**Data Use Agreement**

The undersigned parties agree to the following terms of this Data Use Agreement, effective as of the date of last signature ("Agreement").

I. The Agreement is between [INSERT RECEIVING PARTY HERE] with a principal place of business at [RECEIVING PARTY ADDRESS], and the University of Notre Dame ("Holder") with a principal place of business at Notre Dame, IN, USA.

II. The terms of this Agreement shall be effective as of [INSERT EFFECTIVE DATE], and shall remain in effect until all Data provided to the Recipient is destroyed or returned to the Holder.

III. For purposes of this Agreement, the "De-identified Data" refers to data elements found in Addendum A.

IV. Data will be shared between the Parties in connection with research conducted under the following protocols: Tesserae.

V. De-identified data collected during each study may be used for data analysis and reporting within scope of each study. It may also be retained and used by the Parties beyond the scope of each study, including after the period of study is complete.

VI. The following persons will have access to the Data during the period of each study:
   a. Receiving Party's research staff that require access to the Data in connection with each study;
   b. Receiving Party's authorized staff and institutional officials responsible for overseeing each study, as necessary to carry out that responsibility;
   c. Permitted agents and subcontractors;
   d. Individuals and institutions permitted in each Disclosing Party's study protocol; and
   e. Third party institutions not listed on Disclosing Party's study protocol with written permission in any form from Disclosing Party.

VII. In consideration of Data being shared between the Parties, the Receiving Party shall:
   a. Only use and disclose the Data only as permitted by this Agreement or as otherwise required by law, and to not use or further disclose the Data.
   b. Permit only the above-specified individuals to use or receive the Data.
   c. Use appropriate safeguards to prevent use or disclosure of the Data other than as provided for by this Agreement;
   d. Report to the Disclosing Party any use or disclosure not provided for by this Agreement of which it becomes aware within 15 days of becoming aware of such use or disclosure;

e. Ensure that any agents and subcontractors to whom it provides the Data agree to the same restrictions and conditions that apply to the Receiving Party with respect to the Data
f. Not reidentify or attempt to reidentify any potentially identifiable personal information received under the data agreement;
g. Take reasonable steps, including contracts, technical measures, or workplace rules, to prevent any employee, agent, consultant, contractor, affiliate, subcontractor, or other related party from reidentifying or making an attempt to reidentify any potentially identifiable personal information that the recipient received under the data agreement;
h. Not further use or disclose any potentially identifiable personal information received under the data agreement;
i. Maintain reasonable physical, administrative, and technical safeguards to protect against reidentification of potentially identifiable personal information received under that data agreement;
j. In the event that potentially identifiable information in the data is discovered by the recipient:
    i. Promptly notify the program manager of the Multimodal Objective Sensing to Assess Individuals with Context (MOSAIC);
    ii. Promptly notify The Intelligence Advanced Research Projects Activity (IARPA);
    iii. Promptly notify the Discloser.
k. Inform a potential discloser in writing before entering into any data agreement of any actual or reasonably likely breaches of other data agreements that the recipient entered into during the past 10 years;
l. In the event of a data breach:
    i. Promptly report any breach of this data agreement to the Discloser;
    ii. In the event that the recipient learns that potentially identifiable personal information that the recipient obtained under this data agreement has been reidentified, comply with applicable Federal or State security breach notification laws.

VIII. This Agreement shall not be assigned by Recipient without the prior written consent of the Holder.

IX. Each party agrees that it will be responsible for its own acts and the results thereof to the extent authorized by law and shall not be responsible for the acts of the other party or the results thereof.

X. Miscellaneous

a. No Agency. All parties acknowledge that they are independent contractors, and nothing contained herein shall be deemed to create an agency, joint venture, franchise or partnership relation between the parties.
b. None of the parties hereto shall have the right, directly or indirectly, to assign, transfer, convey or encumber any of its rights under this Agreement without the prior written consent of the other party.
c. Notwithstanding anything to the contrary contained herein, to the maximum extent permitted by law, in no event will either party be responsible for any incidental, consequential, indirect, special, punitive, or exemplary damages of any kind.
d. Entire Agreement. This Agreement fully supersedes any and all prior agreements or understandings between the parties hereto or any of their respective affiliates with respect to the subject matter hereof, and no change in, modification of or addition, amendment or supplement to this Agreement shall be valid unless set forth in writing and signed and dated by both parties hereto subsequent to the execution of this agreement.

XI. Definitions:

a. Deidentification: personal information that has been processed in some fashion to reduce the ability to identify the individuals to whom the data refer. It does not mean that information has been anonymized to the point where reidentification is never possible.
b. Discloser: A person who discloses potentially identifiable personal information to another person pursuant to a data agreement.
c. Holder: Party sharing the data with the Recipient.
d. Overt Identifier: Any personal information that identifies or can readily be used to identify a particular individual, and includes a name, address, Social Security number, account number, license number, serial number, telephone number, electronic mail address, Internet protocol address, webpage address, or biometric, that alone or in combination with other information identifies or can readily be used to identify a particular individual.
e. Person: An individual, corporation, company, foundation, association, society, partnership, firm, non-profit organization, school, college, or university, or a department, agency, or other instrumentality of Federal, State, or local government.
f. Personal Information: Information about an individual that may or may not include an overt identifier.
g. Potentially Identifiable Personal Information: Any personal information without any overt identifiers.
h. Public Website: A facility by which a person displays information to the general public on the Internet or any comparable successor technology.
i. Recipient: A person who receives potentially identifiable personal information from another person pursuant to a data agreement subject to this Agreement.

j. Research: A systematic investigation designed to develop or contribute to generalizable knowledge, but does not include marketing research.

**IN WITNESS WHEREOF**, the Parties have caused this agreement to be executed as of the day and year of last signature.

| **[RECIPIENT]** | **University of Notre Dame** |
|---|---|
| By:_____ | By:_____ |
| Name: | Name: Aaron Striegel |
| Title: | Title: Professor, PI - Tesserae |

**Addendum A**

All data is initially shared via access to a Google Drive. Each field should be changed as appropriate under the shared column.

| Shared | Dataset | Overview |
|---|---|---|
| Yes | Tesserae – Base Data | The base data for Tesserae as described in the Wiki. |
| No | Tesserae – Enhanced Data | The enhanced data for Tesserae including more sensitive but still de-identified pieces of information relevant to the study. |
| Upon Request | Social Media | The social media dataset is fully de-identified and is made available as requested. |