Data Sharing Agreement

*Controller to controller*

|  |  |
| --- | --- |
| Document Title | Data Sharing Agreement – controller to controller |
| Version | 1.0 |
| Approved by | [insert] |
| Approval date | [insert] |
| Document supersedes | [insert] |
| Review date | [insert] |

Revision history

|  |  |  |
| --- | --- | --- |
| Version no | Revision date | Nature of revision |
| 1.0 | [insert] | [insert] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Data Sharing Agreement**

This agreement is made on [Date]

1. **Parties to this agreement**

**The First Controller**

COMPANY NAME (“a party”) with registered offices at XXX

**The Second Controller**

COMPANY NAME ("a party" or “second controller”) with registered offices at XXX

1. **Background**

The following document reflects the arrangements that have been agreed and are detailed in the terms and conditions of business and the contractual agreement. The following document forms part of this agreement and has been put in place to facilitate the sharing of personal information between the parties.

This agreement allows for data to be shared between the parties and to be processed by the parties for the stated purposes and in accordance with the obligations set out in this agreement. The agreement sets out the framework for the sharing of personal data between the parties as data controllers and defines the principles and procedures that the parties shall adhere to and the responsibilities of the parties to each other. This agreement may be amended from time to time upon written agreement between the parties when deemed necessary.

Under this Agreement, both Parties acknowledge and agree that they will each process personal data independently as separate controllers.

1. **Definitions**

In this Agreement:

* "Agreement" means this agreement between the parties.
* "Data subjects’ information" means the personal data of an adult or child shared between the parties in connection with this Agreement.
* "Data Protection Law" means any laws and regulations relating to the use or processing of personal data in the UK including: (i) The UK General Data Protection Regulation ("UK GDPR"); (ii) the Data Protection Act 2018 ("DPA") and (iii) the Privacy and Electronic Communications (EC Directive Regulations 2003); and all other applicable laws and regulations relating to the processing of personal data and/or Special categories of Personal data and/or governing individuals rights to data privacy, including statutory instruments; in each case, as updated, amended or replaced from time to time; "DP Regulator" means any governmental or regulatory body or authority with responsibility for monitoring or enforcing compliance with the Data Protection Laws including the Information Commissioner’s Office (ICO);
* "Enquiry" means any request, complaint, investigation, notice or communication from a Data Subject or a DP Regulator.
* "Party" or "Parties" means either (or both) First Controller and Second Controller.
* "Personal Data Breach" shall have the meaning set out in Article 4 of the UK GDPR;
* “Purpose” refers to the purposes for processing data, as set out in Annex A;
* "Third Party" means any third party participating in either parties work, as it pertains to the Agreement
* The terms "Data Subject", "Personal Data", “special categories of personal data”, "processing", "Processor" and "Controller" (and their derivatives) shall have the meanings set out in the applicable Data Protection Laws.

1. **Roles and Responsibilities**

Each Party shall nominate a single point of contact within the organisation who can be contacted in respect of queries or complaints, this person being accountable for the processing activities.

**First Controller - Single Point of Contact**

Name:

Contact Details

**Second Controller - Single Point of Contact**

Name:

Contact Details

1. **Data Protection and General obligations**

When processing personal data, the Parties shall (and shall procure that any of their staff involved in connection with the activities under this Agreement shall) at all times:

1. comply with the provisions and obligations imposed on them by the Data Protection Laws at all times when processing Personal Data in connection with this Agreement, including all relevant notification requirements contained therein.
2. comply with the obligations set out in this agreement and only process the Protected Data for the Purpose and in accordance with the Annex A and B to this Agreement.
3. not do, cause or permit anything to be done which may result in a breach by the other Party of Data Protection Laws.
4. If either Party materially breaches the obligations set out in this Agreement, and, if remediable, such breach is not remedied within 30 days the other Party shall be entitled to terminate this Agreement upon immediate effect.

*General Obligations*

1. Each Party shall ensure that it has in place all necessary notices and lawful basis to enable lawful transfer of Data subjects’ Data in accordance with this Agreement.
2. As part of its compliance with sub-paragraph 1) above and in accordance with Article 13 and 14 of the UK GDPR, the First Controller will share its Privacy Notice with the data subjects (specify when e.g. at the point of first engagement.
3. In accordance with Article 14 of UK GDPR, the Second Controller shall be responsible for providing data subjects with the privacy notice in relation to its own processing of personal data as a data controller. Therefore, the Second Controller will share its Privacy notice with the data subjects (specify when e.g. at the point of first engagement.
4. Each Party shall implement and maintain adequate and appropriate technical and organisational security measures in order to protect Participant Data against unauthorised or unlawful processing, and against accidental loss, destruction or damage. Participant Data should at a minimum always be password protected and the number of staff who can access Participant Data should be restricted to those for whom access is strictly necessary for the relevant processing.
5. Each party shall ensure that the Shared Personal Data are accurate.
6. Notwithstanding any of the provisions of this Agreement, each Party acknowledges that it is responsible for its own compliance with Data Protection Laws.
7. Each party shall be individually responsible towards their obligations as Data Controllers under the Data Protection Laws (which include obligations towards the data subjects and their rights) and provide reasonable assistance, information and co-operation where reasonably requested by the other Party in respect of data protection matters relevant to this agreement, including (but not limited to):
   1. any claim, complaint and/or exercise or purported exercise of rights by a Data Subject under the Data Protection Laws (including Subject Access Request) or any investigation or enforcement activity by the applicable data protection authority, which relates to or is connected with the other Party’s processing of the Protected Data; and
   2. assisting the other Party in complying with its obligations as a Controller. Such assistance may relate to or include responding to a complaint by a Data Subject, investigating a Data Breach, informing the applicable data protection authority and the affected Data Subjects of a Data Breach in accordance with the Data Protection Laws, providing information to Data Subjects on the other Party’s behalf as required by the Data Protection Laws and communicating the other Party’s privacy notices and/or policies to the relevant Data Subjects;
8. If a party receives an Enquiry which relates directly or indirectly to its sharing of personal data pursuant to this Agreement, or to the other party's compliance with the Data Protection Laws, it shall notify the other party as soon as reasonably practicable.
9. Each party shall maintain records of all processing operations under its responsibility that contain at least the minimum information required by the Data Protection Laws and shall make such information available to any Data Protection Regulator on request.
10. Each Party shall conduct a data protection impact assessment before processing the Protected Data, in circumstances where a data protection impact assessment is required pursuant to Article 35 of the UK GDPR.
11. Each party shall provide evidence of its compliance with the Data Protection Laws upon reasonable request of the other Party.
12. Each party shall implement appropriate technical and organisational measures so as to ensure an appropriate level of security is adopted to mitigate the risks associated with its processing of the Protected Data.
13. Each party shall promptly notify the other Party in the event that it receives updates or corrections to any of the Protected Data.
14. **Personal Data Breaches and Reporting Procedures**

Each party shall comply with its obligation to report a Personal Data Breach that does or may affect any of the Shared Personal Data to the appropriate Supervisory Authority and (where applicable) Data Subjects under Article 33 of the GDPR and shall during the term of the agreement inform with no undue delay the other party of any Personal Data Breach irrespective of whether there is a requirement to notify any Supervisory Authority or data subject(s). The notification also applies to any breaches of security which may compromise the security of the shared personal data.

Neither party shall take any action in relation to any Enquiry or Personal Data Breach where it relates to the other party's processing of Personal Data as a "controller" without prior written notice to the other party and providing the other party with a reasonable opportunity to contribute to the response to mitigate the impact of the action on the other party.

The parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any data security breach in an expeditious and compliant manner.

1. **Data Retention**

Neither party shall retain or process Shared Personal Data for longer than is necessary to carry out the Agreed Purposes subject to its obligation to continue to retain Shared Personal Data in accordance with any statutory or industry or professional retention periods applicable under the Data Protection Legislation.

1. **Data Sharing**

The purpose of sharing Personal Data and the specific categories of Personal Data that will be shared are included in Annex A of this Agreement. Each party agrees it shall not process the Personal Data for any reason other than the Purposes included in this agreement.

1. **Indemnity**

When the Parties are acting as data controllers separately or jointly, and in accordance with relevant Data Protection Laws or any other legislation, each party shall hold the other parties acting a controller of data harmless against any liabilities, losses, damages, costs or expenses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of or damage to reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and any other reasonable professional costs and expenses suffered or incurred by the other party to this agreement arising out of or in connection with any claim made against the other party in relation to any breach by other party of the UK GDPR or other obligations under this agreement.

1. **Security and Training**

The data discloser shall be responsible for the security of transmission to the data receiver by using appropriate technical methods. The minimum extent of which is detailed below. The parties to this agreement will ensure that encryption procedures are used for all data concerns whether at rest or in transit

Each Party shall implement appropriate technical and organisational measures to protect the Personal Data in their possession (or held on their behalf) against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration, or disclosure, including but not limited to -

1. Ensuring IT equipment, including portable equipment, is kept in lockable areas when unattended and not leaving portable equipment containing personal data unattended.
2. Ensuring that staff use appropriate secure passwords for logging into systems or databases containing personal data.
3. That all IT equipment is protected by anti-virus software, firewalls, passwords, and suitable encryption devices. Redundant devices will be securely destroyed or professionally sanitized to ensure all residue data is permanently removed.
4. Limiting access to relevant databases and systems to those of its officers, staff agents and sub-contractors who have a legitimate need to access the personal data and ensuring that passwords are changed and updated regularly to prevent inappropriate access when such individuals are no longer engaged by the party.
5. Conducting regular threat assessment or penetration testing on systems and having in place an incident response plan.
6. Ensuring all staff handling personal data have been made aware of their responsibilities regarding the shared personal data.
7. **Resolution of Disputes with Data Subjects or the Data Protection Authority**

In the event of a dispute or claim brought by a data subject or the relevant data protection supervisory authority concerning the processing of shared personal data against any of the parties to this agreement, the parties will inform one other about any such disputes or claims and will reasonably cooperate with a view to an amicable settlement.

The parties agree to respond to any non-binding mediation procedure initiated by a data subject or by the relevant data protection supervisory authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

In respect of breaches relating to the agreement, each party shall abide by a decision of a competent court.

1. **Data Processors and sub-processors**

Where data is shared by a controller with a data processor or sub-processor as defined in the UK GDPR Article 4(8), and where a contract has been made in accordance with Art.28(1-3)(a-h), each of those parties, no matter the number, will be bound by the provision of Data Protection Law and guarantees to implement sufficient technical and organisational measures to protect the data for which the controller or controllers are responsible. The processor will be liable to the relevant controllers for any losses or damages suffered by any party to this agreement who is acting as a controller of data in accordance with Data Protection Law.

It is acknowledged by all parties including processors and their approved sub-processors that liability for compensation for an infringement of the regulation is not limited to the controllers and that in accordance with UK GDPR Art.82(4) each party may be held liable for the entire damage to ensure effective compensation.

A party to this agreement shall be exempt from liability if it can prove it is not in any way responsible for the event.

Where a party to this agreement has paid compensation due to an infringement, that party may in turn claim back from the other controllers or processors concerned, as part of the compensation paid corresponding to their part of the responsibility for the damages.

1. **Waiver**

No failure or delay by either Party in exercising any right or remedy under this Agreement will operate as a waiver of such right or remedy nor will any single or partial exercise or waiver of any such right or remedy preclude its further exercise or the exercise of any other right or remedy.

1. **International Data Transfers**

Neither Party shall transfer any Personal Data received from the other party to any location which is outside the EEA (unless the recipient is based in a country which the European Commission has decided offers sufficiently adequate protection for personal data when compared with the EU (an “Adequate Country”)) without the other party’s prior written consent. If the other party consents to the transfer of Protected Data to a recipient located outside of the EEA and not in an Adequate Country, the Party transferring the Protected Data shall:

consider if any exception applies that would permit the transfer, without undertaking a transfer risk assessment and identifying any appropriate safeguards.

In the absence of any applicable exception, undertake a Transfer Risk Assessment, Identify and apply an appropriate safeguard (e.g. IDTA – International Data Transfer Agreement; UK Addendum - to replace existing EU standards contractual clauses which are no longer valid after 21.03.24; UK binding corporate rules, ICO approved contract clauses).

1. **Governing Law**

This Agreement shall be governed by and construed in accordance with the laws of England and Wales, and the Parties hereby submit to the exclusive jurisdiction of the courts of England and Wales.

1. **Miscellaneous**
2. Nothing in this Agreement is intended to or shall operate to create a partnership or joint venture between the parties, or to authorise either party to act as agent for the other and neither party shall have authority to act in the name of or on behalf of the other, or to enter into any commitment or make any representation or warranty or otherwise bind the other in any way.
3. Neither party may assign, transfer, charge or otherwise encumber, declare a trust over or deal with in any other manner this Agreement or any right, benefit or interest under it, or subcontract any of its obligations under it, without the prior written consent of the other party.
4. Save as expressly provided in this Agreement, the rights and remedies provided under this Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.
5. Unless expressly provided in this Agreement, no term of this Agreement is enforceable pursuant to the Contracts (Rights of Third Parties) Act 1999 by any person who is not a party to it.
6. For the purposes of this clause and in accordance with the GDPR Articles 44, 45 and 46, a transfer of personal data shall mean any sharing of personally identifiable information by any party to another party to this agreement. This agreement does not include -
   1. Onward sharing of the personal data with any other third party acting as a data controller without a legal or contractual obligation
   2. Without prior agreement, the publication of the shared personal data via any medium, including, but not limited to, social media, websites and publicly available communications.
7. The data receiver shall not share the personal data with an organisation which is not a party to this agreement without the express written permission of all parties, or without a legal or professional obligation.
8. If any court or competent authority finds that any provision of this Agreement (or part of any provision) is invalid, illegal or unenforceable, that provision (or part) shall, to the extent required, be deemed to be deleted, and the validity and enforceability of the other provisions of this Agreement shall not be affected. If any invalid, unenforceable or illegal provision of this Agreement would be valid, enforceable and legal if some part of it were deleted, the parties shall negotiate in good faith to amend such provision such that, as amended, it is legal, valid and enforceable, and, to the greatest extent possible, achieves the parties' original commercial intention.
9. In case the applicable data protection and ancillary laws change in a way that the Agreement is no longer adequate for the purpose of governing lawful data sharing exercises, the Parties agree that they will negotiate in good faith to review the agreement in light of the new legislation.
10. No purported variation of this Agreement shall be valid unless it is in writing (which excludes email) and signed by or on behalf of each party.
11. This Agreement constitutes the entire agreement and understanding of the parties with respect to the subject matter of this Agreement and supersedes any prior agreements, representations, understandings or arrangements between the parties (oral or written) in relation to such subject matter. Each party acknowledges that: (a) upon entering into this Agreement, it does not rely and has not relied, upon any representation (whether negligent or innocent), statement or warranty made or agreed to by any person (whether a party to this Agreement or not) except those expressly set out in this Agreement; and (b) the only remedy available in respect of any misrepresentation or untrue statement made to it shall be a claim for damages for breach of contract under this Agreement. Nothing in this paragraph 8) shall limit or exclude any liability for fraud.
12. This Agreement and any dispute or claim (whether contractual or non-contractual) arising out of or in connection with it, its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (whether contractual or non-contractual) arising out of or in connection with this Agreement, its subject matter or formation.
13. If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this agreement. If any one or more of the provisions contained in this Agreement is, in whole or in part, invalid, illegal or unenforceable in any respect, the validity, legality or enforceability of the remaining provisions, the Parties agree to negotiate in good faith to review the Agreement in the light of the new legislation.
14. Nothing in this agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other party.
15. **Entire agreement**

This Agreement together with the Contract/Service Agreement/Funding agreement constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.

1. **Review and Changes in the Law**

This Agreement shall be reviewed in line with the Annex B.

The Parties acknowledge that the arrangements outlined in this Agreement may need to be changed to comply with any changes in the requirements of the Data Protection Laws. Each Party shall cooperate with the other Party in good faith to review and agree and document appropriate and reasonable changes to this Agreement to ensure that it addresses any change in the Data Protection Laws in accordance with good market practice.

1. **Termination**

This Agreement shall continue in force until the sooner of:

1. the Purpose no longer being pursued by the Parties;
2. [the Main Agreement terminating for any reason];
3. [a Party serving at least [3 month’s] written notice on the other Party to terminate the Agreement].

**This Agreement** has been signed on the date appearing at the head of page 1.

Signed for and on behalf of

**First Controller:** [Organization Name]

Signature: ……………………………………….

Name: ………………………………………

Position: ………………………………………

Date: ………………………………………

Signed for and on behalf of

**Second Controller:** [Organization Name]

Signature: ……………………………………….

Name: ………………………………………

Position: ………………………………………

Date: ………………………………………

**Annex A**

The Parties acknowledge that the Personal Data to be shared by the First Controller with the Second Controller is as follows

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Category of Data subjects** | **Categories of data and Specific data held (e.g. Contact details – emails, phone number)** | **Purposes for sharing** | **Lawful basis on which the sharing takes place** |
| **1** | XXX | XXX | XXX | XXX |
| **2** | XXX | XXX | XXX | XXX |
| **3** | XXX | XXX | XXX | XXX |
| **4** | XXX | XXX | XXX | XXX |

The Parties acknowledge that the Personal Data to be shared by the Second Controller with the First Controller is as follows

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Category of Data subjects** | **Categories of data and Specific data held (e.g. Contact details – emails, phone number)** | **Purposes for sharing** | **Lawful basis on which the sharing takes place** |
| **1** | XXX | XXX | XXX | XXX |
| **2** | XXX | XXX | XXX | XXX |
| **3** | XXX | XXX | XXX | XXX |
| **4** | XXX | XXX | XXX | XXX |

**Annex B**

|  |  |
| --- | --- |
| Technical and organisational measures for the secure transfer of the Protected Data | [Set out how the data will be physically shared between the Parties – eg encryption]. |
| Termination Procedure | [Set out what will happen to the Protected Data once the Agreement has come to an end e.g. securely deleted or destroyed]. |
| Review of the Agreement | The Parties shall review this Agreement every [12] months. |
| [Additional information in respect of the data sharing?] | [if relevant, you could decide to include particular ways on how to manage SAR, other data subject’s rights, data breaches etc, giving more detailed information in addition to the provision of this agreement] |