiality best practices and require their signed acknowledgment of understanding of and abidance to the training prior to credentialing them to access PII data and regularly, thereafter. (See Appendix B: List of Processor personnel with Access to State PII)

   d. Send emails containing PII only if encrypted and being sent to and being received by email addresses of persons authorized to receive such information.

   e. If Processor uses a non-affiliated third party to perform services and discloses Personally Identifiable Information to the third party, such shall be pursuant to a written agreement between the parties which must require the third party to implement and maintain reasonable security procedures no less stringent than those required in this Agreement;

   f. Regularly review privacy and IT security policies, procedures, and practices to ensure compliance with PIGA and this Agreement;

   g. Designate a person who addresses any complaints or questions an Entity may have regarding the Processor's privacy practice;, and,

   h. Promptly provide written notice to the State as provided for herein if it learns of any unauthorized use, misappropriation, or disclosure of any PII. Processor must, at its own expense, cooperate with the State in seeking injunctive or other equitable relief with respect to any unauthorized use, misappropriation, or disclosure of any Personal Information.

D. Security Breach Detection and Investigation

1. The Processor must give written notice to the State as provided for herein within one (1)- business day after the Processor discovers or is notified of the Breach of the Security of a System.

2. Once it discovers or is notified that it incurred a Breach of the Security of a System, Processor must conduct in good faith a reasonable and prompt investigation to determine the likelihood that PII of an Entity has been or will be misused, e.g., for identity theft. If the investigation shows that there is a reasonable chance that the data will be misused, the Processor must abide by the Underlying Agreement's requirement regarding mitigation and remediation.

E. Security Breach Notification

1. As soon as reasonably practicable, but not later than 45 days of the business' discovery or notification of the Breach of the Security of a System, Processor must provide Notice to affected data subjects that is given in writing and sent to the most recent address of the data subject or meet the obligations under Title 10 §1305 (e) and (f).

2. A Processor may delay notification if requested by a law enforcement agency or to determine the scope of the breach, identify all the affected data subjects, or restore the integrity of the system. However, the Processor must send notification within 7 days after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security if the original 45–day period has already elapsed or within 45 days of becoming aware of the breach of the security of a system.

3. Notice may be sent via email if a data subject has already consented to receive electronic notices, or the Processor primarily conducts its business via the Internet.

4. The Processor may provide notice of a security breach by email, posting on its website, and to statewide media if the cost of notice would exceed $100,000 or the number of data subjects to be notified exceeds 175,000 individuals.

F. In the Event of a Breach - Notice to Consumer Must Include:

1. To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of Personally Identifiable Information were, or are reasonably believed to have been, acquired;

2. Contact information for the Processor's designee who can address data subjects' questions and concern, including a toll-free number if the Processor has one;

3. Toll-free numbers and addresses for each of the three credit reporting agencies: Equifax, Experian, and TransUnion;

4. Toll-free numbers, addresses, and websites for the Federal Trade Commission (FTC) and the Maryland Office of the Attorney General (OAG);

5. A statement that the data subject can obtain information from these sources about steps to avoid identity theft.

6. The Processor must provide a draft of the notification to and receive approval from the State prior to sending the notification to the OAG.

G. Processor Notice to the Attorney General

1. Prior to sending notification to affected data subjects, the Processor shall notify the Office of Attorney General.

    a. At a minimum, the notice must include the number of affected Maryland residents, a description of the breach, including when and how it occurred, any steps the business has taken (or plans to take)

relating to the breach of the security of a system, and the form of notice that will be sent to affected individuals and a sample notice.

b. All notifications shall be deemed to have been duly given (i) if delivered by hand or overnight courier service, mailed by certified or registered mail, or sent by email, as follows:

The OAG's notification:

By U.S. Mail:
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

With a copy to:
Attn: Security Breach Notification
(410) 576-6566
By Email:
Idtheft@oag.state.md.us

H. Term and Termination

1. Term

a. The Term of this Agreement shall be effective as of the date executed by the State below and shall terminate when all of the PII provided to or created or received by Processor in connection with the Underlying Contract, is destroyed or returned to the State, in accordance with the termination provisions of sub (3) of this Section.

b. Destruction of Records. Processor shall have and abide by a data retention schedule. When, upon authorization by the State, Processor destroys records, Processor shall take reasonable steps to protect against unauthorized access to or use of personal information.

c. If it is impossible to return or destroy all the PII provided to, or created or received by Processor, Processor's obligations under this Agreement shall be ongoing with respect to such information, unless and until a separate written agreement regarding that information is entered into with the State.

2. Termination

This Agreement is subject to the termination provisions of the Underlying Contract.

3. Effect of Termination

a. Upon any termination of this Agreement, Processor shall return or, if agreed to by the State, destroy all PII received from the State in connection with the Underlying Contract, or pursuant thereto the Processor created, maintained, or received on behalf of the State, Processor shall retain no coPIIes of the PII. This provision shall apply to PII that is in the possession of Processor's subcontractors or agents. If the return or destruction of all PII is not possible, the Processor shall maintain at least the same level of security to the data until such time as the data is destroyed or returned. The Processor shall attest to the return or destruction of PII. (See Appendix C: Certification of Data Destruction).

b. In the event of any intentional, willful, or grossly negligent material breach by Processor of any obligation of this Agreement or applicable law, the State shall have the right to immediately terminate any contract then in force between the Parties, including but not limited to the Underlying Contract.

I. Survival

The obligations of the Processor under this Agreement shall survive its expiration or earlier termination.

J. Unfair or Deceptive Trade Practices.

A violation of the Maryland Personal Information Privacy Act is an unfair or deceptive trade practice as defined by the Maryland Consumer Protection Act.

K. General Provisions

This Agreement shall be governed and construed in accordance with the laws of the State of Maryland, without regard to its choice of law provisions. This Agreement is not intended to modify the Parties' respective obligations to comply with any applicable federal, State, and local laws, rules, and regulations, or any obligations under the Underlying Contract.

L. Ambiguity.

Any ambiguity in this Agreement shall be resolved to permit the State to comply with the PIGA [and any applicable state or federal privacy regulation(s))] and its provisions with respect to the privacy and security of personally identifiable information.

M. Regulatory References

A reference in this Agreement to a section in the PIGA, including any regulations promulgated thereto, means the section as in effect or as amended.

N. Notices

All notices, requests, demands and other communications given under this Agreement shall be in writing and shall be deemed to have been received as of the posted date and time in the named email inbox, as follows:

Notice to State

_____
Designated Agency Privacy Officer

_____
Email Address

Notice to State

_____
Agency Contract Monitor

_____
Email Address

With a Copy to:

_____
Agency AAG Name

_____
Email Address

Notice to the Processor

_____
Processor Designee

_____
Mailing Address

_____
Phone

_____
Email Address

O. Entire Agreement

This Agreement sets forth the entire agreement and understanding of the Parties relating to the subject matter herein and supersedes all prior or contemporaneous discussions, understandings, and agreements, whether oral or written, between them relating to the subject matter hereof.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

Executed on this day of 202_

By: _____
[Authorized Signatory]
[Name of Agency]

Executed on this day of 202_

By: _____
Processor Authorized Signatory

Approved as to form and legal sufficiency this
day of 202_

By: _____
Assistant Attorney General
[Name of Agency]

DUA Appendix A: Types of Personally Identifiable Information to Be Processed

Contract Number:

The listed types of Personally Identifiable Information are required for the Processor to meet the service provisions written in the Underlying Contract. Alternatively, provide a schema of field names required to meet the stated service provisions.

Specific PII Type(s):

☐ First Name or Initial

☐ Last Name

☐ Address

☐ State or Government Issued Identification number (e.g., SSN, Driver's license, passport, individual tax ID, …)

☐ Financial or other Account Number, Bank Account number, and any required security code, access code, or password

☐ Unique Biometric or Genetic print or image

☐ Geospatial Location

☐ Other:

In the event additional types of PII are processed in the future, a DUA modification that includes the new PII element(s) must be completed prior to processing the data.

DUA Appendix B: List of Processor Personnel with Access to State PII

The Processor shall maintain a current list of personnel (similar to the format below) who are granted access to ***Personal Information.*** The Processor shall provide the list to the State upon request.

Last Name, First Name, MI	Job Position	Date Granted Access	Date Removed Access

DUA Appendix C: CERTIFICATION OF DATA DESTRUCTION

Vendor/Processor's Name # Pursuant to State Contract Number	Processor's Contact Name: Processor's Contact Phone:
Date(s) of Destruction	State Representative Authorizing destruction
Description of Destroyed records, record series, or data sets – Include digital, tapes, hardware, paper	

Inclusive Dates of Destroyed data or records

Method of Destruction (check) (Must be NIST compliant)			
☐ Cross Shred	☐ Block Erase	☐ Degauss	☐ Incinerate
☐ Pulverize	☐ Cryptographic Erase	☐ Melt	☐ List Other:

Outsourced Data Destruction Vendor Name (attach certificate of destruction)

Outsourced Vendor Address

Do the destroyed records listed above constitute all records containing Personal Information/Personally Identifiable Information provided to the Processor as part of the State Contract? ☐ Yes ☐ No

If Processor retains any PI/PII related to State Contract number _____, the Processor is bound by contract to maintain reasonable security measures to protect the data until the Processor securely returns the data to the State or destroys the data.

I attest that the above is true and accurate:

Authorized Signatory Name	Title
Authorized Signature	Date

Witness Date