SCHEDULE 1

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

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 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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

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

(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

Not applicable: the Parties have elected not to permit additional parties to accede to these Clauses.

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

(a) 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.

(b) 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

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, 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 organizational 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.

(b) The data importer shall grant access to 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 authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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.

(d) 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 ([2]) (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:

(i) 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;

(ii) 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;

(iii) 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

(iv) 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

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) 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.

(c) 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.

(d) 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.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorization 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 30 (Thirty) days 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.

(b) 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. ([3]) 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.

(c) 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.

(d) 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.

(e) 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

(a) 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 authorized to do so by the data exporter.

(b) 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 organizational 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.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

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.

(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) 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.

(c) Notwithstanding paragraph (b), 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.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) 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.

(e) 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.

(f) The Parties agree that if one Party is held liable under paragraph (e), 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.

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

Clause 13

Supervision

(a) The competent supervisory authority shall be determined as follows:

(i) 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 shall act as competent supervisory authority.

(ii) Where the data exporter is not established in an EU Member State but has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which such representative is established shall act as competent supervisory authority.

(iii) Where the data exporter is not established in an EU Member State and is not required to appoint a representative, the supervisory authority of the Member State in which the data subjects whose personal data is transferred are located shall act as competent supervisory authority.

(iv) Where specified in the Order Form, the supervisory authority identified therein shall act as competent supervisory authority, provided such designation is consistent with the above principles.

(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 ([4]);

(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: (a) the law of the EU Member State specified in the Order Form (if applicable); or (b) where no such law is specified in the Order Form, the law of the EU Member State in which the data exporter is established; or (c) where the data exporter is not established in an EU Member State, the law of Ireland.

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: (i) the courts of the EU Member State specified in the Order Form (if applicable); or (ii) where no such courts are specified in the Order Form, the courts of the EU Member State in which the data exporter is established; or (iii) where the data exporter is not established in an EU Member State, the courts of Ireland.

(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.

---

[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] 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.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[4] 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 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):

Name: The entity identified as "Customer" or "Controller" in the applicable Order Form

Address: As set out in the Order Form

Contact person's name, position and contact details: As set out in the Order Form or as otherwise notified in writing

Activities relevant to the data transferred under these Clauses: Use of the data importer's services as described in the Agreement and Order Form

Signature and date: By entering into the Order Form that incorporates this DPA, the data exporter is deemed to have signed these Clauses

Role: Controller

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

Name: Actionable Science Inc

Address: 11501 Dublin Blvd, STE 200, Dublin 94568

Contact person's name, position and contact details: Saurabh Kumar, CEO and Chief Privacy Officer, saurabh@rezolve.ai

Activities relevant to the data transferred under these Clauses:

Provision, operation, and support of an AI-powered service desk and employee support platform on behalf of the data exporter, including:

- Hosting and secure storage of personal data within cloud infrastructure used to deliver the services
- User account administration, authentication, authorization, and role-based access management
- Processing of service requests and support interactions submitted by authorised users
- Delivery of technical support and customer assistance related to the services
- Monitoring, logging, and analysis of system usage, access, and security-relevant events for operational, performance, and security purposes
- Implementation of security controls, incident detection, investigation, response, and remediation

- Performance of encrypted backup, disaster recovery, and service continuity activities
- System maintenance, updates, and reliability improvements necessary to operate the services
- Compliance, audit support, and documentation necessary to demonstrate adherence to applicable data protection obligations
- Retention of personal data for the duration of the services and deletion or return of personal data upon termination in accordance with the Agreement and Clause 8.5 of the SCCs
- Such other processing activities as may be necessary to provide the services described in the Agreement and as instructed by the data exporter from time to time.

Signature and date: By entering into the Order Form that incorporates this DPA, the data importer is deemed to have signed these Clauses

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: Data exporter's employees and authorized users of the data exporter's systems.

Categories of personal data transferred:

- **Name:** Full name of data exporter's employees and authorised users as registered on the platform for user identification and support ticket attribution
- **Business email address:** Corporate email addresses used for user authentication, account management, service notifications, and correspondence relating to support requests
- **Job title and company affiliation:** Professional role and departmental information used for access control, ticket routing, and service entitlement verification
- **IP address:** Internet Protocol addresses collected during platform access for security monitoring, session management, and technical troubleshooting
- **Usage metadata:** Platform interaction data including login timestamps, session duration, service requests submitted, features accessed, and system-generated logs necessary for service delivery, performance monitoring, and technical support

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No special categories of personal data (as defined in Article 9 of Regulation (EU) 2016/679) or data relating to criminal convictions and offences (Article 10 of Regulation (EU) 2016/679) are intended to be transferred or processed under these Clauses.

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

Continuous, on an ongoing basis as part of the provision of services under the Agreement.

Nature of the processing

The data importer carries out the following processing activities in connection with the provision of services to the data exporter:

- Hosting and storage of personal data on cloud infrastructure
- Account administration and access management
- Service delivery and support
- Logging and monitoring of access and security-relevant events
- Encrypted backups and restoration
- Incident response and security management
- Deletion or return of data upon termination

Purpose(s) of the data transfer and further processing

To provide, support, and maintain the data importer's services to the data exporter under the Agreement.

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

Personal data shall be retained for the duration of the Agreement between the parties. Upon termination or expiry of the Agreement, personal data shall be deleted or returned to the data exporter in accordance with Clause 8.5 and the data processing provisions of the Agreement. If the Agreement does not specify a post-termination deletion period, personal data shall be deleted within one (1) year following termination, unless a shorter period is agreed in writing.

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

See Annex III for details of authorized sub-processors. The duration of sub-processor processing is co-extensive with the duration of the main processing relationship under these Clauses.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority for the purposes of these Clauses shall be:

(a) Where the data exporter is established in an EU Member State: the supervisory authority of that Member State;

(b) Where the data exporter is established in the United Kingdom only: Not applicable to EU SCCs (see UK IDTA for UK transfers);

(c) Where the data exporter is established outside the EU/UK but within GDPR territorial scope: the supervisory authority identified in the Order Form, or in the absence of such identification, the Irish Data Protection Commission (as the supervisory authority of the Member State where the data importer's EU-based sub-processor infrastructure is primarily located);

(d) Where specified in the Order Form, the supervisory authority identified therein, provided such designation is consistent with the requirements of Clause 13.

For the avoidance of doubt, where transfers are subject to UK Data Protection Laws rather than Regulation (EU) 2016/679, the Information Commissioner's Office shall act as competent supervisory authority pursuant to the UK International Data Transfer Addendum.

ANNEX II

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

Description of the technical and organizational 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 pseudonymization and encryption of personal data:

- All personal data in transit is encrypted using Transport Layer Security (TLS) 1.2 or higher.
- All personal data at rest is encrypted using Advanced Encryption Standard (AES-256) or equivalent encryption mechanisms provided through Microsoft Azure's managed encryption services.
- Encryption keys are managed through Azure Key Management services with access restricted to authorised personnel.
- Data at rest is stored in encrypted format using Azure SQL Database built-in encryption mechanisms, ensuring data remains secure even if physical storage is compromised. Data in transit uses TLS 1.2 protocol for all network transmissions, ensuring data integrity and privacy between communicating applications. Encryption algorithms are limited to proven, standard algorithms (SHA2, AES, RSA) approved by the Security Steering Committee. All communication between public networks and internal office networks is encrypted. HTTPS protocol is enforced for all internal and external applications. Portable media containing company information is encrypted. For wireless networks, transmissions are encrypted using WPA2 technology, IPsec VPN, or TLS.
- Encryption key management procedures are in place to support organizational use of cryptographic techniques. Appropriate tools are used to generate strong cryptographic keys. Key length and encryption algorithms are determined based on applicable legal requirements and risks identified through risk assessment procedures. Encryption keys are stored securely in encrypted format. Encryption keys for sensitive data are changed at least semi-annually.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services:

- Role-based access control (RBAC) ensuring access is limited to authorised personnel based on job function.
- Least-privilege principles applied to access provisioning.
- Multi-factor authentication (MFA) required for administrative and privileged access.
- Access provisioning and de-provisioning tied to HR processes and role changes.
- Access rights reviewed periodically and revoked promptly upon role change or termination.

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:

- Regular encrypted backups performed and stored in controlled, access-restricted environments.
- Backup access is restricted.
- Restoration procedures documented and tested periodically to ensure availability and integrity.

Measures for security incident response and recovery:

- A documented Incident Response Plan addresses ransomware, cloud security, and data breach scenarios.
- Immediate containment procedures isolate affected systems to prevent further unauthorised access.
- Forensic evidence and audit logs are preserved prior to any restoration activities.
- Root cause analysis and mitigation of exploited vulnerabilities are completed before system restoration.
- A designated incident response coordinator manages and coordinates all aspects of incident response.
- Backups are protected with immutability and isolation to ensure ransomware resilience.
- Business continuity targets are established with defined recovery time objectives appropriate to the criticality of the services, documented in the data importer's internal business continuity plan.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing:

- Security controls are subject to ongoing monitoring.
- Periodic vulnerability scanning conducted.
- Internal security reviews conducted.
- Incident response procedures maintained and tested through periodic exercises.
- A dedicated Breach Response Team is established comprising senior leadership with appropriate authority and expertise in executive management, data protection, information security, and technical operations.
- Breach identification occurs through a combination of manual procedures (internal incident reporting, client notification channels) and automated detection systems (including but not limited to intrusion detection, security monitoring, behavioural analytics, and content inspection technologies).
- Upon confirming a personal data breach, the data importer notifies the data exporter without undue delay in accordance with Clause 8.6(c) of these SCCs.
- Notification content includes: nature of the breach, categories and approximate numbers of data subjects and personal data records affected, likely consequences, and measures taken or proposed to mitigate adverse effects.
- A breach register is maintained documenting all personal data breaches regardless of whether notification to supervisory authorities is required.

Measures for user identification and authorization:

- Role-based access controls aligned to job function requirements.

- Least-privilege principles applied.
- Access provisioning and de-provisioning tied to HR processes and role changes.
- Multi-factor authentication for administrative and privileged access.
- Periodic access reviews.

Measures for the protection of data during transmission:

- TLS 1.2 or higher encryption for all data in transit.

Measures for the protection of data during storage:

- AES-256 or equivalent encryption for data at rest provided through Microsoft Azure's managed encryption services.
- Encryption keys logically protected and access restricted.

Measures for ensuring physical security of locations at which personal data are processed:

- Personal data is processed in Microsoft Azure data centres.
- Azure data centres implement layered physical security controls including access restrictions, surveillance, and environmental safeguards.

Measures for ensuring events logging:

- System access, administrative actions, and security-relevant events are logged centrally.
- Logs are protected against unauthorised modification.
- Logs are monitored for anomalous activity to support detection and incident response.

Measures for internal IT and IT security governance and management:

- Mandatory security and privacy training for personnel.
- Confidentiality obligations included in employment contracts.

Measures for certification/assurance of processes and products:

- ISO 27001 certification maintained.
- SOC 2 certification maintained.
- Third-party audit reports available upon request subject to confidentiality obligations.

Measures for ensuring limited data retention:

- Personal data retained only for the duration necessary to fulfil the purposes of processing.
- Upon termination of the agreement, data deleted or returned in accordance with documented data retention and deletion procedures.
- Deletion applies to production systems and backups within defined and controlled timeframes.
- During the term of the Agreement, the data exporter is responsible for deleting personal data of departed employees and users via the platform's administrative functions. Upon termination of the Agreement, the data importer is responsible for bulk deletion or return of all remaining personal data in accordance with Clause 8.5 of the SCCs and the agreed upon retention period.

Measures for assisting the data exporter in responding to data subject requests:

- The data importer maintains administrative interfaces enabling the data exporter to access, view, correct, export, and delete personal data of individual data subjects.

- Upon reasonable request, the data importer provides technical assistance to locate and retrieve personal data relating to identified data subjects.
- The data importer's systems support data portability through standard export formats (e.g., CSV, JSON).
- Deletion requests can be processed through the platform's administrative functions; the data importer confirms deletion upon request.
- The data importer responds to data exporter enquiries regarding data subject requests within five (5) business days, or sooner where required to meet regulatory deadlines.

For transfers to (sub-) processors, also describe the specific technical and organizational 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

- Sub-processors engaged pursuant to Clause 9 are required by contract to implement adequate technical and organisational measures providing a level of protection for personal data.
- Sub-processor arrangements include data protection obligations.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors:
1. Name: Microsoft Corporation (Azure)

Address:
One Microsoft Way, Redmond, Washington 98052, United States

Contact person’s name, position and contact details:
Microsoft Data Protection Officer
Email: privacy@microsoft.com

Description of processing (including a clear delimitation of responsibilities):
Provision of cloud infrastructure, hosting, storage, networking, security, monitoring, and support services used to operate the Controller’s services.

Location of processing / transfer mechanism:

EU and United States; transfers safeguarded by SCCs and supplementary measures as described in Microsoft’s DPA.

2. Name: Anthropic PBC

Address:

548 Market Street, PMB 90375, San Francisco, California 94104, United States

Contact person's name, position and contact details:

Anthropic Privacy Team / Data Protection Officer

Email: privacy@anthropic.com

Description of processing

Provision of artificial intelligence model inference and related services used to generate responses based on input data.

Location of processing / transfer mechanism:

Primarily United States; transfers safeguarded by SCCs and contractual safeguards described in Anthropic's Trust Center and DPA.

3. Name: OpenAI, L.L.C.

Address:

3180 18th Street, San Francisco, California 94110, United States

Contact person's name, position and contact details:

OpenAI Privacy Team / Data Protection Officer

Email: privacy@openai.com

Description of processing:

Provision of artificial intelligence APIs and related services, including processing of prompts and outputs.

Location of processing / transfer mechanism:

United States and other approved locations; transfers protected by SCCs and supplementary safeguards as set out in OpenAI's DPA and Trust Center

4. Name: Google Cloud Platform (Google LLC)

Address:

1600 Amphitheatre Parkway, Mountain View, California 94043, United States

Contact person's name, position and contact details:

Google Data Protection Office

Email: privacy@google.com

Description of processing (including a clear delimitation of responsibilities):

Provision of cloud infrastructure, hosting, compute, storage, networking, logging, and security services supporting the Controller's platform.

Location of processing / transfer mechanism:

EU and United States; transfers governed by SCCs and Google Cloud DPA safeguards.

5. Name: Pinecone Systems, Inc.

Address:

548 Market Street, PMB 90169, San Francisco, California 94104, United States

Contact person's name, position and contact details:

Pinecone Privacy Team

Email: privacy@pinecone.io

Description of processing (including a clear delimitation of responsibilities):

Provision of managed vector database and similarity search services, including storage and retrieval of embeddings and associated metadata.

Location of processing / transfer mechanism:

EU and United States regions (as configured by Controller); transfers safeguarded by SCCs and contractual measures described in Pinecone's Trust Center.

6. Name: Actionable Science Labs Private Limited

Address:

F-14, Nehru Colony, D-1 Block, Dehradun-248001, Uttarakhand, India

Contact person’s name, position and contact details:

Udaya Bhaskar Reddy, Chief Technology Officer

Email: ub@rezolve.ai

Description of processing (including a clear delimitation of responsibilities):

Provision of technical support and configuration services to the data importer, including initial tenant configuration, troubleshooting, and ongoing support activities. Personnel may access personal data on a limited and ad hoc basis to investigate and resolve specific support or configuration issues. Processing is performed solely on the data importer's documented instructions for the purpose of delivering the contracted SaaS services.

Location of processing / transfer mechanism:

India; transfers safeguarded by Processor to Sub-Processor SCCs (Module 3) entered into between Actionable Science Inc and Actionable Science Labs Private Limited.