3.2: Example of Data Ownership Contract Language

This guide includes sample contract language related to each element of data ownership described in Tool 3.1: Understanding Data Ownership.

To most effectively use this tool, we recommend first reading 3.1: Understanding Data Ownership to better understand the core elements of data ownership and related considerations.

The sample language for each element is only an example. Any contract will need to be developed in accordance with agency policies with input from your legal team. The service provider or contractor is represented by the word PROVIDER, and the agency is called the Customer.

# Data Management

*On an ongoing basis PROVIDER preserves multiple copies of Customer data from which data can be recovered in the event of accidental deletion or data loss. PROVIDER stores copies of Customer data and data recovery procedures in different physical locations from the primary equipment processing the Customer data.*

*PROVIDER maintains records of personnel authorized to access the systems that contain Customer Data. PROVIDER identifies those personnel who may grant, alter, or cancel authorized access to data and resources. PROVIDER ensures that individuals have separate identifiers where more than one individual may access the same system containing Customer data.*

# Data Location

*Customer data that PROVIDER processes on Customer’s behalf will be transferred to and stored and processed in the United States. Any subcontractors that may interact with customer data will also maintain facilities in the United States and will ensure all Customer data is provisioned within the United States.*

Data Access

*Customer data will be used only to provide Customer with the defined services and for purposes compatible with providing those services. PROVIDER will not use Customer data or derived information for any commercial purposes. Customer retains all rights, titles, and interests in and to their data, and PROVIDER acquires no rights to Customer data other than the rights granted to provide the service. PROVIDER will not disclose Customer data except as directed by the Customer or as required by law. PROVIDER will provide Customer on request with an audit report detailing all access to Customer data.*

Data Privacy/Confidentiality

*Access controls to be applied to the services offered by PROVIDER include authentication via passwords and/or two-factor authentication, encryption of data in transit and at rest, and logging of access on several levels. Data is accessible and manageable only by properly authorized staff, direct database query access is restricted, and application access rights are established and enforced by PROVIDER. The content of communications (including sender and recipient addresses) sent through some email or messaging services between the Customer and PROVIDER may not be encrypted. Customer is solely responsible for the results of its decision to use such unencrypted communications or transmissions.*

Data Rights Retention

*Customer will have the ability to access and extract data stored in service at all times during the term of service. PROVIDER will retain Customer data stored in the service in a limited function account for 180 days after expiration or termination of service agreement so that Customer may extract the data. At the end of the 180-day retention period, PROVIDER will disable Customer’s account and delete Customer data. Customer is solely responsible for the retention or extraction of software provided by Customer. PROVIDER has no liability for the deletion of data as described in this section.*