UMBRELLA DATA SHARING AGREEMENT K3688
BETWEEN
STATE OF WASHINGTON
OFFICE OF FINANCIAL MANAGEMENT
AND

AGENCY NAME Washington's Lottery	**DSA #** K122

Table of Contents

UMBRELLA DATA SHARING AGREEMENT

This Umbrella Data Sharing Agreement ("DSA or Agreement") is entered into by and between the **OFFICE OF FINANCIAL MANAGEMENT**, hereinafter referred to as "OFM or DATA PROVIDER", and Washington State

Agency Name	

hereinafter referred to as "RECIPIENT", pursuant to the authority granted by chapter 39.34 of the Revised Code of Washington, relevant federal statutes, and related regulations.

OFM DSA Administrator:		**RECIPIENT** DSA Administrator	
Name:	Becci Riley	Name:	Joshua Johnston
Title:	Executive IT Contracts Administrator	Title:	Deputy Director
Division:	Legal & Legislative Affairs	Division:	Executive
Address:	302 Sid Snyder Ave SW Olympia, WA 98501	Address:	814 4th Ave E Olympia, WA 98506
Phone:	360.522.3575	Phone:	360-810-2878
E-mail:	Becci.riley@ofm.wa.gov	E-mail:	Joshua.johnston@walottery.com

1. UMBRELLA DSA APPLICABILITY

This Umbrella DSA applies to all Data shared between the parties and documents the general terms and conditions, procedures, roles and responsibilities, and appropriate data security constraints required for the accurate exchange of Data between the parties.

Data Sharing Addendum (Addendum): Specific Data provided to RECIPIENT will be documented in addenda that will document the purpose for which the Data is shared. Each Addendum will be attached and subject to this DSA. Each Addendum will include any additional or special requirements for handling of the Data that is the subject of the Addendum.

2. DEFINITIONS

"Addendum" means an attachment to this Data Sharing Agreement that describes the Data or information to be shared with RECIPIENT and the handling of such Data, which may be in addition to the requirements in the body of this Agreement or specific to the activities authorized under the addendum.

"Agreement" means this Data Sharing Agreement, including all documents attached or incorporated by reference.

"Data Access" refers to methods and rights granted to RECIPIENT to receive Data.

"Data Classification" refers to the sensitivity of Data as defined by the Office of the Chief Information Officer (OCIO) in OCIO Standard 141.10, as may be modified by the OCIO from time to time. Current categories are set forth in Attachment 1, OCIO Data Classification.

"Data Encryption" refers to ciphers, algorithms or other encoding mechanisms that will encode Data to protect its confidentiality. Data encryption may be required during data transmission and/or data storage depending on the level of protection required for this Data.

"Data Storage" refers to the state Data is in when at rest.

"Data Transmission" refers to the methods and technologies to be used to move a copy of the Data between systems, networks, and/or workstations.

"Disclosure" means to permit access to or release, transfer, or other communication of Data or information by any means including oral, written, or electronic means.

"Data" means information, including but not limited to PII, provided by OFM under this DSA, whether that information originated in OFM or in another entity.

"OCIO" means the Washington State Office of the Chief Information Officer.

"Personally Identifiable Information (PII)" means information identifiable to any person, including, but not limited to, information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, social security numbers, driver's license numbers, credit card numbers, any other identifying numbers, and any financial identifiers.

3. PERIOD OF AGREEMENT

This DSA shall begin on the date of execution and end on June 30, 2026 unless terminated sooner or extended as provided herein. This DSA may be extended as needed by the parties in up to three (3) year increments. Such extensions will be by mutual agreement and will be in the form of written amendment(s) to this DSA.

The parties agree that they will review the terms and conditions of this DSA and any then current Addendum at least annually to ensure that the content is accurate.

The term of any Addendum executed under this DSA will be stated therein. The expiration date of any Addendum may not exceed the then-current expiration date of this DSA.

4. DATA SECURITY (OCIO 141.10.4.2(5)); (OCIO 141.10.4.2(6))

Any data-specific requirements related to the subjects in this section will be set out in addenda to this DSA.

a. Authorized Access Only

Access to the Data provided by OFM will be restricted to RECIPIENT staff, officials, and agents who are authorized to access the Data and need it to perform their official duties as detailed in the Addendum under which the Data is shared.

b. Data Storage

All Data provided by OFM must be stored in a secure environment with access limited to the least number of RECIPIENT staff, officials, and agents needed to complete the purpose of the Addendum under which the Data is shared.

c. Data Protection

In all cases and under each Addendum, RECIPIENT will take due care and take reasonable precautions to protect OFM provided Data from unauthorized physical and electronic access. RECIPIENT will strive to meet or exceed the requirements of the OCIO policies and standards outlined in policy 141.10 (located at: https://ocio.wa.gov/policy/securing-information-technology-assets-standards) for data security and access controls to ensure the confidentiality, availability and integrity of all Data shared.

d. IT Data Security Administration

RECIPIENT's IT Data Security Administrators will provide to the OFM IT Data Security Administrator relevant documentation that outlines the data security program components supporting data shared under each Addendum. This documentation will define all data security methods and technology for each individual data exchange to ensure RECIPIENT is in compliance with all appropriate OCIO security standards and/or other applicable standards for such data.

This documentation will serve to satisfy any potential requirement each agency may have under OCIO Security Standards to document the management and security of Data and information.

5. DATA CONFIDENTIALITY

RECIPIENT acknowledges the personal or confidential nature of the Data shared hereunder and agrees that RECIPIENT staff with access to the Data will comply with all laws, regulations, and policies that apply to protection of the confidentiality of the Data. If Data provided under this DSA is to be shared with a contractor, the contract(s) must include all of the data security provisions within this DSA and within any amendments, addenda, attachments, or exhibits within this DSA.

a. Non-Disclosure of Data

1) Individuals accessing Data by reason of this DSA and its addenda will do so only for the specific purpose described in the Addendum under which the Data is shared. Data may not be repurposed across addenda for any reason.

2) OFM, at its discretion, may at any time disqualify any person from authorized access to Data provided pursuant to this DSA. Notice of disqualification shall be in writing and shall immediately upon delivery of notice to RECIPIENT, terminate the disqualified person's access to any Data provided under this DSA. Disqualification of one or more persons by OFM does not affect other persons authorized by or pursuant to this DSA.

b. Penalties for Unauthorized Disclosure of Information

In the event RECIPIENT fails to comply with any term of this DSA, OFM shall have the right to take such action as it deems appropriate to protect the OFM Data from disclosure or otherwise mitigate potential harm resulting from such failure to comply. The exercise of remedies pursuant to this paragraph shall be in addition to all sanctions provided by law, and to legal remedies available to parties injured by unauthorized disclosure.

c. Data Segregation

1) OFM Data shall be segregated or otherwise distinguishable from non-OFM Data. This is to ensure that when no longer needed by the RECIPIENT, all OFM Data can be identified for return or destruction. It also aids in determining whether OFM Data has or may have been compromised in the event of a security breach.

2) When it is not feasible or practical to segregate OFM Data from non-OFM Data, then both the OFM Data and the non-OFM Data with which it is commingled shall be protected as described in this DSA and the relevant Addendum under which such Data is shared.

6. NOTIFICATION OF DATA BREACH

If RECIPIENT or its agents detect a compromise or potential compromise in the IT security for Data provided under this DSA, such that PII may have been accessed or disclosed without proper authorization, RECIPIENT must give notice to OFM within one (1) business day of discovering the compromise or potential compromise. RECIPIENT must take corrective action as soon as practicable to eliminate the cause of the breach and, in consultation and collaboration with OFM, shall be responsible for ensuring that appropriate notice is made to those individuals whose personal information may have been improperly accessed or disclosed. In addition, if credit monitoring is required as a result of the breach, then RECIPIENT will be financially responsible for the cost of such credit monitoring.

7. DISPOSITION OF DATA

Upon termination of this DSA, or any Addendum subject to this DSA, RECIPIENT agrees to erase, destroy, and render unreadable all Data received under this DSA or the relevant Addendum and provide written notification (See Exhibit A, Certification of Data Disposition) within fifteen (15) days of the date of disposal to the Addendum Administrators with a copy to the OFM DSA Administrator set forth in this DSA. Destruction methods must comply with OCIO policy 141.10 section 8.3 and follow the OCIO Media Handling and Data Disposal Best Practices. (OCIO 141.10.4.2(7)).

8. ON-SITE OVERSIGHT AND RECORDS MAINTENANCE

RECIPIENT agrees that OFM shall have the right, at any time, to monitor, audit and review activities and methods in implementing this DSA in order to assure compliance therewith, within the limits of RECIPIENT' technical capabilities.

Both parties hereto shall retain all records, books, or documents related to this DSA for six years, except Data destroyed as set forth in the section titled *DISPOSITION OF DATA* of this DSA. The Office of the State Auditor, federal auditors, and any persons duly authorized by the parties shall have full access to and the right to examine any of these materials during this retention period.

9. INDEMNIFICATION

Each party to this DSA shall be responsible for any and all acts and omissions of its own staff, employees, officers, agents and independent contractors. Each party shall furthermore defend and hold harmless the other party from any and all claims, damages, and liability of any kind arising from any act or omission of its own staff, employees, officers, agents, and independent contractors.

10. AMENDMENTS AND ALTERATIONS TO THIS DSA

With mutual consent, OFM and RECIPIENT may amend this DSA at any time, provided that the amendment is in writing and signed by authorized representatives of each party.

11. ORDER OF PRECEDENCE

In the event of an inconsistency in this DSA, an Addendum hereto, or any amendment, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

a. Applicable Federal and State laws;
b. The terms and conditions of this DSA whether by reference or otherwise.
c. Addenda to this DSA

12. TERMINATION

a. <u>For Convenience</u>

Either party may terminate this DSA in whole or in part, including any Addendum attached hereto, with thirty (30) days' written notice to the other party's Agreement Administrator named on Page 1. In case of termination, any and all Data that is the subject of such termination that was provided by OFM pursuant to this DSA shall either be immediately returned to OFM or immediately destroyed, as instructed by OFM. As set forth in the section titled *DISPOSITION OF DATA* of this DSA, written notification to OFM confirming the disposition of the Data must be given.

b. For Cause

OFM may terminate this DSA, in whole or in part, at any time prior to the date of completion if and when it is determined that RECIPIENT has failed to comply with the conditions of this DSA. OFM shall promptly notify RECIPIENT in writing of the termination and the reasons for termination, together with the effective date of termination. In case of termination, the Data provided by OFM shall be returned to OFM or destroyed on or before the date of termination, as instructed by OFM. As set forth in the section titled *DISPOSITION OF DATA* of this DSA, written notification to OFM confirming the disposition of the Data must be given.

13. GOVERNING LAW

This DSA, including any amendments, addenda, attachments, or exhibits hereto, shall be construed under the laws of the State of Washington. Venue shall be proper in Superior Court in Thurston County, Washington.

14. SEVERABILITY

The provisions of this DSA are severable. If any provision of this DSA is held invalid by any court; that invalidity shall not affect the other provisions of this DSA and the invalid provision shall be considered modified to conform to the existing law.

15. SIGNATURES

The parties have read and understand this DSA and hereby assert that they are authorized to enter into this DSA on behalf of their organization. The signatures below indicate agreement between the parties.

OFFICE OF FINANCIAL MANAGEMENT		**RECIPIENT:** Washington's Lottery	
DocuSigned by: Roselyn Marcus 30768F7E7F2D4EB...	02/17/2022	DocuSigned by: Joshua Johnston 69DB022B1CBE4FC...	02/22/2022
Signature	Date	Signature	Date
Roselyn Marcus		Joshua Johnston	
Printed Name		Printed Name	
Assistant Director Legal & Legislative Affairs		Deputy Director	
Title		Title	

APPROVED AS TO FORM:

Cam Comfort, AAG

/s/ 1.31.2022

EXHIBIT A
Certification of Data Disposition

Recipient Agency Name: Washington's Lottery

OFM Data Sharing Agreement (DSA) Number: K 3688

OFM Data Sharing Addendum: Addendum for One Washington Project Dated: 02/22/2022

Date of Disposition ________________________

Media (type, serial number, other unique identifiers) ____________________________________

Date the media was sanitized: ____________________________________

The person performing the activity was: ____________________________________

The method used (reference Office of the Chief Information Officer standard 141.10 at https://ocio.wa.gov/policy/media-handling-and-data-disposal-best-practices for most current acceptable methods) to render all Data unusable (e.g. software tool used and/or physical destruction of the media) was:

____

All copies of any Data sets related to this DSA/Addendum that have not been disposed of in a manner described above, have been returned to OFM's Addendum Administrator named below:

Name/Title ____

Media to be disposed must stay within the control of the agency from the time it is collected until the time it is sanitized. Storage media to be disposed should be collected by, and in the constant possession of dedicated, trusted personnel. Media must be maintained in a secure, locked area until it can be sanitized.

By the authorized signature below, the Data Recipient hereby certifies that the Data provided by OFM has been handled and rendered unusable as indicated above and as required in the DSA designated above.

Signature of Recipient Addendum Administrator _____________________________ Date: ___________

Name/Title ____

Return original to OFM Addendum Administrator indicated on page 1 of the referenced Addendum. Retain a copy for your records.

ATTACHMENT 1

OCIO Data Classification

Office of the Chief Information Officer DATA CLASSIFICATION as set forth in OCIO Standard 141.10

Category 1 – Public Information. Public information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

Category 2- Sensitive Information. Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

Category 3 – Confidential Information. Confidential Information is information that is specifically protected from either release or disclosure by law. It may include but is not limited to:

a. Personal information as defined in RCW 42.56.590(10) and RCW 19.255.010. Information about public employees as provided in RCW 42.56.250.
b. Lists of individuals for commercial purposes as provided in RCW 42.56.070(8).
c. Information about the infrastructure and security of computer and telecommunication networks as provided in RCW 42.56.420(4).

Category 4 – Confidential Information Requiring Special Handling. Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.
b. Serious Consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.