JOINT CONTROLLER AGREEMENT

1 **Definitions and interpretation**

1.1 In this Schedule:

Appropriate Safeguards	means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under the Data Protection Laws from time to time;
CCPA	means means the California Consumer Privacy Act, California Civil Code sections 1798.100 et seq., as amended, and its implementing regulations;
Communication	means a complaint, enquiry, notice, request or other communication (but excluding any Data Subject Request) relating to either party's obligations under any Data Protection Laws in connection with this Agreement and/or the Processing of any of the Shared Personal Data, including any compensation claim from a Data Subject or any notice, investigation or other action from a Data Protection Supervisory Authority relating to any of the foregoing;
Consent	means a freely given, specific, informed and unambiguous indication (by a statement or by a clear affirmative action) by which the relevant Data Subject has agreed to the relevant transfer(s) and/or Processing of the Shared Personal Data relating to them that has not been withdrawn. To the extent the relevant Shared Personal Data is Special Category Personal Data, this definition should be read as if the word 'unambiguous' above read 'unambiguous and explicit'. The terms **freely given**, **specific**, **informed**, **unambiguous** and **explicit** in this definition shall be construed in accordance with Data Protection Laws;
Contact Point	means, in respect of each party, the person identified as such in accordance with paragraph 1 of Appendix 5 of this Schedule;
Controller	has the meaning given in Data Protection Laws;
Data Protection Laws	means, as applicable to either party and/or to the rights, responsibilities and/or obligations of either party in connection with this Agreement: (a) the EU GDPR; (b) the UK GDPR and the Data Protection Act 2018; (c) the Privacy and Electronic Communications (EC Directive) Regulations 2003; (d) any other applicable law relating to the Processing, privacy and/or use of Personal Data; (e) any laws which implement or supplement any such laws; and (f) any laws that replace, extend, re-enact, consolidate or amend any of the foregoing; and (g) the CCPA (as applicable).
Data Protection Supervisory Authority	means any regulator, authority or body responsible for administering Data Protection Laws;
Data Subject	has the meaning given in Data Protection Laws;
Data Subject Request	means a request made by a Data Subject to exercise any right(s) of Data Subjects under Chapter III of the GDPR in relation to any of the Shared Personal Data or concerning the Processing of such data;
Disclosing Party	means each party to the extent it (or any person acting on its behalf) discloses or otherwise makes accessible any Shared Personal Data to the other party (or any person acting on the other party's behalf);
GDPR	means the EU General Data Protection Regulation, Regulation (EU) 2016/679, and the UK GDPR as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further

	amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time);
Permitted Lawful Basis	means the permitted lawful basis under Article 6(1) of the GDPR under which the Shared Personal Data is shared by the Disclosing Party with the Receiving Party and Processed by the Receiving Party, which the parties have agreed are Consent and Legitimate Interests;
Permitted Purpose	means use of the Received Personal Data for the purposes of providing the platform for Collectives on Stack Overflow;
Permitted Recipients	means the following who need access to the Received Personal Data for the Permitted Purpose: *(a)* the relevant Receiving Party's employees; and (b) the relevant Receiving Party's contractors and sub-contractors' (together with their employees);
Personal Data	has the meaning given in Data Protection Laws;
Personal Data Breach	has the meaning given in Data Protection Laws;
Processing	has the meaning given in Data Protection Laws (and related expressions, including **Process**, **Processed** and **Processes** shall be construed accordingly);
Processor	has the meaning given in Data Protection Laws;
Received Personal Data	means Shared Personal Data in respect of which the relevant party is the Receiving Party;
Receiving Party	means each party to the extent it (or any person acting on its behalf) receives or accesses any Shared Personal Data disclosed or made available by the other party (or any person acting on the other party's behalf);
Shared Personal Data	means Personal Data received by or on behalf of one party from or on behalf of the other party, or otherwise made available by one party to the other for the Permitted Purpose;
Special Category Personal Data	means special categories of Personal Data as referred to in Data Protection Laws; and

1.2 Unless the context otherwise requires, references to this Schedule include its Appendices.

2 **Status of this schedule and the parties**

Each party shall be a Controller of the Shared Personal Data. If the parties share the Shared Personal Data, it shall be shared and managed in accordance with the terms of this Schedule.

3 **Compliance with Data Protection Laws**

3.1 Subject to compliance by the other party with its express obligations in other provisions of this Schedule, each party shall at all times comply with all Data Protection Laws in connection with the exercise and performance of its respective rights and obligations under this Agreement.

3.2 This Schedule allocates certain rights and responsibilities among the parties as enforceable contractual obligations between themselves, however nothing in this Schedule is intended to limit or exclude either party's responsibilities or liabilities under Data Protection Laws (including under Article 82 of the GDPR and the duties owed by each party to Data Subjects under any Data Protection Laws).

4 **Agreed basis for sharing**

4.1 The parties have determined that it is necessary to share the Shared Personal Data in order to achieve the Permitted Purpose.

4.2 The parties agree that this Agreement relates to ongoing and routine data sharing.

4.3 The parties have documented additional details relating to the sharing of the Shared Personal Data in Appendix 1 of this Schedule, which includes:

4.3.1 the aims of each party in sharing the Shared Personal Data;

4.3.2 why sharing the Shared Personal Data on the terms of this Agreement is necessary to achieve those aims; and

4.3.3 the benefits to the Data Subjects and/or society of the parties sharing the Shared Personal Data;

5 General obligations

5.1 Each party, to the extent it acts as Receiving Party, undertakes to the relevant Disclosing Party that it shall undertake all Processing of Received Personal Data only:

5.1.1 for the Permitted Purpose in accordance with this Agreement and in all respects in accordance with Data Protection Laws; and

5.1.2 to the extent consistent with the Permitted Lawful Basis,

5.2 The parties agree that in respect of Shared Personal Data, the relevant Disclosing Party:

5.2.1 is, as between the parties and subject to paragraphs 5.3 and 9.1, the primary point of contact for Data Subjects;

5.2.2 subject to paragraphs 5.3 and 9.1, shall direct Data Subjects to its Contact Point in connection with the exercise of their rights as Data Subjects and for any enquiries concerning the Shared Personal Data and identify its Contact Point in all information referred to in paragraphs 5.2.5 and 5.2.11 as the contact point for all Data Subject Requests or other Communications from Data Subjects regarding the sharing or other Processing of such Shared Personal Data;

5.2.3 shall ensure that the Shared Personal Data has been collected, Processed and transferred in accordance with the Data Protection Laws as applicable to that data at all times prior to the receipt of that data by the Receiving Party (or any person acting on its behalf);

5.2.4 shall ensure the Shared Personal Data is accurate and up to date when disclosed or made accessible to the relevant Receiving Party and shall promptly notify the Receiving Party if such Shared Personal Data becomes inaccurate or out of date during the term of this Agreement (together with revised and corrected data);

5.2.5 is solely responsible for both parties' compliance with all duties to provide information to Data Subjects under Articles 5(1)(a), 13 and 14 of the GDPR or any similar Data Protection Laws, including as required for all Processing of Shared Personal Data by or on behalf of the Receiving Party for the Permitted Purpose on the Permitted Lawful Basis in accordance with this Agreement and shall comply with its respective obligations in Appendix 4;

5.2.6 shall ensure that the Shared Personal Data when transferred from the UK to the Receiving Party (or anyone acting on its behalf) in connection with this Agreement:

(a) is not subject (or potentially subject) to any laws giving effect to Article 71 (Protection of personal data) of the agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community; and

(b) is not subject to the laws of any jurisdiction outside of the United Kingdom;

5.2.7 to the extent Consent is identified in this Agreement as the Permitted Lawful Basis in respect of the Shared Personal Data, is solely responsible for obtaining the Consent of Data Subjects, in accordance with Data Protection Laws as required for the transfers and Processing of that Shared Personal Data undertaken by either party in connection with this Agreement;

5.2.8 without prejudice to its other obligations, shall ensure that it is entitled to transfer the Shared Personal Data to the Receiving Party and that the Receiving Party (and each of the Receiving Party's Permitted Recipients) is entitled under all applicable laws and legal theories to Process the Shared Personal Data for the Permitted Purpose in accordance with the terms of this Agreement;

5.2.9 shall promptly notify the Receiving Party if it becomes aware that any such Consent referred to in paragraph 5.2.7 is withdrawn or if a relevant Data Subject has requested that their Shared Personal Data is no longer Processed by either party for the Permitted Purpose;

5.2.10 is solely responsible for ensuring that where the Shared Personal Data was received by the Disclosing Party from a third party, or has been Processed by a third party on behalf of the Disclosing Party, it has in place arrangements with those third parties:

(a) as required by all Data Protection Laws (including, where applicable, Articles 26, 28 and 32 of the GDPR);

(b) which are adequate to permit the Disclosing Party to share the Shared Personal Data with the Receiving Party (and its Permitted Recipients) under all Data Protection Laws; and

(c) as required for the Receiving Party (and its Permitted Recipients) to Process such data in accordance with this Agreement; and

5.2.11 shall make available to Data Subjects the essence of this Schedule (and notify them of any changes to it) as required by Article 26 of the GDPR. Such essence must be outlined in the information provided by the Disclosing Party under paragraph *5.2.5.* Confidential Information shall be redacted when such essence is made available further to this paragraph 5.2.11.

5.3 Notwithstanding the terms of this Schedule, the parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Laws against any relevant party as Controller.

5.4 Each party shall use its reasonable endeavours to assist the other to comply with any obligations under all Data Protection Laws in connection with this Agreement and shall not perform its obligations under this Schedule in such a way as to cause the other party to breach any of the other party's obligations under applicable Data Protection Laws to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

5.5 Without prejudice to any other obligation, if either party becomes aware any of the Shared Personal Data is inaccurate or out of date, it shall promptly notify the other.

6 **Technical and organisational measures**

6.1 The Receiving Party shall at all times:

6.1.1 put in place and maintain appropriate technical and organisational measures as required by Data Protection Laws;

6.1.2 implement and maintain appropriate technical and organisational measures to protect the Received Personal Data in its possession or control against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access, taking into account:

(a) the nature of the data to be protected;

(b) the harm that might result from any failure to so protect the Received Personal Data;

(c) the state of technological development; and

(d) the cost of implementing any measures;

6.1.3 ensure that it has the capability (technological and otherwise), to the extent required by Data Protection Laws, to:

(a) provide, correct or delete at the request of a Data Subject all the Received Personal Data relating to that Data Subject; and

(b) comply with any Data Subject Requests,

provided the relevant Disclosing Party complies with its obligations under this Agreement; and

6.1.4 without prejudice to any other obligation in this paragraph 6, implement and comply with the technical and organisational measures specified in Appendix 3 of this Schedule.

6.2 Each party shall comply with its respective obligations, and may exercise its respective rights and remedies, under Appendix 3 of this Schedule.

7 **Third party Processing**

7.1 Each party undertakes not to disclose or transfer Received Personal Data in respect of which it is the Receiving Party to any third party other than to a Permitted Recipient where necessary for the Permitted Purpose. Each party transferring or disclosing Received Personal Data in respect of which it is the Receiving Party shall ensure it is transferred and disclosed subject to equivalent and legally binding obligations which are no less onerous than those applicable to the Receiving Party under this Schedule.

7.2 In respect of any Processing of Received Personal Data performed by a Processor on behalf of a Receiving Party, that Receiving Party shall:

7.2.1 carry out adequate due diligence on such Processor to ensure that it is capable of providing the level of protection for the Received Personal Data as is required by this Agreement and Data Protection Laws; and

7.2.2 ensure that suitable written agreements are at all times in place with each Processor as required under all Data Protection Laws (including Articles 28 and 32 of the GDPR).

7.3 The relevant Receiving Party shall be liable to the Disclosing Party for all acts and omissions of each of its Permitted Recipients in connection with Received Personal Data. Each obligation in this Schedule on a party to do, or refrain from doing, anything shall include an obligation on that party to ensure all its Permitted Recipients do, or refrain from doing, such thing.

8 **International transfers**

The Receiving Party shall process Received Personal Data outside: (i) both the UK and the European Economic Area ("**EEA**"); or (ii) any other territory in which restrictions are imposed on the transfer of Controller Data across borders under the Data Protection Laws, only in compliance with the Standard Contractual Clauses attached hereto in Appendix 6 in order to put in place Appropriate Safeguards to protect Controller Data.

9 **Dealing with Data Subject Requests and Communications**

9.1 Responsibility for complying with any Data Subject Request or Communication falls on the party which first received such Data Subject Request or Communication. In complying with any Data Subject Request or addressing any Communication each party shall comply with its obligations and as agreed in the section on 'Detailed procedures for addressing Data Subject Requests and Communications' in Appendix 5.

9.2 If either party receives a Communication relating to the Shared Personal Data Processed by (or on behalf of) the other party, it shall:

9.2.1 promptly (and in any event within two Business Days of receipt) notify the Contact Point at the other party; and

9.2.2 consult with the other party in advance of giving any response, to the extent reasonably practicable.

9.3 Without prejudice to paragraph 9.1, if a party which is the Receiving Party receives a Data Subject Request it believes relates to Processing of Received Personal Data, it shall promptly (and in any event within two Business Days of receipt) notify the Contact Point of the Disclosing Party and provide them with full details.

9.4 Each party shall use all reasonable endeavours to provide the other party with full and prompt co-operation and assistance in relation to any Data Subject Request or Communication made to enable the other party to comply with the relevant timescales set out in Data Protection Laws and to find an efficient, timely and amicable solution to any issues arising out of any Data Subject Request or Communication. Without prejudice to the generality of the foregoing, the other party shall respond to any request for co-operation or assistance under this paragraph 9.4 within five days.

10 **Personal Data Breaches**

10.1 Each party shall promptly (and in any event within 48 hours) notify the Disclosing Party if it suspects or becomes aware of any actual or threatened occurrence of any Personal Data Breach in respect of any Received Personal Data which it (or any person acting on its behalf) Processes as Receiving Party. In such circumstances, the relevant Receiving Party shall promptly provide:

10.1.1 sufficient information as the Disclosing Party (or its advisors) reasonably requires to meet any obligations to report a Personal Data Breach under Data Protection Laws (in a timescale which facilitates such compliance);

10.1.2 the Data Protection Supervisory Authorities investigating the Personal Data Breach with complete information as requested by those Data Protection Supervisory Authorities from time to time;

10.1.3 all reasonable assistance the Disclosing Party (or its advisors) requires, including:

(a) co-operation with Data Protection Supervisory Authorities (including with investigations or actions to mitigate or remediate the Personal Data Breach);

(b) making available all relevant data and records required for either party to comply with Data Protection Laws or as otherwise reasonably required by the Disclosing Party;

(c) taking such reasonable steps as are directed by the Disclosing Party to assist in the investigation, mitigation and remediation of a Personal Data Breach (which may include providing the Disclosing Party with physical access to any facilities affected and facilitating the interview of staff and others involved in the matter); and

(d) co-ordination with the Disclosing Party regarding the management of public relations and public statements relating to the Personal Data Breach.

10.2 The Receiving Party's obligations under this paragraph 10 shall be performed at the Disclosing Party's reasonable expense, except to the extent that the Personal Data Breach (or the circumstances giving rise to the Personal Data Breach or it being threatened or suspected) arose out of any negligence or willful default of that Receiving Party or any breach by the Receiving Party of its obligations under this Agreement, in which case the costs shall be borne by the Receiving Party OR Receiving Party's cost and expense.

11 **Data protection impact assessments**

11.1 The parties shall determine whether or not a data protection impact assessment is required in respect of the planned sharing of the Shared Personal Data and if applicable, the parties have completed a data protection impact assessment and have agreed that this Agreement will assist with mitigating certain risks that have been identified.

11.2 Where a party considers that:

11.2.1 a data protection impact assessment is necessary for compliance with Data Protection Law; or

11.2.2 the risks identified by a previous data protection impact assessment necessary for compliance with Data Protection Law may have changed in respect of the sharing or other Processing activities conducted under or in connection with this Agreement,

the other party shall provide such reasonable assistance as that party may reasonably require.

11.3 The assistance referred to in paragraph 11.2 may include:

11.3.1 a systematic description of the envisaged Processing operations and Permitted Purpose of the Processing of the Shared Personal Data;

11.3.2 an assessment of the necessity and proportionality of the Processing operations;

11.3.3 an assessment of the risks to the rights and freedoms of Data Subjects;

11.3.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of the Shared Personal Data; and

11.3.5 any prior consultation with the relevant Data Protection Supervisory Authority which may be necessary.

12 **Records**

Each party shall maintain complete, accurate and up to date written records of all of its Processing of the Shared Personal Data and as necessary to demonstrate its compliance with this Schedule and all Data Protection Laws.

13 **Governance and review**

Prior to sharing the Shared Personal Data, the parties shall establish, and then comply with and maintain, the arrangements set out in Appendix 5 of this Schedule until the earlier of the termination or expiry of this Agreement.

14 **Audit**

14.1 Each party shall (and shall ensure all its Permitted Recipients shall):

14.1.1 make available to the other party such information as is required to demonstrate that party's compliance with its obligations under this Schedule;

14.1.2 not more than once in any 12-month period upon reasonable prior notice allow for, permit and contribute to audits, including inspections, by the other party (or another auditor mandated by the other party) during normal business hours to the extent necessary to verify the audited party's compliance with its obligations under this Schedule; and

14.1.3 provide (or procure) access to all relevant systems, personnel, business premises and records for the purposes of each such audit or inspection referred to in paragraph 14.1.2 and provide (and procure) all further reasonable co-operation, access and assistance in relation to any such audit or inspection.

14.2 Each party shall allow the other to exercise its rights at paragraph 14.1 in the period up to six years after the termination or expiry of this Agreement.

14.3 When conducting audits and inspections, the relevant party conducting the audit or inspection shall comply with the other party's reasonable directions in order to minimise disruption to the other party's business and to safeguard the confidentiality of the other party's Confidential Information. The party subject to the audit or inspection may require any third parties conducting such audit or inspection to enter into direct confidentiality undertakings with it.

15 **Retention**

15.1 Subject to paragraph 15.2, each party shall retain the Received Personal Data in accordance with the retention periods identified for the specific element of the Shared Personal Data in accordance with Appendix 1 of this Schedule.

15.2 The parties shall, to the extent they are Receiving Party:

15.2.1 subject to paragraphs 15.2.2 to 15.2.4 (inclusive), Process all Received Personal Data for no longer than such Processing is necessary for the Permitted Purpose and compliant with this Schedule and all Data Protection Laws;

15.2.2 cease to Process all Received Personal Data on the earlier of termination or expiry of this Agreement; and

15.2.3 immediately, confidentially and securely destroy or dispose of all Received Personal Data (and all copies) in its possession or control that can no longer be Processed in accordance with this Schedule.

16 **Costs**

Except as expressly stated in this Agreement, each party shall pay its own costs and expenses incurred in connection with the negotiation, preparation, signature and performance of this Schedule.

17 **Survival**

Except as otherwise expressly stated in this Schedule, the provisions of this Schedule shall survive termination or expiry of this Agreement and continue indefinitely.

Appendix 1 **The Shared Personal Data**

Shared Personal Data to be shared by Stack with Customer

Reference:	Stack to Customer
Subject matter of Personal Data to be shared	Inviting users to Collectives, assigning tags and recognizing users.
Type of Personal Data to be shared	User ID
Special categories of Personal Data in this data	None
Categories of Data Subject	Users of Collectives
What happens with the data when it is received?	Customer can decide which Stack Overflow users to invite to Collectives to become a recognized user and can invite them to join Collectives. They can also assign tags to specific users/user IDs.

Shared Personal Data to be shared by Customer with Stack

Reference:	Customer to Stack
Subject matter of Personal Data to be shared	Acknowledging invited users to Collectives, assigning tags and recognizing users.
Type of Personal Data to be shared	User ID
Special categories of Personal Data in this data	None
Categories of Data Subject	Users of Collectives
What happens with the data when it is received?	Customer information returns to the public collective site.

APPENDIX 2 FURTHER DETAILS OF THE PERSONAL DATA SHARING

Data sharing objectives

The parties have determined the following aims and objectives of sharing the Shared Personal Data for the Permitted Purpose: To facilitate the use of Collectives.

1 **Necessity**

The parties have determined that sharing the Shared Personal Data on the terms of this Agreement is necessary to achieve those aims because: It will facilitate the Collectives product.

2 **Benefits of data sharing**

The parties have determined the following benefits will be derived by Data Subjects and/or society from sharing the Shared Personal Data: Facilitate the Collectives.

3 **Risks of data sharing and mitigation measures**

3.1 The parties have determined the following risks may arise from sharing the Shared Personal Data and have agreed measures to remove or mitigate such risks, including those measures set out in this Agreement:

Data subjects may not be clear about which entity to exercise their rights with. This has been addressed by providing information in the Collectives Privacy Notice.

4 **Security management**

4.1 Where the relevant Disclosing Party shares Shared Personal Data, it shall provide the Shared Personal Data in a manner consistent with Appendix 1 of this Schedule.

5 **Personnel**

5.1 Each party shall, to the extent it is the relevant Receiving Party, at all times ensure the Processing of the Received Personal Data by natural persons shall be limited to its employees and the employees of its Permitted Recipients (collectively, **personnel**) that need to Process it for the relevant Permitted Purpose in accordance with this Agreement and that all such personnel:

5.1.1 are reliable and have undergone adequate training in the use, care, protection and handling of Received Personal Data as required for compliance with all Data Protection Laws and this Schedule ;

5.1.2 are informed of the confidential nature of the Received Personal Data and the relevant party's obligations under this Appendix 3 and subject to appropriate obligations of confidentiality;

5.1.3 do not publish, disclose or divulge any of the Received Personal Data to any third party where the party subject to this obligation would not be permitted to do so;

5.1.4 are subject to (and comply with) a binding written contractual obligation to keep the Received Personal Data confidential (unless disclosure is required under applicable UK or EU Law); and

5.1.5 are aware of and comply with their duties under this Schedule and those in the MSA;

APPENDIX 4 TRANSPARENCY ARRANGEMENTS

See link to Collectives ™ Privacy Notice https://stackoverflow.com/legal/privacy-policy

6 **Contact Points**

6.1 The Contact Point for Stack is privacy@stackoverflow.com in relation to Privacy and Data Protection matters or as notified to Customer in writing from time to time in accordance with the Privacy Notice provisions.

6.2 The Contact Point for Customer is the notice address as specified in the MSA (or as notified to Stack in writing from time to time in accordance with the MSA).

6.3 privacy@stackoverflow.com shall be the first contact points for third parties in relation to Data Subject Requests and Communications and any other matter relating to the Shared Personal Data. Each party's respective Contact Point shall have overall internal responsibility within their respective party for appropriately addressing and responding to Data Subject Requests and Communications within the scope of that party's obligations.

6.4 Any notice or communication that is required by this Schedule to be sent to a Contact Point shall be sent to the relevant contact method or email address of the Contact Point. Such notices and communications shall be deemed delivered in accordance with the same rules specified in the MSA.

7 **Reporting**

7.1 The parties each undertake that they shall report to the other party on:

7.1.1 the volume of Data Subject Requests (or purported Data Subject Requests) relating to Shared Personal Data from Data Subjects (or third parties on their behalf); and

7.1.2 any Communications relating to the Shared Personal Data (including any requests for disclosure of the Shared Personal Data which is required or purported to be required by applicable law),

provided that it has received a Request during that period.

8 **Relationship between Contact Points**

8.1 The Contact Points of each party shall meet, by phone if necessary, coordinated with the regular client meetings not less than once every three months to manage the relationship between the parties and assess:

8.1.1 the overall effectiveness of the sharing arrangements set out in this Agreement;

8.1.2 any Communications or other areas of concern;

8.1.3 whether each Permitted Lawful Basis and Permitted Purpose remain valid and appropriate;

8.1.4 whether the benefits as set out in Appendix 2 of this Schedule are being delivered and whether the Shared Personal Data needs to continue to be shared;

8.1.5 whether the privacy notices and arrangements under this Agreement remain appropriate;

8.1.6 the latest quality checks conducted under Appendix 2 of this Schedule (or any similar data);

8.1.7 whether the risks of the data sharing have changed; and

8.1.8 whether the technical and organizational measures as set out at Appendix 3 of this Schedule are adequate.

8.2 Following each meeting pursuant to this paragraph 3, the Contact Points shall promptly provide a joint report of their findings to the relevant stakeholders.

9 **Quality Checks**

The parties shall each conduct a periodic test of a sample of Shared Personal Data in respect of which it is Disclosing Party to test that it is accurate and up to date. Such test shall be conducted at least once in each 12 months of the term of this Agreement. The parties may rely on a test of the same or substantially similar data set which it may have conducted in the previous 12 months, including under other data sharing arrangements with third parties.

10 **Review**

10.1 The parties shall review periodically the content of this Schedule (the **Review**), which shall include confirmation:

10.1.1 that the arrangements reflect current practice and the objectives of the parties;

10.1.2 that the scope of the Permitted Purpose is still relevant and the scope for which the Shared Personal Data is being used by the Receiving Party has not been expanded without agreement of the parties;

10.1.3 that the benefits to the Data Subjects or society, as stated in Appendix 2 of this Schedule are being realized;

10.1.4 whether the arrangements in this Appendix 5 are adequate and working in practice;

10.1.5 that any relevant new guidance issued by any Data Protection Supervisory Authority raised by either party during the Review has been considered as part of the Review;

10.1.6 whether the Shared Personal Data should continue to be shared under this Agreement; and

10.1.7 that the Data Subjects are still the focus of the sharing arrangement and whether their rights are being respected.

10.2 The Review shall take place at least every *six* months during the first two years following its commencement, and at least every 12 months thereafter.

stackoverflow

APPENDIX 6 **EU GDPR—2021 standard contractual clauses (SCCs) for the transfer of personal data to third countries—module one—controller to controller**

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.5 (e) and Clause 8.9(b);

(iii) [Not used]

(iv) Clause 12(a) and (d);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation ([2]) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of

natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union ([3]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

[Not used]

Clause 10

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. ([4]) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([5]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.**]**

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(a) **Where the data exporter is established in an EU Member State:** The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

OR

(a) **Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:** The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

OR

(a) **Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:** The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.**]**

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([6]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to

communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of [*specify Member State*].

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of [*specify Member State*].

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Footnotes:

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(2) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.
(3) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.
(4) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.
(5) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.
(6) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

APPENDIX

EXPLANATORY NOTE:
It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. **LIST OF PARTIES**

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1.	Name: Stack Exchange, Inc. Address: 110 William Street, 28th Floor, New York, NY 10038 Contact person's name, position and contact details: See Item 2. Activities relevant to the data transferred under these Clauses: Collectives – provision of question and answer platform for developers. Signature and date: [.....] Role (controller/processor): Controller
2.	EU Representative Denis Nikolaev, MD Stack Overflow 63 Frieslandstraat, Amsterdam, 1082TL, Netherlands

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

1.	Name: Customer listed in the applicable MSA Address: As listed in the applicable MSA Contact person's name, position and contact details: As listed in the notice provision of the MSA Activities relevant to the data transferred under these Clauses: Placing of tags, inviting users to Collectives page of Question and answer platform for developers. Signature and date: [.....] Role (controller/processor): Controller
2.	[.....]

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

Users of the Collectives service

Categories of personal data transferred

User ID

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

[NONE]

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis

Nature of the processing

Inviting users to Collectives, assigning tags and recognizing users.

Purpose(s) of the data transfer and further processing

Customer can decide which Stack Overflow users to invite to Collectives to become a recognized user and can invite them to join Collectives. They can also assign tags to specific users/user IDs.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data will be retained for as long as it is required and if user relationship ends, data will be retained subject to any legal limitation periods or where it is required in order to establish or defend claims.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

None

C. **COMPETENT SUPERVISORY AUTHORITY**

Identify the competent supervisory authority/ies in accordance with Clause 13

Netherlands

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organizational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

[*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*]

Due to the nature of the processing and the nature of the joint-controllership between the Parties, it is unlikely that the Customer will transfer any personal data as Importer. However, in the event that such transfer occurs, the following measures described below shall apply:

- Measures of pseudonymization and encryption of personal data
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing
- Measures for user identification and authorization – both internal and third-party service providers are used to authenticate and verify user IDs, for example at sign in stage.
- Measures for the protection of data during transmission – encryption
- Measures for the protection of data during storage -encryption
- Measures for ensuring physical security of locations at which personal data are processed – internal processes and for external third-party locations, contractual safeguards to ensure physical security of locations
- Measures for ensuring events logging- IT systems and internal policies.
- Measures for ensuring system configuration, including default configuration – internal IT systems
- Measures for internal IT and IT security governance and management – internal governance and management systems,
- Measures for certification/assurance of processes and products – certification processes where applicable.
- Measures for ensuring data minimization -internal compliance policies (data protection by design and default) to ensure only minimum amt of data is used.
- Measures for ensuring data quality internal measures to ensure data quality
- Measures for ensuring limited data retention- data retention policies – data is only retained for as long as it is required,
- Measures for ensuring accountability- DPIAs, audits as required.
- Measures for allowing data portability and ensuring erasure]- measures incorporated into the DSAR process