STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1
Purpose and scope

1. 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) for the transfer of personal data to a third country.
2. The Parties:
    a. 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
    b. 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').
3. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
4. 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

1. 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 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.

2. 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

1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
    a. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
    b. Clause 8 – Module One: Clause 8.5 (5) and Clause 8.9(2); Module Two: Clause 8.1(2), 8.9(1), (3), (4) and (5); Module Three: Clause 8.1(1), (3) and (4) and Clause 8.9(1), (3), (4), (5), (6) and (7); Module Four: Clause 8.1 (2) and Clause 8.3(2);
    c. Clause 9 – Module Two: Clause 9(1), (3), (4) and (5); Module Three: Clause 9(1), (3), (4) and (5);
    d. Clause 12 – Module One: Clause 12(1) and (4); Modules Two and Three: Clause 12(1), (4) and (6);
    e. Clause 13;
    f. Clause 15.1(3), (4) and (5);
    g. Clause 16(5);
    h. Clause 18 – Modules One, Two and Three: Clause 18(1) and (2); Module Four: Clause 18.
2. Paragraph (1) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
3. 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 – Optional
Docking clause

1. 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.
2. 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.
3. 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 Instructions

1. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
2. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 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, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

1. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties 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 subjects. 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. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain

under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

2. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
3. 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 breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
4. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 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 and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

1. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
2. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate

documentation on the processing activities carried out on behalf of the data exporter.

3. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
4. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
5. The Parties shall make the information referred to in paragraphs (2) and (3), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

1. OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [Specify time period] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.
2.
3. OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify

time period] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

4. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
5. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
6. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
7. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

1. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

2. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
3. In fulfilling its obligations under paragraphs (1) and (2), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

1. 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.
   [OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such a redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]
2. 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.
3. 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:
   a. 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;
   b. refer the dispute to the competent courts within the meaning of Clause 18.

4. 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 of Regulation (EU) 2016/679.
5. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
6. 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

1. 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.
2. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
3. Notwithstanding paragraph (2), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
4. The Parties agree that if the data exporter is held liable under paragraph (3) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
5. 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.

6. The Parties agree that if one Party is held liable under paragraph (5), 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.
7. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

1. [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

   [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 and has appointed a representative pursuant to Article 27 of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27 of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

   [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 without however having to appoint a representative pursuant to Article 27 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.
2. 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

1. 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 of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
2. The Parties declare that in providing the warranty in paragraph (1), they have taken due account in particular of the following elements:
    a. 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;
    b. 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;
    c. 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.

3. The data importer warrants that, in carrying out the assessment under paragraph (2), 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.
4. The Parties agree to document the assessment under paragraph (2) and make it available to the competent supervisory authority on request.
5. 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 (1), 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 (1).
6. Following a notification pursuant to paragraph (5), 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(4) and (5) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

1. 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:
    a. 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
    b. 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.
2. 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.
3. 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.).
4. 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.

5. Paragraphs (1) to (3) are without prejudice to the obligation of the data importer pursuant to Clause 14(5) 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

1. 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(5).
2. 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. 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

1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
2. 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(6).

3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
    a. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (2) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
    b. the data importer is in substantial or persistent breach of these Clauses; or
    c. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.
4. 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.
5. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (3) 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.
6. Either Party may revoke its agreement to be bound by these Clauses where
    a. the European Commission adopts a decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or
    b. 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

[OPTION 1: 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).]

[OPTION 2: These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow 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

1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
2. The Parties agree that those shall be the courts of _____ (specify Member State).
3. 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.
4. The Parties agree to submit themselves to the jurisdiction of such courts.

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

1.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]

Name: ...
Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): ...

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

Name: Codility Limited
Address: 107 Cheapside

9th Floor
London EC2V 6DN
United Kingdom
VAT ID: GB 981191408

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): Processor
B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Candidates, employees

Categories of personal data transferred
The personal data of candidates processed by Codility is predominantly contact information, but may also include details relating to the candidates' education and current professional role. This data is either entered by the customer (ie. a Recruiter) and/or by the candidate directly. This information is provided to the customer by the candidate.

Customers may specify that candidate data be anonymised.
Data likely includes:
First name
Last name
Email address
Data may also include (at the request of the customer):
School attended
Degree/Field
Years of experience
Profile URL (for example, their GitLab account, Linkedin profile)
Phone number
The level of detail is configured by the customer (ie. account admin). Only the email address is required for invites to be sent to Candidates.

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.
N/A

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

Nature of the processing
This data are used for several of purposes including:

- Inviting candidates to participate in CodeCheck tests that assess their skills and competence in relevant areas such as coding and software development
- Inviting candidates to online interviews on CodeLive with customers (engineers running interviews).
- Providing feedback to customers on candidate performance in assessments and online interviews

Purpose(s) of the data transfer and further processing
Performing services according to contractual obligations

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
Customer data is kept while the customer has an active contract, and for up to 90 days after a contract ends or is terminated. Application logs are kept while the customer has an active contract, and for up to 1 year after a contract ends or is terminated.

As Codility is defined as the Data Processor of Candidates' data the company is obliged to handle data in line with the instructions given by the Data

Controller (the Customer). Codility expects to return and /or delete Candidate data at a time defined by the contract governing the provision of Codility's services to the customer. In some cases, personal data are anonymised for statistical analysis and research purposes.

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

C. COMPETENT SUPERVISORY AUTHORITY

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

...

ANNEX II

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

EXPLANATORY NOTE:

The technical and organisational 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.

Measures of pseudonymisation and encryption of personal data

Codility applies only tested encryption technologies to help secure your corporate data. The access to our service as well as the user data are encrypted with TLS 1.2 (AES256). Additionally, all the backup data are stored and secured with OS-level encryption (AES 256).
Data is also anonymised using random strings of numbers. This process cannot be undone.

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
Codility is performing backups of data and all backups are redundant which means we can restore all data in a timely manner.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
Codility is undergoing external audits on an annual basis. Also on an ongoing basis the InfoSec Team is monitoring the controls and processes performance inside the company. Team is constantly monitoring systems where data is being processed.

Measures for user identification and authorisation
Users identification is performed using JumpCloud and GSuite accounts. Both require an MFA. Accesses are connected with account and user privileges.

Measures for the protection of data during transmission
Codility applies only tested encryption technologies to help secure your corporate data. The access to our service as well as the user data are encrypted with TLS 1.2 (AES256). Additionally, all the backup data are stored and secured with OS-level encryption (AES 256).

Measures for the protection of data during storage

Codility applies only tested encryption technologies to help secure your corporate data. The access to our service as well as the user data are encrypted with TLS 1.2 (AES256). Additionally, all the backup data are stored and secured with OS-level encryption (AES 256).

Measures for ensuring events logging

Codility gathers and stores logs for the purposes of monitoring, debugging, and reacting to possible problems; in particular, we use them to make sure our verification process is fair and unbiased. We use ELK stack for logs storing and processing, which provides replication mechanisms. Our logs show access to and modifications of the Personal Information. We also backup the log database. Copy of logs from Codility Platform can be obtained upon request.

Measures for ensuring system configuration, including default configuration

Codility created standards for different systems and how they should be configured. The Codility IT Team is making sure that all systems are configured properly.

Measures for internal IT and IT security governance and management

Codility is certified with ISO 27001 and has implemented all necessary policies and controls to make sure Codility information security system is compliant with the highest standards.

Measures for certification/assurance of processes and products

Codility is undergoing regular external audits to make sure that our product is secured.

Measures for ensuring data minimisation

The personal data of candidates processed by Codility is predominantly contact information, but may also include details relating to the candidates' education and current professional role. This data is either entered by the customer (ie. a Recruiter) and/or by the candidate directly. This information is provided to the customer by the candidate.

Customers may specify that candidate data be anonymised.

- Data likely includes:
- First name
- Last name

- Email address

Data may also include (at the request of the customer):

- School attended
- Degree/Field
- Years of experience
- Profile URL (for example, their GitLab account, Linkedin profile)
- Phone number

The level of detail is configured by the customer (ie. account admin). Only the email address is required for invites to be sent to Candidates.

Measures for ensuring limited data retention

Customer data is kept while the customer has an active contract, and for up to 90 days after a contract ends or is terminated. Application logs are kept while the customer has an active contract, and for up to 1 year after a contract ends or is terminated.

As Codility is defined as the Data Processor of Candidates' data the company is obliged to handle data in line with the instructions given by the Data Controller (the Customer). Codility expects to return and /or delete Candidate data at a time defined by the contract governing the provision of Codility's services to the customer. In some cases, personal data are anonymised for statistical analysis and research purposes.

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure

All data is stored on digital media which can be easily accessed and moved around.

Also upon direct request to our DPO and security team data can be easily erasure

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Codility make sure that the sub processors are using the same measusers as Codility.

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

The table below lists the sub-processors Codility uses with the service the sub-processor provides, the data type, the country or location of the destination of the transfer and the measures in place to ensure compliance with the GDPR. Further information regarding the security measures put in place by Codility's processors and sub-processors can be viewed at the relevant corporate websites.

Sub-Processor	Use Case	Data Type	Location	Measures	Notes	Additional Information
Miro	Whiteboard	Anonymous	US	ISO 27001 certified and SOC II Compliant, Standard Contractual Clauses		Miro, 201 Spear Street, Suite 1100, San Francisco, CA 94105 trust@miro.com
Elastic	Logs Storage	Anonymous	US	ISO 27001 certified and SOC II Compliant, Binding Contract		800 West El Camino Real Suite 350 Mountain View, California 94040 info@elastic.co
Hotjar	Usage analytics	Anonymous	EU	ISO 27001 certified		Hotjar Ltd Dragonara Business Centre 5th Floor, Dragonara Road, Paceville St Julian's STJ 3141 Malta, Europe
Satismeter	Customer feedback	Anonymous	EU	Binding Contract,	Registered In the Czech Republic	SatisMeter s.r.o., a company registered under the laws of Czech Republic in the

				Data Processing Agreement, GDPR compliant		Commercial Register kept by the Municipal Court in Prague, Section C, Inset 243804, and having its registered office at Česká 1113/1, Prague 5, 158 00, Czech Republic. ondrej.sedlacek@satismeter.com
Typeform	Candidate feedback	Personal	EU	Binding Contract, Data Processing Agreement, GDPR compliant	Registered In Barcelona, Spain	TYPEFORM SL (Carrer Bac de Roda, 163, local, 08018 - Barcelona (Spain)
Amazon (AWS)	Database and back-ups	Personal	US	ISO 27001 certified and SOC II Compliant, Binding Contract		AWS, 410 Terry Ave N Seattle, WA, 98109-5210 United States
Rackspace	Back-ups	Anonymous	US	ISO 27001 certified, Binding Contract, Binding Contract		1 Fanatical Pl Windcrest, TX, 78218-2179 United States
Sendgrid	E-mails	Personal	US	ISO 27001 certified, Standard Contractual Clauses	Acquired by Twilio	75 Beale St #300, San Francisco
Google Analytics	Usage analytics	Anonymous	US	ISO 27001 certified and SOC II Compliant, Binding Contract		600 Amphitheatre Parkway in Mountain View, California, United States.Floor 28 San Francisco, CA 94111
Mixpanel	Usage analytics	Anonymous	EU	GDPR compliant		One Front Street, Floor 28 San Francisco, CA 94111
Twilio	Video conferencing	Personal	US	ISO 27001 certified, Standard Contractual Clauses		75 Beale St #300, San Francisco
Mailchimp	Newsletters	Personal	US	SOC II Compliant, Standard		The Rocket Science Group, LLC 675 Ponce de Leon Ave NE

				Contractual Clauses		Suite 5000 Atlanta, GA 30308 USA
Sumasoft	Customer Service Services	Personal	EU	ISO 27001 certified		Suma Center, 2nd Floor, Opposite Himali Society, Erandawane, Pune, Maharashtra – 411004
Salesforce	Customer Relationship Management	Personal	EU & US	ISO 27001/17/18 certified, SOC Compliant, Binding Contract		Salesforce Tower 415 Mission Street, 3rd Floor San Francisco, CA 94105 Main: 1-800-NO-SOFTWARE Fax: 415-901-7040 Sales: 1-800-NO-SOFTWARE
SalesLoft	Sales Management	Personal	US	ISO 27001/17/18 certified, SOC II Compliant, Standard Contractual Clauses		Atlanta (HQ), GA United States 1180 W Peachtree St NW #600
Zendesk	Customer Service Software	Personal	US	ISO 27001 certified, SOC II compliant, Binding Contract		1019 Market St, San Francisco
ChurnZero	Sales Management	Personal	US	SOC II Compliant, Standard Contractual Clauses		Arlington (HQ), VA United States 2231 Crystal Dr