**MEMORANDUM OF AGREEMENT (herein “the Agreement”)**

Between:

University of Cape Town acting through DataFirst (hereinafter referred to as “DataFirst”)

A university incorporated in terms of the Higher Education Act, 1997, and the statute of the University of Cape Town, as published and gazetted on 24 January 2020 in Government Gazette No 41, 42967 and amended under Government Gazette No 45954, Government Notice No 1793 of 25 February 2022 herein represented by the Registrar of the University of Cape Town and being duly authorized thereto, having its principal place of business at Bremner Building, Lower Campus, Lovers’ Walk, Rondebosch, 7700, Cape Town, South Africa

and:

**[Insert name of Party B]**

(Hereinafter referred to as ‘Party B’)

(DataFirst and Party B are hereinafter collectively referred to as the “Parties” and individually as the “Party”)

1. **PURPOSE AND SCOPE**

The purpose of this MOA is to clearly identify the roles and responsibilities of each Party as they relate to DataFirst curating and publishing research micro-datasets (hereinafter referred to as the “Data”), deposited by Party B.

1. **BACKGROUND**

DataFirst’s research data service, based at the University of Cape Town, gives long-term access to research data on African countries. DataFirst also provides training courses in data analysis and data curation. Our repository is an awardee of the prestigious international [CoreTrustSeal](https://amt.coretrustseal.org/certificates) Trusted Repository Certification, and the only African open research data repository to hold this award.

Party B wishes to collaborate with DataFirst to make their data available to the research community as:

Public access data shared under a Creative Commons [CC-BY Attribution-only use license](https://creativecommons.org/licenses/by/4.0/)

Public access data shared under a Creative Commons CC-BY-SA Attribution plus Share-Like license

Non-Commercial (Licensed) access data shared under a [Creative Commons CC-BY-NC](https://creativecommons.org/licenses/by-nc/4.0/deed.en) Attribution plus Non-Commercial use (research use) license

Data Enclave/Restricted-access use data (shared in our Secure Research Data Centre at the University of Cape Town[[1]](#footnote-1))

1. **RESPONSIBILITIES UNDER THIS MOA: DATAFIRST**

DataFirst shall undertake the following activities related to Data deposited by **[Party B]** as elaborated on in Annexure B:

* 1. Quality-check the data and ensure the data is anonymised for public access.
  2. Disseminate the data in compliance with national legislation pertaining to the protection of personal information[[2]](#footnote-2) and research ethics requirements.
  3. Make the data and documents available in the long term.
  4. Publish informative metadata with the data.
  5. Provide Party B with data quality feedback from data users.
  6. Provide Party B with regular statistics on the use of their data.
  7. Inform data users that they must cite Party B as the data producer in any research publications based on the data.

1. **RESPONSIBILITIES UNDER THIS MOA**: **[Party B]**

Party B shall undertake the following activities:

* 1. Deposit microdata files[[3]](#footnote-3) with DataFirst to be shared openly or with the wider research community
  2. Describe the said data in an inventory to be attached to this Agreement as Annexure “A”.
  3. Warrant that they have the legal right or ethics clearance to collect the data to be deposited with DataFirst.
  4. Warrant that they are the data owners or have permission from the Data owners to deposit the data with DataFirst for sharing.
  5. Provide all data collection and data analysis documentation.
  6. Agree to process usage information supplied by DataFirst in accordance with South Africa’s [Protection of Personal Information Act 2013](https://www.gov.za/documents/protection-personal-information-act).

1. **INTELLECTUAL PROPERTY**

Subject to the further provisions of this clause, all rights, title, ownership, and interest (including intellectual property rights) in and to any materials, which belong to any of the Parties, and/or their vendors and/or licensors (as the case may be) shall at all times remain the sole property of such Party, and/or their vendors or licensors.

Subject to the further provisions of this clause, neither Party shall in any manner alter or remove or affect the display of the respective intellectual property rights notices (and disclaimers) of the other Party and/or their vendors and licensors without the prior written approval of the other Party, and their vendors or licensors where applicable.

1. **SERVICES AND FEE**
   1. DataFirst shall provide the services for the sum per dataset indicated in the attached quotation.
   2. This shall be a one-off fee payable on or before deposit of the data.
   3. Fees do not apply to deposits from national and local government agencies.
2. **DURATION**

This Agreement shall commence on the date of the last Party signing**.**

1. **TERMINATION**

Either Party shall be entitled to terminate this Agreement on three month’s written notice to the other Party.

1. **IT IS MUTUALLY UNDERSTOOD AND AGREED BY AND BETWEEN THE PARTIES THAT**:
   1. Ownership of the data remains with the depositor.
   2. This MOA may be adapted, when necessary, with the agreement of both Parties in writing.
   3. This Agreement may be terminated at the request of either Party.
2. **BREACH CLAUSE**

This Agreement may be cancelled, by written notice by a Party to the other Party, on the grounds of a breach of any term of this Agreement by a Party either:

* 1. summarily if the breach is incapable of remedy; or
  2. if the Party in breach has failed to remedy its breach within 14 days of written notice calling upon it to do so without prejudice to any other rights in law of the Party cancelling the Agreement.

1. **MISCELLANEOUS LEGAL PROVISIONS**
   1. ***Domicilium****:*
      1. The Parties choose for the purpose of this Agreement their *domicilia citandi et executandi* at the following address: -
         1. in the case of DataFirst at:

physical address:

Bremner Building, Lower Campus, Lovers’ Walk

University of Cape Town,

Rondebosch, 7700

and shall be marked for the attention of:

The Registrar

* + - 1. in the case of Party B to:

physical address:

**[Physical address of Party B]**

and shall be marked for the attention of:

**[Legal Signatory for Party B]**

* + 1. a notice or legal process shall be deemed to have been duly given:
       1. seven (7) days after posting, if posted by registered post to the Party’s address in terms of this sub-clause;
       2. on delivery, if delivered to the Party’s physical address in terms of either this sub-clause or the next sub-clause dealing with service of legal documents;
    2. A Party may change its address for this purpose, by notice in writing to the other Party.
    3. Notwithstanding anything to the contrary herein contained, a written notice or communication which has been actually received by a Party will be regarded as sufficient notice, irrespective of the fact that it has not been dispatched to the appointed *domicilium* or delivered to such *domicilium*.
  1. **Whole Agreement**:

This is the entire agreement between the Parties.

This Agreement and **Annexure A** thereto contain all the express provisions agreed on by the Parties regarding the subject matter hereof and the Parties waive the right to rely on any alleged express provision not contained herein.

**No representations**:

Neither Party relies in entering into this Agreement on any warranties, undertakings, representations, disclosures of any nature whatsoever which have not been incorporated into this Agreement as warranties or undertakings.

* 1. **No Variations**:

No amendment, variation or consensual cancellation of this Agreement shall be of any force or effect unless reduced to writing and signed by the Parties.

* 1. **Non-waiver**:

Neither Party shall be regarded as having waived or be precluded in any way from exercising any right under or arising from this Agreement by reason of such Party having at any time granted any extension of time for, or having shown any indulgence to, the other Party with reference to any performance hereunder, or having failed to enforce, or delayed in the enforcement, any right of action against the other Party.

* 1. **Cession**:

Neither Party may cede that Party’s rights or delegate that Party’s obligations without the prior written consent of the other Party.

* 1. **Applicable Law**:

This Agreement shall be interpreted and implemented in accordance with the law of the Republic of South Africa.

* 1. **Confidentiality**:

The contents of this Agreement and its terms are confidential to the Parties and their professional advisers and may not be disclosed by them to anyone whatsoever unless disclosure is required by law, or by order of Court, or for purposes of any legal or arbitration proceedings between them, or unless otherwise agreed between the Parties.

1. **PROTECTION OF PERSONAL INFORMATION**

DataFirst undertakes to process information in accordance with Annexures “C” and “D”.

1. **LIMITATION OF LIABILTY**

Neither Party will be liable to the other Party for any indirect or consequential loss or damages.

The Parties indicate agreement with this MOA by their signatures hereto.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: DataFirst’s Representative

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: DataFirst’s Representative

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: Representative of Party B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: Representative of Party B

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date

**Annexure A. Description of the Data**

The Data provided by Party B is:

**[General description or list of datasets to be deposited by Party B. A list of datasets can be attached to this MOA]**

**Annexure C. How DataFirst’s Open Data Repository Complies with POPIA**

**Sharing Anonymised Data**

DataFirst complies with South African legislation, specifically South Africa’s [Protection of Personal Information Act](https://popia.co.za/) 4 (POPIA) of 2013 (Information Regulator, South Africa, 2013). POPIA governs the retention and further processing of personal information[[4]](#footnote-4) on data subjects. That is, it governs the holding and processing of personally identifiable information. Thus, the terms of POPIA do not apply to distribution of anonymised information, where a data subject cannot be identified in the data. DataFirst complies with POPIA by sharing only anonymised data online.

Data deposited with us for sharing is generally already anonymised by the data producers. DataFirst always undertakes disclosure control on the data prior to dissemination, to confirm that the data has been confidentialised. DataFirst does also at times receive data files that contain personally identifiable information. The personal information must be held by DataFirst and further processed to anonymise and otherwise prepare the data for research re-use. The retention and processing of this information is done in accordance with POPIA 2013 legislation. Details follow on our compliance with POPIA when holding and processing such personally identifiable information.

**Data Retention**

POPIA 2013 restricts the retention period for the holding of information (to only as long as “necessary for achieving the purpose for which the information was collected”) (Condition 3 Clause 14 (1)) (Information Regulator, South Africa, 2013, pp. 31-32). However, the Act makes provision for long-term retention of personal information “for historical, statistical or research purposes” provided the responsible party holding the information puts safeguards in place to ensure the information is used just for these purposes (Condition 3 Clause 14 (2)) (Information Regulator, South Africa, 2013, p. 32). DataFirst has such safeguards in place. The information is held on our secure server with information security protocols in place and with controlled access for staff only.

**Data Processing**

POPIA requires that further processing of personal information must be compatible with the purpose for which the data was collected (POPIA 2013 Condition 4 Clause 15 (1) pp 33-34). However, it waives this requirement when information[[5]](#footnote-5) is used for research purposes and the responsible party ensures that “further processing is carried out solely for such purposes and will not be published in an identifiable form” (Condition 4 Section 15 (3) (e)) (Information Regulator, South Africa, 2013, p. 34). This type of Personal information deposited with DataFirst is only held by DataFirst for the purposes of creating de-identified data for public distribution. The identifiable data is not published or shared beyond DataFirst staff for the purposes of data cleaning and anonymisation.

**Processing of Special Personal Information**

POPIA also requires consent from data subjects to process special personal information[[6]](#footnote-6) about them, but also waives this requirement if the information is processed “for historical, statistical or research purposes”, and “where seeking consent from data subjects would involve disproportionate effort” and where “guarantees have been put in place to ensure information processing does not negatively affect the privacy of data subjects (POPIA 2013 Part B Clause 27 (d) (i) (ii)) (Information Regulator, South Africa, 2013, pp. 42-43).” DataFirst has the same safeguards in place for special personal information as for other personal information, which is that we house the information securely and process the data only to create anonymised versions for public distribution, and do not publish the “special” in any personally identifiable form.

**Annexure D. How DataFirst’s secure Remote Access Data Enclave Complies with POPIA**

DataFirst complies with South African data legislation, specifically South Africa’s [Protection of Personal Information Act](https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf) 4 (POPIA) of 2013 (Information Regulator, South Africa, 2013). POPIA governs the retention and further processing of personal information on data subjects. The Act defines ‘‘personal information’’ as “information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person (Information Regulator, South Africa, 2013, p. 15).” That is, it governs the holding and processing of personally identifiable information. This addendum describes our compliance with POPIA when sharing potentially disclosive data in our Remote Access Data Enclave (RADE).

**Background**

Highly disaggregated data is valuable for research to inform government policy. In 2013 DataFirst responded to demands from policy researchers for highly disaggregated data by following the example of data services worldwide and creating a “safe room” at the university for controlled access to this type of data. However, on-site access is neither efficient nor equitable for researchers from non-SA universities. In 2024 DataFirst therefore worked with UCT ICTS to set up a Remote Access Data Enclave to enable controlled online access to data for accredited researchers in the wider academic community. Restricted access data we share in the RADE does not include direct identifiers. However, because it has low-level geographic variables and other sensitive variables, there is a possibility that individuals may be identified in the data. The RADE has therefore been set up to prevent the risks of respondents’ identities being revealed and published. RADE procedures are compliant with POPIA restrictions on the handling of personal data, as explained below.

**Data Retention**

POPIA 2013 restricts the retention period for the holding of information (to only as long as “necessary for achieving the purpose for which the information was collected”) (Condition 3 Clause 14 (1)) (Information Regulator, South Africa, 2013, pp. 31-32). However, the Act makes provision for long-term retention of personal information “for historical, statistical or research purposes” provided the responsible party holding the information puts safeguards in place to ensure the information is used just for these purposes (Condition 3 Clause 14 (2)) (Information Regulator, South Africa, 2013, p. 32). At DataFirst variables with personally identifiable data are removed from the restricted-access versions made available in the RADE.

**Data Processing**

POPIA requires that further processing of personal information must be compatible with the purpose for which the data was collected (POPIA 2013 Condition 4 Clause 15 (1) pp 33-34). However, it waives this requirement when information is used for research purposes and the responsible party ensures that “further processing is carried out solely for such purposes and will not be published in an identifiable form” (Condition 4 Section 15 (3) (e)) (Information Regulator, South Africa, 2013, p. 34). POPIA makes the same exceptions for the prohibition of processing of personal information on children (Part C Clause 35 (1) (d) (ii) and (e)) (Information Regulator, South Africa, 2013, p. 48).

POPIA also requires consent from data subjects to process special personal information[[7]](#footnote-7) about them, but also waives this requirement if the information is processed “for historical, statistical or research purposes”, and “where seeking consent from data subjects would involve disproportionate effort” and where “guarantees have been put in place to ensure information processing does not negatively affect the privacy of data subjects (POPIA 2013 Part B Clause 27 (d) (i) (ii)) (Information Regulator, South Africa, 2013, pp. 42-43).” DataFirst has the same safeguards in place for special personal information as for other personal information,

**The 5 Safes Data Protection Framework at DataFirst**

DataFirst’s applies “[5 safes framework](https://ukdataservice.ac.uk/help/secure-lab/what-is-the-five-safes-framework/#:~:text=The%20Five%20Safes%20framework%20is%20a%20set%20of,them%20and%20other%20data%20providers%20in%20the%202010s.)” developed by the UK Data Service in the RADE for data protection. The framework includes:

**1. Safe data**:

Direct identifiers are removed from the data shared via the RADE

**2. Safe projects**:

Research projects undertaken in the RADE must be approved by data depositors and DataFirst. Researchers must present a project proposal for obtain RADE access. They must also provide reasons why their research cannot be undertaken with the public access versions of the data.

**3. Safe people**:

Researchers are interviewed and must sign a confidentiality agreement with DataFirst to be accredited with “safe” researcher status. Researchers at research and educational institutions are eligible to apply for RADE access and must provide information on themselves and their institution

**4. Safe settings**:

The RADE virtual environment prevents unauthorised access and use. The remote desktop environment requires two levels of authentication and is locked down and monitored by digital supervision software.

**5. Safe outputs**:

all outputs from RADE research are vetted by DataFirst to ensure they are non-disclosive

Further information can be found on our [RADE webpage](https://www.datafirst.uct.ac.za/services/secure-data-services).

1. This option is for data that is potentially disclosive because it has secondary identifiers or detailed geography and must therefore be shared in a safe room. [↑](#footnote-ref-1)
2. In SA, the Protection of Personal Information Act, 2013 makes provision for long-term retention and processing of personal information “for historical, statistical or research purposes” provided the responsible party holding the information puts safeguards in place to ensure the information is anonymised or shared for research purposes only. DataFirst has such safeguards in place. Addendum 1 elaborates on these safeguards. [↑](#footnote-ref-2)
3. Note that DataFirst does not accept metadata or documents for sharing as a substitute for data files. [↑](#footnote-ref-3)
4. The Act defines ‘‘personal information’’ as “information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person (Information Regulator, South Africa, 2013, p. 15).” [↑](#footnote-ref-4)
5. POPIA makes the same exceptions for the prohibition of processing of personal information on children (Part C Clause 35 (1) (d) (ii) and (e)) (Information Regulator, South Africa, 2013, p. 48). [↑](#footnote-ref-5)
6. Special personal information is defined by the Act as information on the someone’s religious/philosophical beliefs, race/ethnic original, trade union membership, political persuasion, health/sex life, and criminal behaviour, as well as biometric information (Information Regulator, South Africa, 2013, p. 42). [↑](#footnote-ref-6)
7. Special personal information is defined by the Act as information on the someone’s religious/philosophical beliefs, race/ethnic original, trade union membership, political persuasion, health/sex life, and criminal behaviour, as well as biometric information (Information Regulator, South Africa, 2013, p. 42). [↑](#footnote-ref-7)