

Data Access Agreement



Parties			
“We” or “Us” or “Our”	The University of Melbourne Parkville, VIC 3010 ABN 84 002 705 224	“You” or “Your”	The individual seeking access to the Data and, where applicable, the institution with which they are affiliated and on whose behalf they are accessing the Data.
Department/School/Institute:	Australian Urban Research Infrastructure Network (AURIN).		
AURIN Contact:	Attention: Pascal Perez, Director, AURIN Project The University of Melbourne VIC 3010		
Details			
Project Title	As described in Your application for the Data		
Data	Telstra Data and other data We provide to you under this Agreement		
Format	As agreed by the Parties and approved by Telstra Limited in writing.		
Purpose	You may only access, use and analyse Telstra Data in the sandbox environment provided by Telstra solely for the purpose of developing proof-of-concepts, a Minimum Viable Product and for research purposes agreed in writing by Us and Telstra with You.		
Delivery Date	Upon execution		
Fees	Nil		
End Date	12 months from the Delivery Date		

By clicking ‘I Accept’ on the AURIN Data Provider platform, the User agrees to be bound by this Data Access Agreement. This click-through acceptance constitutes execution of this Agreement, which AURIN enters into as agent for Telstra Limited.

1. Condition Precedent

You agree and acknowledge that Your access to the Data is subject to the written approval of Telstra Limited (**Telstra**) (which will be facilitated by Us). If Telstra approves access to the Data, the Agreed Terms will apply. However, if Telstra does not approve access, this Data Access Agreement will be terminated with immediate effect and neither party will have any liability to the other.

2. Special Conditions

- (a) These Agreed Terms are subject to the special conditions (if any) set out Annexure A.
- (b) In the event of inconsistency between the special conditions and the provisions of these Agreed Terms, the Special Conditions shall apply to the extent of the inconsistency.

3. Supply of the Original Data

- (a) We agree to supply the Data to You for the Purpose on these Agreed Terms.
- (b) You must access the interfaces and environment we provide or make available to you under these Agreed Terms, and use the Telstra Data and Data, in each case, only for the Purpose, and not for any other purpose (including Commercial Purposes) or otherwise in breach these Agreed Terms.
- (c) You must comply with our directions with respect to your access and use of all interfaces, environment and Data pursuant to these Agreed Terms.

4. Ownership and Licence

- (a) Telstra retains ownership of the Data, and all Intellectual Property rights in the Data.
- (b) We grant to You a royalty-free, non-transferable, non-exclusive, non-sublicensable (other than to End Users in accordance with clause 5), revocable (on termination) access licence (via the AURIN Infrastructure) to use the Data for the Purpose only, subject to the terms of these Agreed Terms.
- (c) We will provide the Data in the format and by the Delivery Date as specified in the cover page above.

5. Your use of the Data

- (a) You agree:
 - (i) to only use Telstra Data in accordance with this Agreement, and subject to the restrictions specifically set out with respect to your use of such Telstra Data;
 - (ii) to only store, handle and use the Data for the Purpose, in compliance with all applicable laws and regulations, including, for example, those relating to privacy;
 - (iii) to treat the Data as Our Confidential Information and take all reasonable steps to keep the Data secure and Confidential, and to protect the Data from misuse and unauthorised access;
 - (iv) to ensure that all necessary and relevant ethics and regulatory approvals are in place for the Purpose before You use the Data, and to comply with such approvals at all times;
 - (v) to ensure the Data is only used by You or at Your organisation by End Users directly involved in the Purpose; and
 - (vi) if You are an organisation (i.e. a body corporate), Your End Users will be required to agree to the Terms of Use prior to obtaining access to and using the Data;
 - (vii) if You are an individual (i.e. a natural person) and not an organisation, You will be required to agree to the Terms of Use and satisfy Our reasonable registration and approval procedures prior to obtaining access to and using the Data; and not to transfer the Data to anyone else or, if You are an organisation, outside Your organisation without Our prior written consent.

6. Risk

- (a) We make no representations and, to the extent permitted by law, exclude all express or implied warranties regarding the merchantability or fitness for a particular purpose, or that the use of the Data will not infringe any patent, copyright, trade mark, or other proprietary rights.
- (b) You use the Data at Your own risk. Except to the extent prohibited by law, You assume all liability

for damages which may arise from Your use, storage or disposal of the Data. We will not be liable to You for any loss, claim or demand made by You, or made against You by anybody else, due to or arising from Your use of the Data, except to the extent permitted by law when caused by Our gross negligence or wilful misconduct.

7. Confidentiality

- (a) Each party must:
 - (i) keep the other party's Confidential Information secret and confidential,
 - (ii) only use the other party's Confidential Information for the Purpose, and
 - (iii) take all steps reasonably necessary to protect Confidential Information from unauthorised access, use or disclosure.
- (b) Neither party may disclose the other party's Confidential Information except:
 - (i) to its personnel and other representatives if they need to know the Confidential Information for the Purpose. Each party will be liable to the other party for any unauthorised access, use or disclosure of Confidential Information by its representatives,
 - (ii) if disclosure is required by law or the rules of any stock exchange, provided that it first notifies the other party where practical.
- (c) If asked, each party must return or destroy all copies of the other party's Confidential Information, but it may keep:
 - (i) one (1) copy of the Confidential Information solely for the purpose of compliance with any applicable law or in the event of a dispute arising out of this Agreement, and
 - (ii) any copies of the Confidential Information (on a confidential basis) if they are electronically archived and not readily accessible or contained in board papers or other internal senior management reports.
- (d) **Confidential Information** of a party means all information provided by or on behalf of that party to the other party, in any form and whether before or after the date of this Agreement, and Telstra's

Confidential Information includes the Telstra Data, but does not include information that is:

- (i) in the public domain, other than as a result of a breach of this Agreement,
- (ii) known to the other party before it received it and is not subject to an existing obligation of confidence between the parties,
- (iii) is developed by the other party independently or is received from a third party who is entitled to disclose it lawfully without violating any obligation of confidence by that third party.

8. Privacy & Data Security

- (a) Each party must comply with the *Privacy Act 1988* (Cth) and any other laws and binding industry codes relating to the management of personal information, whether or not it is an organisation bound by those laws and codes, in relation to any personal information that it receives from the other party under this Agreement.
- (b) To the extent that a party holds data received from the other party, it must implement technical and organisational measures in accordance with industry best practice to protect that data from unauthorised access, misuse or interference.
- (c) You must comply with the special conditions in Annexure A.

9. Branding

Neither party may use, or authorise anyone else to use, the other party's name, brand and/or logo without the other party's express written permission.

10. Dispute resolution

If a dispute arises between the parties in relation to these Agreed Terms, then the parties agree to negotiate in good faith on a commercially realistic basis to resolve the dispute. If a dispute cannot be resolved by negotiation within 30 days of one party notifying the other in writing of the issue(s) in dispute, the matter must be referred to an agreed alternative dispute forum in Melbourne, Victoria before commencing any legal proceedings (other than interlocutory proceedings) in relation to the dispute.

11. Term and termination

- (a) These Agreed Terms start on the date they are signed by both parties and will end on the End Date specified in the cover page.
- (b) We may terminate these Agreed Terms without any liability on 5 days' written notice to you.
- (c) You agree and acknowledge that if Telstra terminates access to the Data Your access to the Data will cease and We have no liability to you in relation to such access.
- (d) Either party may terminate these Agreed Terms by written notice to the other if the other breaches the Agreed Terms and that breach is not remedied within 30 days after receipt of a notice in writing to remedy the breach.
- (e) On expiry or termination of these Agreed Terms, You must (at Your own cost) return or destroy all remaining Data according to Our reasonable instructions.
- (f) Clauses 4(a), 3, 6, **Error! Reference source not found.**, 7, 9, 10 and 11(e) survive the expiration or termination of this Agreement, along with any provision which by its nature is intended to so survive.

12. General

- (a) These Agreed Terms are subject to the laws of the State of Victoria, Australia.
- (b) A party must not assign or otherwise transfer rights and obligations under these Agreed Terms to anyone else without the consent of the other party, which consent must not be unreasonably withheld.
- (c) These Agreed Terms override all prior written agreements between the parties in respect of the Data transfer.
- (d) These Agreed Terms may only be changed if both parties agree to do so in writing signed by both parties.
- (e) Both parties must do all such further acts, and execute such further documents and instruments, as may be necessary to give full effect to the rights and obligations under these Agreed Terms.
- (f) Separate copies of these Agreed Terms may be signed by each party, each of which will be an original (including if the copy is electronic), and all

signed copies will together constitute one document.

- (g) Any notice or other communication required to be given under these Agreed Terms must be provided in writing to the UoM Contact or Your Contact (as appropriate).

13. Definitions

In these Agreed Terms, capitalised words have the meaning given in the cover page or as set out below:

AURIN Infrastructure means infrastructure managed by AURIN as controlled and administered by the Licensor such as the 'AURIN Data Provider' available at <<https://aurin.org.au/resources/aurindataprovder/>>.

Commercial Purposes means the sale, lease, licence or transfer of the Data or the use of the Data for contract research, to produce or manufacture products for general sale, or to conduct research activities that result in any sale, lease, licence or transfer of the Data to a for-profit organisation. Industrially sponsored academic research shall not be considered use of the Data for commercial purposes unless the criteria outlined above in this definition are met.

Confidential Information means information disclosed by a Discloser to a Receiver under these Agreed Terms which is identified as confidential at the time of the disclosure and for the avoidance of any doubt, includes the Data. Disclosures are not confidential if the information disclosed is: (a) publicly available; (b) rightfully known to the other before disclosure; or (c) independently created by the other without access to the disclosed information.

Data means data being transferred and related information, supplied by Us under these Agreed Terms, as described in the cover page.

End Users means end users who have met Our reasonable registration and approval procedures, and have agreed to the Terms of Use.

Intellectual Property means all rights resulting from intellectual activity whether capable of protection by statute, common law or in equity and including copyright, discoveries, inventions, patent rights, registered and unregistered trade marks, design rights, circuit layouts and plant varieties and all rights and interests of a like nature including but not limited to methods and techniques, together with any documentation relating to such rights and interests whether registered or unregistered and existing in Australia or elsewhere in the world.

Telstra Data means the Data, including location data, and all other data provided or otherwise made available by Telstra to Us for provision to You under these Agreed Terms.

Terms of Use means the terms of use for AURIN Infrastructure in the form set out in Schedule 2, as amended from time to time and available on the AURIN website at <<https://aurin.org.au/legal/aurin-terms-of-use/>>.

Agreed Terms

Annexure A – Special Conditions

15. DATA BREACH

15.1 You must:

- (A) keep the Telstra Data secret and confidential, and must implement technical and organisational measures to protect Telstra Data used by it (but this does not extend to measures in Telstra's specified environment);
- (B) not disclose or make accessible any Telstra Data to a person (including itself) outside Telstra's specified environment or location without Telstra's written consent;
- (C) on request by Us, promptly provide an up-to-date list of all its personnel approved by Telstra and to whom access to Telstra Data has been granted; and
- (D) be responsible for all costs incurred by Telstra to immediately restore the Telstra Data if any Telstra Data is lost, destroyed, corrupted or altered in connection with use by You, except to the extent such loss, destruction or alteration to Telstra Data is caused or contributed to by Telstra.

15.2. If You become aware of a Data Breach, or are or may be required by law to disclose any Telstra Data, then You must immediately notify Us and the 'Telstra Security Response' team by telephone ((+61) 1300 757 799) and email (security.response.team@team.telstra.com) or by using such other contact details as Telstra may notify You through Us.

15.3. In the event of a Data Breach with respect to the acts or omissions of, or the environment of, You, Your personnel must at Your cost:

- (A) promptly disclose to Us (for disclosure to Telstra) all information and documents relevant to that Data Breach, including all relevant information about the processes, procedures, protocols, and security practices and procedures used in performing the Project;
- (B) co-operate with Us and Telstra in investigating what has occurred and the circumstances surrounding that Data Breach; and
- (C) give Us and Telstra reasonable access to Your premises, personnel, processes and systems required by Us and Telstra for the purpose of carrying out an investigation into the Data Breach.

15.4 You must not disclose to any third party the existence or circumstances surrounding any Data Breaches without Our or Telstra's prior written approval.

15.5 Where the Data Breach relates to 'Personal Information' as defined under the *Privacy Act 1988* (Cth) and the Data Breach is:

- (A) within the Telstra IT environment, Telstra will be solely responsible for determining whether the Data Breach results in a real risk of serious harm to any of the individuals to whom the Personal Information relates; or
- (B) within the Our IT environment, We will be solely responsible for determining whether the Data Breach results in a real risk of serious harm to any of the individuals to whom the Personal Information relates, but if such Data Breach impacts or relates to Telstra Data, then We must act in good faith and consult with Telstra in relation to Our assessment of the risk and impact of such Data Breach.

15.6 If You are prohibited by law or otherwise unable to give Us or Telstra sufficient notice under clause 15.2 for Us or Telstra to reasonably prepare and seek a protective order or other appropriate remedy in relation to any proposed disclosure, You must take reasonable steps to challenge or resist the legal requirement to disclose.

16. DATA SECURITY

16.1 You must patch any device, server, system or network elements in Your environment that connects to Telstra's networks or through which Telstra Data may be accessed as soon as reasonably practicable after a security patch becomes available, and must procure each Third Party Personnel to ensure that such personnel's device, server, system or network elements are patched accordingly.

- 16.2 You must ensure that any laptop or tablet used to access, store or process Telstra Data has end point encryption installed.
- 16.3 You must:
- (A) only access or permit its personnel to access Telstra Data as permitted under this Agreement;
 - (B) establish and maintain complete, accurate and up-to-date records (Data Records) of Telstra Data accessed, which must include details of Your personnel who accessed the Telstra Data and the date and purpose for which it was accessed; and
 - (C) at Our or Telstra's request, provide Us and Telstra with copies of the Data Records in real time, and if not possible, within 24 hours of real time.
- 16.4 You must have in place appropriate software, systems and processes that are designed to detect and prevent loss of Telstra Data.
- 16.5 You must only access and use the Telstra Data in the environment specified and provided by Telstra.
- 16.6 If You are permitted to store Telstra Data by Telstra, then You must, for backup copies made by it (**Back-Ups**):
- (A) store Back-Ups securely notified by Telstra through Us to You;
 - (B) retain Back-Ups for 30 business days, which period may be extended at the request of Us or Telstra, and at no additional charge, for any further period nominated by Us or Telstra;
 - (C) implement a tested and proven secure backup and restore plan to ensure that all Telstra Data will be backed up in accordance with the requirements of this clause 16.5; and
 - (D) ensure that Us and Telstra has access at all times to the Telstra Data while it is in Your possession or control and provide that Telstra Data to Telstra at Our or Telstra's request.
- 16.7 You must:
- (A) ensure that any server or computer that is used by You to access or use Telstra Data that can access the internet or be accessed from the Internet undergo vulnerability scans:
 - (1) at least on a monthly basis; and
 - (2) promptly following any system change; and
 - (B) if a vulnerability scan performed by AURIN reveals any vulnerabilities:
 - (1) immediately take all necessary steps to remediate such vulnerabilities; and
 - (2) provide a report to Us and the 'Telstra Response Team' detailing the vulnerabilities and the remediation taken as soon as reasonably practicable.
- 16.8 If You are required to replace data storage infrastructure, then You must ensure that:
- (A) any materials and data that is derived from Telstra Data is permanently erased from the infrastructure; or
 - (B) the infrastructure is destroyed in a secure destruction centre.
- 16.9 Where Telstra Data is required to be de-identified, destroyed or permanently erased by You under this Agreement the de-identification, destruction or erasure method must be approved in writing by Us and Telstra.

17. ADDITIONAL OBLIGATIONS

- 17.1 You must not identify Telstra as the source of any data, including the Data and Telstra Data, without Our and Telstra's prior written consent (consent, including in relation to citations and for publication requirements, will not be unreasonably withheld).
- 17.2 You must not:

- (a) use the Telstra Data in isolation to inform policy or service provisions and you must, and are solely responsible for, appropriately cross referencing and checking the Telstra Data to test validity;
- (b) take any action, analyse or perform analytics on the Telstra Data to generate insights or use, analyse, access, copy, modify, transfer, reverse engineer, disclose or de-anonymise any such Telstra Data, including personal information and attempting to re-identify any individuals or otherwise, without Our prior written consent;
- (c) whether directly or indirectly (including through a third party) store the Telstra Data in, or incorporate or combine the Telstra Data with, software or materials offered under an open source licence. For the avoidance of doubt, this restriction does not prevent You from using open source software or tools to access, analyse, or otherwise use with the Telstra Data for the Purpose, provided that the Telstra Data itself is not integrated as part of any open source software or materials;
- (d) take any steps or permit any person to alter, modify or display the Telstra Data in a manner that reduces the level of aggregation, including of any data type or field within the Telstra Data or otherwise increases the risk of re-identification of any data subject;
- (e) commingle or combine the Telstra Data with any other information or data (including publicly available or third party data) or otherwise enable or facilitate such combination without Our and Telstra's prior written consent (which may be withheld if we reasonably believe it would result in an increased re-identification risk);
- (f) use or authorise any person to use any data made available by Telstra and Us with or as part of Telstra Data in any manner that has not been approved by Telstra and Us, and must ensure that no measurement or analytics are applied or run over the data provided to You;
- (g) resell, rent, loan, sub-licence, lease or distribute the Telstra Data to any third party, or otherwise through a service bureau or outsourcing offering;
- (h) use the Telstra Data in a manner that may expose Telstra and Us to any claim, legal or administrative action;
- (i) whether directly or indirectly build a competitive product or service; and
- (j) without Our and Telstra's prior written consent, use the Telstra Data to:
 - (i) train any artificial intelligence or machine learning models and software;
 - (ii) publish, sell, rent, transfer or provide any person with access to any such data;
 - (iii) associate or link such data with any individual; and
 - (iv) use such data to target or engage with any person.

Notification to Us and Telstra

- 17.3 You must immediately notify Telstra and Us if you suspect or become aware that there is, or has been, any breach of clause 17.2 above (including any potential or actual re-identification any data subject or individual arising out of or in connection with Telstra Data (or any part of it)).

Deletion of Telstra Data

- 17.4 You must:
- (a) at Our request, delete and destroy all copies of the Data and Telstra Data in your possession and control; and
 - (b) delete and destroy, and certify such deletion and destruction to us in writing, all copies of the Data and Telstra Data in your possession and control on the earlier of: (i) the date You no longer require the Data and Telstra Data for the Purpose; and (ii) the date of termination or expiry of these Agreed Terms or your engagement with Us.

Intellectual Property

- 17.5 Despite any other provision to the contrary and as between the parties, Telstra owns all rights (including intellectual property rights) in the Telstra Data (including all modifications or enhancements). You irrevocably assign immediately on creation all rights, title and interests in any such data to the extent that You may at any time acquire any right, title or interest, including Intellectual Property Rights, in such data.
- 17.6 You must ensure that all Telstra Data must only be used, hosted and accessed in Australia.

Fundamental term

- 17.7 This clause 17 is a fundamental term of these Agreed Terms.

18. DEFINITIONS

- 18.1 For the purpose of these data security and data breach provisions:

Data Breach means any actual, apparent, suspected or anticipated:

- (1) impairment, compromise or damage to the confidentiality, reliability, integrity, value or assurance of Telstra Data;
- (2) flaw or vulnerability of any kind in the security controls or other measures used to protect Telstra Data;
- (3) misuse or loss of, interference with or unauthorised access to, modification of or disclosure of Telstra Data; and/or
- (4) breach of Your obligations relating to any Telstra Data under this Agreement.