

[IMPORTANT - PLEASE READ]

INSTRUCTIONS

TEMPLATE DATA SHARING AGREEMENT

The template Data Sharing Agreement that follows is intended to promote responsible data practices and sharing between organisations in the nonprofit sector, and, where applicable, their private sector partners. It borrows from corporate best practices and approaches, and is intended as:

1. a transactional roadmap for responsible data sharing in a given context
2. an educational tool for organisations to understand obligations in this area
3. requiring early and deep discussion and due diligence of expectations around approaches, policies and procedures and related roles and responsibilities amongst the parties
4. a starting point for negotiations of an eventual written agreement between the parties. Each provision must be carefully considered and it is not just appropriate but necessary for modifications (both additions and deletions) to be made based on context and the views of the parties. Footnotes should be deleted. Nothing in this template is fixed or pre-determined and it is intended only to assist the parties by providing them with a basis for discussion.

This template agreement contemplates considerable ethical, programmatic, and legal responsibilities, and should only be utilised in close consultation with appropriate country office management, information technology/digital teams, and local and home office legal counsel at each participating organisation/company. This agreement requires discussion and modification, and application to each specific context and party.

In addition to the body of the text, careful attention should be paid to the footnotes. These provide, for example, factors to be considered in reviewing the template and explanations regarding certain provisions. They are intended to assist the reader in analysing the points at issue in the template.

While the parties signing the agreement will generally be sharing personal information that has already been collected, the following page provides a basic template form of consent that organisations may wish to consider adapting for use when collecting personal information. Like the agreement itself, the form of consent is a mere template that should be carefully reviewed and modified to ensure its suitability for the specific context in which it is being used.

Finally, this document has been prepared utilising the generous time and expertise of the law firm Dentons, for which the humanitarian and development sector is grateful.



TEMPLATE FORM OF CONSENT[[1]](#footnote-1)

I, the undersigned, hereby acknowledge and consent to the following:

1. ● (the “Organisation”) will collect the following personal information (my “PI”) from me: ●.[[2]](#footnote-2)
2. The following categories of persons within the Organisation will have access to my PI: ●.[[3]](#footnote-3)
3. The Organisation will use my PI for the following purposes (the “Purposes”): ●.[[4]](#footnote-4)
4. The Organisation may disclose my PI to the following third parties: ●.[[5]](#footnote-5)
5. If I have any questions about the Organisation’s collection, use or disclosure of my PI; if I wish to obtain a copy of my PI in the Organisation’s possession; or to correct, update or delete any such PI, I may contact the following person:[[6]](#footnote-6)

Name and title: ●
Mailing address: ●
Phone number: ●
Email address: ●

1. The Organisation will not retain my PI for longer than is reasonably required to achieve the Purposes and will delete my PI upon request, it being understood that without my PI the Organisation may no longer be able to achieve some or all of the Purposes.

[Consider adding a description of the safeguards that the Organisation uses to protect PI]



THIS DATA SHARING AGREEMENT (this “Agreement”) is made among the undersigned parties (each a “Party”; and, collectively, the “Parties”).[[7]](#footnote-7)

1. The Parties are ●;[[8]](#footnote-8)
2. The Parties are currently operating in ●;[[9]](#footnote-9) (the “Jurisdiction”);
3. The Parties intend to share Personal Information (as defined below), on the terms set forth in this Agreement, in order to advance the program or other purpose described in Schedule A (the “Purpose”);

The Parties hereby agree as follows:

# INTERPRETATION

## Definitions: In this Agreement (which includes its schedules), the following terms shall have the meanings indicated below:

“Business Day” means any calendar day except for Saturday or Sunday[[10]](#footnote-10) or any day when banks are generally closed for business in the Jurisdiction.

“Confidential Information”[[11]](#footnote-11) means this Agreement and all data and information relating to the business and management of any Party (including, without limitation, information pertaining to its programs, initiatives, properties, donors, contributions, grantors, clients, business plans or objectives), data analyses or insights, and any information and data included therein or derived therefrom and the form, format, mode or method of compilation, selection, configuration, presentation or expression thereof, or any other Intellectual Property of such Party; provided, however, that Confidential Information shall not include any data or information which:

### is or becomes publicly available through no fault of a Receiving Party;

### is disclosed to a Receiving Party by a third party under no obligation of confidentiality to the applicable disclosing Party;

### is independently developed by a Receiving Party without reference to the information provided by the applicable disclosing Party;

### is already known or in the possession of a Receiving Party prior to receipt of the information from a disclosing Party; or

### is Personal Information.

“Data Breach” means any unauthorised use, disclosure or other handling of Shared Information.

“Disclosing Party” means a Party in its capacity as a discloser of Shared Information.

“Effective Date” means the date indicated immediately above the signatures to this Agreement.

“Intellectual Property” means any property, tangible or intangible, that may be subject to intellectual property rights of any kind (including without limitation copyrights, trademarks and patents) and includes, without limitation, ideas, formulae, algorithms, concepts, techniques, processes, procedures, approaches, methodologies, plans, systems, research, information, documentation, data, data compilations, specifications, requirements, designs, diagrams, programs, inventions, technologies, software, tools, products knowledge, know-how, including without limitation, trade secrets, and other materials or things.

“Intellectual Property Rights” means: (a) any and all proprietary rights anywhere in the world provided under (i) patent law; (ii) copyright law, including moral rights; (iii) trademark law; (iv) design patent or industrial design law; (v) trade secret law; or (vi) any other statutory provision or common law principle applicable to the Parties and their assets that may provide a right in either Intellectual Property or its expression or use; and (b) any and all applications, registrations, licenses, sub-licenses, franchises, agreements or any other evidence of a right in any of the foregoing.

“Person” means any individual, sole proprietorship, partnership, unincorporated association, unincorporated syndicate, unincorporated organisation, firm, limited liability company, corporation, body corporate, trustee, trust, governmental authority or other entity or organisation.

“Personal Information” means any information relating to an identifiable individual.[[12]](#footnote-12)

“Receiving Party” means a Party in its capacity as the recipient of Shared Information.

“Shared Information” means the Personal Information in a Party’s possession described in Schedule B, regarding the categories of individuals described in Schedule C.

## Headings: The division of this Agreement into Sections and the insertion of headings are for convenience of reference only and shall not affect the construction or interpretation of this Agreement. The terms “this Agreement”, “hereof”, “hereunder” and similar expressions refer to this Agreement and not to any particular Section or other portion hereof and include any agreement supplemental hereto.

## Severability: If any provision (or any portion of a provision) of this Agreement shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable for any reason, such invalidity, illegality or unenforceability shall not affect any other provision hereof and this Agreement shall be construed as if such invalid, illegal or unenforceable provision (or portion of a provision) had never been contained herein in regards to that particular jurisdiction.

## Singular and Plural: As the context may require, the singular may be read as the plural and vice-versa.

# DATA SHARING

## Sharing: Each Party hereby grants to each other Party a right of use and access to its Shared Information (including any necessary Intellectual Property Rights), exclusively for the Purpose. Each Party shall provide each other Party with access[[13]](#footnote-13) to that Shared Information and do all things necessary to give effect to such access, including data transfers or granting access to computer systems. No Receiving Party shall use any Shared Information provided to it by a Disclosing Party for any purpose other than the Purpose and shall disclose Shared Information only to those Persons outside that Receiving Party’s organisation identified at Schedule D. The Receiving Party shall be responsible for ensuring that any disclosure it makes of Shared Information complies with applicable law.[[14]](#footnote-14)

## De-personalisation: Except to the extent incompatible with the Purpose, each Disclosing Party shall de-personalise and anonymise all Personal Information before sharing it hereunder such that it can no longer be related to an identifiable individual and therefore no longer constitutes Personal Information.[[15]](#footnote-15)

## Access: Each Receiving Party shall take proactive measures to ensure that access to the Shared Information shared with it by a Disclosing Party is strictly limited to Persons who are required to have such access for the Purpose, and that such authorised Persons do not access, use or disclose the Shared Information for any purpose other than the Purpose.

## Retention: Except as may be strictly required under applicable law,[[16]](#footnote-16) each Receiving Party shall retain Shared Information only for so long as it is necessary or useful to give effect to the Purpose or otherwise required under applicable law or contractual requirements, at which time such Shared Information shall be destroyed in accordance with Section 4(e).

# DATA PROTECTION AND AUDIT RIGHTS

## Security: Each Receiving Party shall implement and maintain all physical, organisational and technological security measures and safeguards that are necessary or appropriate to prevent unauthorised access, disclosure, destruction, loss or alteration of any Shared Information, including without limitation those set forth in Schedule E. Each Receiving Party shall take all reasonable measures to ensure that each access to Shared Information is recorded, including for the purpose of giving maximum practicable effect to the audit rights set forth at Section 3(f).[[17]](#footnote-17)

## High-Risk Personal Information: The Parties acknowledge that certain Personal Information may be particularly sensitive for political, economic or other reasons[[18]](#footnote-18) (such Personal Information, “High-Risk Personal Information”), as identified in Schedule B. With respect to any High-Risk Personal Information to be shared hereunder, each Disclosing Party represents and warrants to each Receiving Party with which it discloses Shared Information that is High-Risk Personal Information, in respect only of that Shared Information, that its collection of Personal Information was strictly necessary to achieve the purposes for which it was collected and was done in accordance with applicable law, and each Receiving Party acknowledges to each such Disclosing Party, in respect only of the Shared Information that is High-Risk Personal Information, that it is absolutely critical that such High-Risk Personal Information be kept confidential and handled with the utmost care and protection and not be the subject of a Data Breach, as such an event could threaten the health or safety of both the individuals concerned and third parties. In addition to complying with its obligations hereunder, each Party shall handle High-Risk Personal Information in accordance with its privacy, network, data security and other policies applicable thereto. This section 3(b) shall be in no way construed as limiting a Party’s obligations with respect to Shared Information that is not High-Risk Personal Information.[[19]](#footnote-19)

## Compliance: Each Party shall, in connection with this Agreement, comply with all applicable laws, rules, and regulations, including, without limitation, those governing Personal Information.[[20]](#footnote-20) [In addition, the Parties shall adhere to ●.][[21]](#footnote-21) Without limiting the generality of the foregoing, by sharing Shared Information each Disclosing Party represents and warrants to each Receiving Party to whom it discloses Shared Information, in respect only of such Shared Information, that the Disclosing Party has implemented all legally required safeguards, received all consents,[[22]](#footnote-22) licenses, permits, or other authorisations necessary or appropriate to enable it to lawfully collect, use and share such Shared Information, as well as to enable each Receiving Party to use and access it as contemplated under Section 2(a). A Receiving Party shall not combine the Shared Information with any other information or data except as contemplated under this Agreement. For greater clarity, a Receiving Party may use Shared Information to create Arising IP (as defined at section 7(b)).

## Generated Personal Information: In the case of Shared Information that a Disclosing Party has generated itself, that Disclosing Party further represents and warrants to each Receiving Party to whom it discloses such generated Shared Information, in respect only of the Shared Information that it has generated itself, that it has complied with any legal requirements applicable to such Personal Information (including any legal requirement to notify the individuals concerned of the existence of such generated Personal Information). A Receiving Party shall not generate such new Personal Information without complying with any applicable legal requirements.[[23]](#footnote-23)

## Data Breach: Each Receiving Party shall promptly notify other Parties in accordance with section 8(e) of any Data Breach. Such notice shall be given within one[[24]](#footnote-24) Business Day of the Receiving Party becoming aware of the Data Breach, except in the case of High-Risk Personal Information in which case notification shall be immediate. In the event of a Data Breach, each Receiving Party shall take all measures that are reasonably required to prevent any recurrence thereof and otherwise cooperate fully with each Disclosing Party from whom it has received Shared Information as necessary to protect each such Disclosing Party to the extent that it is affected by the Data Breach. Each Receiving Party shall contain and make all reasonable efforts to remedy or reduce the impact of a Data Breach and take all steps as may be reasonably requested by each Disclosing Party from whom it has received Shared Information, including but not limited to any steps required under applicable law or required to enable each such Disclosing Party to comply with such law. Each Receiving Party shall strictly comply with each such Disclosing Party’s instructions in responding to a Data Breach, except to the extent that (a) a Receiving Party’s legal counsel has advised it in writing that those instructions are contrary to applicable law (and in which case the Receiving Party shall provide each Disclosing Party with a copy of such advice) or (b) such instructions are contradictory, in which case the Receiving Party shall comply with the instructions that it determines in good faith are most appropriate under the circumstances and promptly advise each such Disclosing Party of that determination; in making any such determination, the Receiving Party shall place the highest priority on the protection of the rights of the individuals whose Personal Information was the object of the Data Breach.

## Audit: Each Disclosing Party shall have the right to make visits, on 10 Business Days’ notice and during business hours (except in case of emergency, in which case such visits may occur unannounced and at any time), to the premises and sites of any Receiving Party that has received Shared Information from it, for purposes of inspection (including of all computer equipment) and to review the security arrangements that such Receiving Party is maintaining with respect to Shared Information. Each Receiving Party shall fully and promptly cooperate with, and assist, each Disclosing Party from whom it has received Shared Information in completing those inspections. Each Disclosing Party may exercise its audit right either directly or through a third party whose services it has retained for that purpose.[[25]](#footnote-25)

## Contact Person: Each Party shall appoint and identify to each other Party an individual (the “Contact Person”) who shall be responsible for overseeing and ensuring that Party’s compliance with this Agreement. The Contact Person’s position and authority shall be sufficient to enable them to properly carry on such oversight and provide such assurance. The Contact Person of a Party shall, upon request by another Party, provide a signed certificate attesting on behalf of that Contact Person’s Party that it is in full compliance with its obligations hereunder.[[26]](#footnote-26)

## Access Rights: A Receiving Party shall notify the Disclosing Party upon receipt of any request from an individual for access to, or rectification of, that individual’s Shared Information received from the Disclosing Party. The Receiving Party shall comply with all of its legal obligations under applicable law governing such a request and shall keep the Disclosing Party informed in that regard. Any rectification of Shared Information by a Receiving Party shall be effected in conjunction with the Disclosing Party such that the Personal Information is rectified by both such Parties.

# TERM AND TERMINATION[[27]](#footnote-27)

## Initial Term: The term of this Agreement shall commence on the Effective Date and shall continue for a period of 30 days (the “Initial Term”), unless terminated earlier in accordance with the provisions of this Agreement.

## Renewal Term: This Agreement shall automatically renew for successive renewal terms of 30 days each (each, a “Renewal Term”), unless a Party notifies each other Parties at least 15 days prior to the expiration of the Initial Term or the then Renewal Term, as the case may be, of that Party’s desire not to renew this Agreement (the Initial Term and any Renewal Terms collectively referred to as the “Term”).

## Termination for Breach: Subject to Sections 4(e) and 4(f), a Party may terminate this Agreement, without prejudice to enforcement of any other legal right or remedy, immediately upon giving written notice of such termination if another Party is in material breach of any provision of this Agreement (including the occurrence of a Data Breach) and such breach continues for a period of 10 days after delivery of a written notice by any non-breaching Party requiring such breaching Party to correct such failure. The aforementioned 10-day cure period shall not apply to a breach hereof that, in the terminating Party’s reasonable opinion, may jeopardise the health, safety or well-being of the individual(s) whose Personal Information is in the breaching Party’s possession.

## Waiver: A Party’s waiver of a breach or default of any provision of this Agreement by another Party shall not be effective unless in writing and shall not be construed as a waiver of any succeeding breach of the same or of any other provision. Nor shall any delay or omission on the part of any Party to exercise or avail itself of any right, power or privilege by such Party shall constitute a waiver.

## Effect of Termination:

### In the event of a termination for breach under Section 4(c) of this Agreement, such termination shall only have effect with respect to the breaching Party, and this Agreement shall, subject to Section 4(f) below, thereby cease to have effect in respect of that breaching Party but shall survive and remain in force among the non-breaching Parties.

### In all other cases of termination, this Agreement shall, subject to Section 4(f) of this Agreement, cease to have effect in respect of a terminating Party but shall survive and remain in force with respect to the non-terminating Parties.

### Upon the termination of this Agreement for any reason, each Receiving Party shall immediately destroy all Shared Information that was disclosed to it by a Disclosing Party, includes all copies thereof and any Shared Information contained in Arising IP (as defined at Section 7(b)), as well as all Confidential Information of each other Party, and provide each other Party with a certificate to that effect signed by the Contact Person or another individual acceptable to that Party.

## Survival of Covenants: Notwithstanding the termination or expiration of this Agreement for any reason with respect to any Party, the covenants set out in Sections 3, 4, 5, 6, 7 and 8 of this Agreement shall survive any such termination or expiration.

# CONFIDENTIALITY

## Obligation: Each Party acknowledges that the Confidential Information of any and all other Parties is confidential and proprietary information of each such other Party, respectively, as the case may be. Each Party shall hold, and shall cause its employees, agents and contractors to hold, Confidential Information of each other Parties in confidence and shall use the same degree of care, by instruction, agreement or otherwise, to maintain the confidentiality of each other Party’s Confidential Information that it uses to maintain the confidentiality of its own Confidential Information, but with at least a reasonable degree of care commensurate with the nature and importance of such Confidential Information. No Party shall make use of another’s Confidential Information other than to advance the Purpose, nor shall it release, disclose, communicate it or make it available to any third party other than its employees, agents and contractors who reasonably need to know it in connection with the exercise of rights or the performance of obligations under this Agreement.

## Subpoena: Section 8(c) shall apply, with the necessary modifications, to any request that a Party may receive to disclose all or any part of another Party’s Confidential Information under the terms of a valid and effective subpoena or order issued by a court of competent jurisdiction or by a governmental or regulatory body.

# INDEMNIFICATION

## (a) Each Party (each [and collectively], an “Indemnitor”) shall [jointly and severally][[28]](#footnote-28) fully indemnify each other Party and its affiliates, present and former directors, officers, employees, partners, advisors, agents, shareholders or members (collectively, the “Indemnified Parties”) against all expenses, losses (other than loss of profits), costs, damages, and reasonable fees and expenses of counsel (collectively, “Losses”) incurred or certain to be incurred that are related directly or indirectly to (i) the Indemnitor’s breach of or default under any representation, warranty or covenant in this Agreement or (ii) any order made or any inquiry, investigation or proceeding instituted, threatened or announced by any court, privacy regulatory authority or any other governmental authority, based upon such Indemnitor’s handling of Personal Information.

## This indemnity shall not apply to an Indemnified Party to the extent that a court of competent jurisdiction in a final judgment that has become non-appealable determines that (i) the Indemnified Party has been [grossly][[29]](#footnote-29) negligent, committed any fraudulent act or found to have acted with willful misconduct in the course of such performance and (ii) the Losses as to which indemnification is claimed, were directly caused by that negligence, fraud or willful misconduct.

## The Indemnitor may, at its own expense, participate in or assume the defense of any legal proceeding brought against the Indemnitor or an Indemnified Party (or in which an Indemnified Party is required to testify or otherwise participate) relating to this Agreement. Any such defense shall be through legal counsel reasonably acceptable to the Indemnified Party. In addition, any Indemnified Parties may employ separate counsel in any such proceeding and participate in the defense thereof. The Indemnified Parties shall assume the fees of such counsel unless:

### the Indemnified Parties have been advised by a written opinion of counsel that representation of both parties by the same counsel would be inappropriate due to actual or potential differing interests; or

### the Indemnitor has failed, within a reasonable period of time after receipt of notice, to assume the defense of such proceeding.

## The Indemnitor shall not be required to assume the fees and expenses of more than one additional counsel per jurisdiction on behalf of all Indemnified Parties. The Indemnitor shall pay related reasonable costs and out-of-pocket expenses incurred by the Indemnified Parties’ personnel as they occur. Neither an Indemnitor nor an Indemnified Party shall effect any settlement of any such action or claim or make any admission of liability without the written consent of the other, such consent to be properly considered and not to be unreasonably withheld.

## An Indemnified Party shall promptly notify the Indemnitor after it learns of any legal proceeding against that Indemnified Party or of any investigation that is based, directly or indirectly, upon any matter in respect of which indemnification may be sought from the Indemnitor. Any failure or delay in so notifying shall relieve the Indemnitor of liability only to the extent that the delay or failure materially prejudices the defense of such proceeding or results in any material increase in the liability which the Indemnitor has hereunder. The Indemnified Party shall provide copies of all relevant documentation to the Indemnitor on an ongoing basis and keep each Indemnitor advised of all discussions and proposed significant actions.

## The Indemnitor hereby waives any right that it may have to require an Indemnified Party to proceed against or enforce any other right, remedy or security or claim from any other person prior to claiming under this indemnity.

## The indemnity obligations of the Indemnitor shall be in addition to any liability which the Indemnitor may otherwise have.

## Neither an Indemnitor nor any Indemnified Party shall make any admission of liability or settle any action, suit, proceeding, claim or investigation without the other’s consent, such consent not to be unreasonably withheld, except that each Indemnitor’s consent shall not be required for any admission or settlement that will not result in the payment of any indemnification under this Agreement.

# INTELLECTUAL PROPERTY

## The Parties acknowledge that each owns all worldwide right, title and interest, including all Intellectual Property Rights, in and to its respective Intellectual Property and Shared Information. Except for the express rights and licenses granted herein (including without limitation those granted in Section 2(a)), this Agreement does not grant any Party any rights, title or ownership interests of any kind whatsoever, express or implied, in another’s Intellectual Property or Shared Information.

## If a Receiving Party (the “Developer”) develops or acquires any new Intellectual Property (“Arising IP”) from a Disclosing Party’s Shared Information shared hereunder, then that Developer’s Arising IP shall be the sole and exclusive property of the Developer and the Developer shall grant to each other Party[[30]](#footnote-30) (each a “Licensee”), an irrevocable, assignable, transferable, sub-licensable, non-exclusive, worldwide, royalty-free and fully paid-up right and license to use and access the Developer’s Arising IP for any purpose whatsoever (the “License”).

## [A Receiving Party shall develop Arising IP only in order to further the Purpose. Arising IP shall be used by the Developer only in connection with the Purpose. Arising IP shall only be licensed by the Developer to the Licensees for use in connection with the Purpose.][[31]](#footnote-31)

## A Receiving Party that develops Arising IP shall ensure that such development is done in a manner compatible with its obligations under Section 4(e)(iii) to destroy all Shared Information upon termination of this Agreement.

## A Developer shall not challenge a Party’s ownership in its Intellectual Property and Shared Information, nor shall it challenge the validity of any such Intellectual Property or Personal Information ownership or do or cause to be done anything that would contest or impair any right, title, or interest of a Party in and to any such Intellectual Property or Personal Information. A Licensee shall not challenge the Developer’s ownership in that Developer’s Arising IP, nor shall it challenge the validity of any Developer’s Arising IP ownership or do or cause to be done anything that would contest or impair any right, title, or interest of the Developer in and to the Developer’s Arising IP.

## Each Party agrees that any use of Shared Information for the development or acquisition of Arising IP is at its own risk and expense. Each Licensee agrees that its use of the Developer’s Arising IP under the License is at its own risk and expense and that the License is granted on an “as-is, where-is” basis, without any warranty or condition, express or implied, statutory or otherwise, including without limitation any implied warranty of accuracy, merchantability or fitness for a particular purpose.

## Arising IP that constitutes or includes Personal Information shall be subject to the terms and conditions set forth in this Agreement.

# MISCELLANEOUS

## Minimum Standards: Without prejudice to any obligation it may have under this Agreement, in storing, securing and otherwise handling Shared Information, a Receiving Party shall maintain a standard of care that is no less than the standard it normally exercises to handle Personal Information in its possession

## Injunctive Relief: Each Party acknowledges that any breach will cause irreparable damage to the other Parties, that monetary damages would be an inadequate remedy and that the amount of such damages would be extremely difficult to measure. A Party may seek an injunction to restrain any and all other Parties from any such breach and pursue all remedies available to it for a breach or threatened breach of another Party’s obligations under this Agreement.

## Subpoena: If a Party receives a request to disclose all or any part of any Shared Information under the terms of a valid and effective subpoena or order issued by a court of competent jurisdiction or by a governmental or regulatory body, that Party shall: (i) immediately notify that other Party of the existence, terms and circumstances surrounding such a request; (ii) consult with such other Party on the advisability of taking legally available steps to resist or narrow such request; and (iii) if disclosure of such Shared Information is required, exercise its commercially reasonable efforts to obtain an order or other reliable assurance that confidential treatment will be accorded to such portion of the disclosed Shared Information which that other Party so designates.

## Accuracy: Each Disclosing Party represents and warrants to each Receiving Party to which it discloses Shared Information, in respect only of that Disclosing Party’s Shared Information, that it has used reasonable efforts to confirm the completeness and accuracy of all such Shared Information and to keep that Shared Information up-to-date, such that the Shared Information is sufficiently complete, accurate and current to give effect to the Purpose.[[32]](#footnote-32)

## Notices: All notices or other communications hereunder shall be deemed to have been duly given and made if in writing and if served by personal delivery upon the Party for whom it is intended, if delivered by registered or certified mail, return receipt requested, or by a national courier service, or if sent by email (receipt of which is confirmed), to the Party at the address set forth below the signatures below, or such other address as may be designated in writing hereafter, in the same manner, by such Party. Any such notification shall be addressed to the Contact Person and shall be deemed delivered: (a) upon receipt, if delivered personally or by email, (b) on the next Business Day, if sent by national courier service for next Business Day delivery.

## Entire Agreement: This Agreement, together with any agreements and other documents to be delivered pursuant hereto or thereto, constitutes the entire agreement between the Parties pertaining to the subject matter hereof and supersedes all prior agreements, negotiations, discussions and understandings, written or oral, between the Parties. Except as expressly provided in this Agreement, there are no representations, warranties, conditions other agreements or acknowledgements, whether direct or collateral, express or implied, that form part of or affect this Agreement. The execution of this Agreement has not been induced by, nor does any Party rely upon or regard as material, any representations, warranties, conditions, other agreements or acknowledgements not expressly made in this Agreement.

## Governing Law: This Agreement shall be governed by, and construed and enforced in accordance with, the laws of ●[[33]](#footnote-33) (excluding any conflict of laws rule or principle which might refer such construction to the laws of another jurisdiction).

## Modification: This Agreement may be modified only upon written agreement by the Parties.

## Assignment: Neither this Agreement nor any of the rights or obligations hereunder may be assigned by any Party without the prior written consent of each other Party.

## No Partnership: Nothing herein shall be deemed to constitute any Party as an agent, representative or employee of another Party, or a plurality of Parties as joint venturers or partners for any purpose. Each Party shall act solely as an independent contractor and shall not be responsible for the acts or omissions of any other Party. No Party will have the authority or right to represent or obligate any other Party in any way.

This Agreement is entered into as of , 20 .

NAME OF PARTY 1:[[34]](#footnote-34) NAME OF PARTY 2:

Signature: Signature:

Name: Name:

Title: Title:

Address: Address:

Email of Contact Person: Email of Contact Person:

NAME OF PARTY 3: NAME OF PARTY 4:

Signature: Signature:

Name: Name:

Title: Title:

Address: Address:

Email of Contact Person: Email of Contact Person:

NAME OF PARTY 5: NAME OF PARTY 6:

Signature: Signature:

Name: Name:

Title: Title:

Address: Address:

Email of Contact Person: Email of Contact Person:

SCHEDULE A

Purpose

●[[35]](#footnote-35)

SCHEDULE B

Personal Information

●[[36]](#footnote-36)

SCHEDULE C

Categories of Individuals[[37]](#footnote-37)

●

SCHEDULE D

Permitted Disclosure[[38]](#footnote-38)

|  |  |
| --- | --- |
| Organisation Name or Category of Persons | Location |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

SCHEDULE E

Safeguards[[39]](#footnote-39)

1. Locked file cabinets
2. Restricted access areas
3. Background checks for staff with access to Personal Information
4. Strong password requirements for computer access
5. Data encryption
1. It is essential to ensure that the individuals disclosing PI understand the substance of this consent. [↑](#footnote-ref-1)
2. List, as exhaustively as possible, all PI that will be collected from the individual. A catch-all provision (such as “all PI reasonably useful to the Organisation”) is insufficient. Indicate, for example, “Name, Date of Birth, Address.” [↑](#footnote-ref-2)
3. In preparing this list, consider the obligation set forth at section 2(c) of the Agreement. [↑](#footnote-ref-3)
4. This list must also be exhaustive. For example, “To evaluate your medical needs and offer the care and services required to address them.” [↑](#footnote-ref-4)
5. This list must also be exhaustive. See footnote 36 for additional guidance. [↑](#footnote-ref-5)
6. Applicable law may require that a contact person be identified for various purposes, including those set forth above. [↑](#footnote-ref-6)
7. This Agreement governs the sharing of Personal Information (see footnote 6 for more details on what constitutes Personal Information). It can be used irrespective of the number of Parties, whether they are for-profit or non-profit, where they are based or operating, the nature of their activities, whether disclosure is unilateral or multilateral, and whether disclosure is one-time or ongoing. It is a template that needs to be adapted for each situation, in light of the circumstances of the data sharing arrangement and the Parties. It should be used only after consulting appropriate members of management and legal counsel. [↑](#footnote-ref-7)
8. This text should describe the activities of the Parties as specifically as possible (for example, “non-profit organisations that provide relief and assistance to persons in need,” “non-profit organisations that provide emergency food relief to refugees displaced by war” or “a non-profit organisation providing medical services in developing countries and a telecommunications service provider operating in the Middle East.”). [↑](#footnote-ref-8)
9. This should refer both to the country and any sub-national jurisdiction (state, province, governorate, etc.). [↑](#footnote-ref-9)
10. Modify to reflect the weekend in the Jurisdiction if it is observed on different days (often the case in Muslim countries). [↑](#footnote-ref-10)
11. If the Parties have already entered into a non-disclosure agreement that governs the handling of Confidential Information, delete this definition, the reference to Confidential Information at subparagraph 4(e)(iii), and article 5. [↑](#footnote-ref-11)
12. Depending on the jurisdiction and the applicable law (see footnote 28), Personal Information may include names, signatures, addresses, telephone numbers, email addresses, personal identification numbers, government-issued identification numbers, financial account numbers, biometric or health data and other personal or unique identifiers. Information that cannot be related to an identifiable individual does not constitute Personal Information. This includes Personal Information that has been stripped of identifying details such that it has become impossible to determine to whom it relates (bearing in mind that, for example, simply removing the name from a file would be insufficient if other details in the file such as age, address, date of birth, etc. enable the reader to identify the individual). Information that is not Personal Information may be Confidential Information (for example, statistical data, business methods, etc.), in which case it would not be governed by the provisions relating to Personal Information but would remain subject to those relating to Confidential Information. Information that is neither Personal nor Confidential Information (for example, the list of countries where a business operates available on its website) would not be governed by this Agreement at all. [↑](#footnote-ref-12)
13. Access can take any number of forms, including physical consultation of paper documents, electronic transfer, creation of a shared database, algorithmic querying, etc. If necessary, the specific form of access contemplated here can be set forth at Schedule A. [↑](#footnote-ref-13)
14. Applicable law (see footnote 28) may impose additional restrictions on cross-border transfers (including both international and domestic borders, such as from one province or state to another). Such restrictions may for example include a requirement to ensure that the Personal Information continues to benefit from the same level of protection against disclosure without consent that it had in the originating jurisdiction. This can be a particular issue when disclosing or transferring data to the United States. Imposing contractual restrictions against unauthorised disclosure may help mitigate this risk. [↑](#footnote-ref-14)
15. De-personalisation must be done with care in order to ensure that the information can no longer be related to an identifiable individual and therefore no longer constitutes Personal Information. See footnote 6 in this regard. The Parties should de-personalise information by default unless doing so would comprise the Purpose. [↑](#footnote-ref-15)
16. See footnote 28 for more details regarding the concept of applicable law. [↑](#footnote-ref-16)
17. Section 3(f) allows each Party to audit the others’ compliance with this Agreement. In order to facilitate such an audit, it is important that each Party keep track of who has accessed the Personal Information shared with it under this Agreement. [↑](#footnote-ref-17)
18. Applicable law may have special restrictions governing highly-sensitive personal information (for example, such information cannot be collected, used or disclosed without the individual’s explicit consent). [↑](#footnote-ref-18)
19. This section addresses information such as political, ethnic or tribal affiliation or sexual orientation that can be especially sensitive in certain contexts. It is especially critical that such High-Risk Personal Information be safeguarded. [↑](#footnote-ref-19)
20. This obligation serves as a catch-all that would put a Party in default for breach of any applicable law, thereby giving each other Party an “out” if the breach is material. [↑](#footnote-ref-20)
21. Consider whether in addition to what may be required by law it is appropriate to require compliance with a privacy standard, for example the [United Nations Development Group guidance](https://undg.org/wp-content/uploads/2017/11/UNDG_BigData_final_web.pdf). Such an approach may, for example, be required by an organisation’s donors. More than one such standard can be referred to, so long as it is possible to comply with all of them at once. Such standards can set forth obligations with respect to obtaining consent from individuals, security protocols, data breach procedures, etc. If one of the Parties is much more sophisticated than the other(s), for example because it is a technology company and the others are non-governmental organisations, consider requiring only that Party to comply with the additional standard. If no such additional standard is desired, delete the highlighted text. [↑](#footnote-ref-21)
22. While the standard for consent will vary depending on the applicable law (see footnote 28),it will generally be a function of the sensitivity of the information and the extent to which an individual would expect the information to be used for a given purpose (implied consent can be sufficient if for example the information is non-sensitive and the use being made is one that is obvious to the individual at the time of collection. Conversely, explicit consent is more likely to be required if the use would come as a surprise to the individual. Those factors can also affect the form and substance required for explicit consent. Note that applicable law may allow Personal Information to be collected, used or shared without consent in certain situations. A Party that properly relies on such an exception is in compliance with this obligation. Note also that donor consent may be required as a condition of an organisation’s grants or contracts. [↑](#footnote-ref-22)
23. This section applies to Personal Information that an organisation might generate about individuals; for example, using their demographic and other information to assign them a “risk score” for disease or other dangers. There may be legal requirements specifically applicable to such Personal Information. [↑](#footnote-ref-23)
24. If this time period is unrealistic, it can be increased but should be as brief as possible under the circumstances. The sooner a Data Breach is notified, the sooner the Disclosing Party can work to contain it. If the notice period is too long, by the time the Disclosing Party is aware of the Data Breach it will be too late to do anything about it. [↑](#footnote-ref-24)
25. Consider scheduling regular audits at monthly or annual intervals. No change to this document would be required; a Disclosing Party merely needs to inform a Receiving Party of its intention to do so. [↑](#footnote-ref-25)
26. In order to give effect to this provision, a Party’s Contact Person needs to be in a position to monitor its compliance with this Agreement and to sign on its behalf that the Party is complying with its terms. The Contact Person therefore needs, among other things, to be a senior representative of the Party and also to be familiar with this Agreement and applicable law. [↑](#footnote-ref-26)
27. The Term is structured as a 30-day period with unlimited 30-day renewals because in certain jurisdictions contracts with an indefinite term are invalid. [↑](#footnote-ref-27)
28. If Parties are “jointly and severally” liable, each Party is responsible for the obligations of all the other Parties (this is the common-law equivalent of solidary liability in civil law jurisdictions). For example, if three Parties are each liable for $100,000 in damages, then each Party is liable for the full amount of $300,000 (although a Party forced to pay the full amount could take recourse against the others for their share of the amount). Whether a Party wants the language regarding joint and several liability to remain may be a function of whether it judges that it will be more likely to pay damages or to receive them. If no joint and several liability is desired then the words “and collectively” should also be deleted. [↑](#footnote-ref-28)
29. The inclusion of the word “grossly” would allow a Party to be indemnified even if it had committed simple negligence. What constitutes gross vs. simple negligence will be a function of the governing law of the contract. [↑](#footnote-ref-29)
30. Under this provision, the Developer of Arising IP grants each other Party a License on that Arising IP. Consider specifying instead that the license is granted only to “each Party that contributed the Shared Information on which the on which the Developer’s Arising IP was based” if appropriate under the circumstances. Note such a license is practicable only if it will be clear which Party’s Shared Information was used to develop Arising IP. If, for example, there is Personal Information is owned or possessed and shared by more than one Party then such a mechanism could be unworkable. [↑](#footnote-ref-30)
31. Consider whether these restrictions are appropriate. The Parties may not want their Shared Information to be used to develop Arising IP that is unrelated to the Purpose, but such a restriction would prevent Arising IP from being used in connection with other projects. Whether Arising IP is licensed to all Parties or only to those whose Shared Information was used to develop it may be a relevant consideration; in the latter case, fewer restrictions may be warranted. [↑](#footnote-ref-31)
32. Acting on the basis of inaccurate or incomplete information could give rise to liability. If this obligation is considered particularly burdensome, instead of stating that the Disclosing Party has taken “reasonable efforts” consider identifying the specific steps that it has taken to ensure accurate information. At a minimum, for example, the Disclosing Party has presumably rejected information that on its face is incorrect (*e.g.*, in the case of individuals giving information in person, a date of birth given by a young adult that would make him 60 years old). [↑](#footnote-ref-32)
33. Consider which governing law is most appropriate for this Agreement on a case-by-case basis. For example, if all Parties have their head office in the same country then that country’s laws may be preferable. As a general matter, it is best not to choose a jurisdiction in the European Union to avoid or reduce the likelihood that the *General Data Protection Regulation* will apply. If in doubt, consider selecting a jurisdiction such as New York whose laws are generally familiar in the legal community. Note that regardless of the choice of governing law, it will remain necessary to comply with local law when handling Shared Information. It is important to distinguish between the law that governs this Agreement (the law that applies if the Parties have a dispute under this Agreement), which the Parties can choose freely, and the law that governs the handling of Shared Information. The Parties are not free to choose which law governs Shared Information; instead, it is determined by a range of factors such as where the individuals are located, where the Parties are based and where the Shared Information will be stored. It is important to consult legal counsel to determine with which laws the Parties need to comply in their handling of Shared Information. [↑](#footnote-ref-33)
34. Add or delete signature blocks as necessary for the actual number of signatories. [↑](#footnote-ref-34)
35. This description must be sufficiently detailed and complete so as to avoid any ambiguity as to what the data sharing relates to and the purposes for which data may be used. Consider stating “See attached document” and joining a brochure or other document describing the program in full. If the program is modified to any meaningful extent after this Agreement is signed, or if the Purpose otherwise changes, this schedule must be amended (and an amendment should be made if there is doubt as to whether it is required). If the data sharing is taking place outside the context of a specific program, describe the specific purpose for which data will be shared. [↑](#footnote-ref-35)
36. This schedule must provide an exhaustive list of all personal information to be shared between the Parties (for example, name, address, sex, phone number, ethnicity, profession, etc.). If new Personal Information is to be shared after this Agreement is signed, this schedule must be amended. All High-Risk Personal Information (see Section 3(b)) should be explicitly identified as such. [↑](#footnote-ref-36)
37. This schedule must identify the categories of individuals whose Personal Information will be shared under this Agreement. For example, it could refer to all individuals receiving aid under the program described at Schedule A, or all individuals resident in a certain location, or who suffer from a specific condition or circumstance. Since the Parties presumably do not want to share all Personal Information in their possession (since some of it is likely irrelevant to the Purpose), this description is important since it will define whose Personal Information is to be shared. To the extent possible, categories of access should be defined (for example, who can modify or add to the information versus who can only access it, or who has full access to all information versus who can view only a portion of it). Consider creating and assigning categories of users such as “owner” (full access), “reader” (read-only access), etc. [↑](#footnote-ref-37)
38. The column “Organisation Name or Category of Persons” must specify to whom a Receiving Party may disclose Personal Information. It is preferable to list specific individuals or departments within an organisation, rather than categories of people or organisations as a whole. It is vital for the Disclosing Party to ensure that it has all necessary consents and authorisations to allow the Receiving Party to disclose Personal Information to these people or categories of people. The column “Location” must specify where the organisation or category of people are physically located, as this can affect what law applies to the disclosure of Personal Information to them. In completing this schedule, consider whether applicable law deems the transfer of Personal Information to a data processor (where Personal Information remains under the control of the transferor and not for some new use by the transferee) to be a use or a disclosure. [↑](#footnote-ref-38)
39. This schedule should list the physical and technological safeguards that each Party wishes the other Parties to use in protecting Personal Information. The list provided above includes examples and should be adapted as circumstances warrant. [↑](#footnote-ref-39)