MODULE 1 CONTROLLER TO CONTROLLER

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of

[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 of 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.

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;

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

(iii) [*This clause is not applicable in this Module – left empty on purpose.*]

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Clause 7 – *Optional. This option is not used – left void on purpose.*

<u>**SECTION II– OBLIGATIONS OF THE PARTIES**</u>

Clause 8

Data protection safeguards

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

8.1 Purpose limitation

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

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

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

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

8.2 Transparency

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

  (i) of its identity and contact details;

  (ii) of the categories of personal data processed;

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

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

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

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

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

8.3 Accuracy and data minimisation

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

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

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

8.4 Storage limitation

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

8.5 Security of processing

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

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

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

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

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

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

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach. The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

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

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union[3] (in the same country as the data importer or in another third country,

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

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

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

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

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

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

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

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

8.8 Processing under the authority of the data importer

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

8.9 Documentation and compliance

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

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

Clause 9

Use of sub-processors

[Not applicable in this module – left void on purpose]

Clause 10

Data subject rights

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

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

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

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

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

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

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

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

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

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

[4] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

Clause 13

Supervision

(a) 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.

(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[5];

(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.

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements maybe 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.

Clause 15

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

15.1 Notification

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

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

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

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Member State where the data exporter "You" (as defined in that certain Subscription and License Agreement) is established. In the event that such law does not allow for third-party rights these clauses shall be governed by the laws of the Netherlands, where the data importer's ultimate parent company, Wolters Kluwer N.V., is based.

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of the Member State where the data exporter "You" (as defined in that certain Subscription and License Agreement) is established. In the event that these Clauses are governed by the laws of the Netherlands under Clause 17, then the Parties agree the competent court in Amsterdam, the Netherlands shall resolve any dispute arising under these Clauses.

(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.

APPENDIX

EXPLANATORY NOTE:

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s): Subscriber (as defined in that certain Ovid Technologies Master Subscription Agreement ("Master Subscription Agreement"))

Contact person's name, position and contact details: Data exporter can be contacted through the contact details mentioned in the notice provision of the Master Subscription Agreement.

Activities relevant to the data transferred under these Clauses: entering into the Master Subscription Agreement.

Signature and date: as set out in the Master Subscription Agreement.

Role: controller

Data importer(s):

Name: Ovid Technologies, Inc.

Address: 28 Liberty St., New York, New York, USA 10005

Contact person's name, position and contact details:

By email to support@ovid.com;; or

By telephone to: 1-800-343-0064 in the U.S. or via your local support number, which can be found at http://ovid.com/callsupport

Activities relevant to the data transferred under these Clauses: execution of the Master Subscription Agreement.

Signature and date: as set out in the Master Subscription Agreement.

Role (controller/processor): controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The data exporter is an enterprise customer and has subscribed to the Online Tools for use by its Authorized Users pursuant to a certain Master Subscription Agreement entered into by and between data exporter and data importer. The personal data transferred concerns employees, contractors, and affiliates of data exporter who are registered as Authorized Users of the Online

Tools in accordance with the Master Subscription Agreement. Capitalized terms used but not defined in this paragraph will have the same meanings as set forth in the Master Subscription Agreement

Categories of personal data transferred

IP address, name, email address, usernames, passwords, electronic activity, location and credit card data concerning data exporter's Authorized Users.

Specific categories of the above that are collected may vary per individual Authorized User, depending on how the Authorized User uses the Online Tools.

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.

Not applicable.

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

Continuous basis as necessary for the purposes of the transfer detailed below.

Nature of the processing

See the description of the purposes below

Purpose(s) of the data transfer and further processing

The transfer is made for the following purposes:

The data exporter will transfer personal data or the Authorized User will provide their personal data to the data importer which will then process the personal data for the following purposes:

(a) to make certain features of the Online Tools available to Subscriber and its Authorized Users,

(b) at an Authorize User's request, to disclose such information to accredited organizations to redeem such Authorizer User's accumulated continuing medical education credits,

(c) managing and making decisions about this Agreement and any matters (such as invoicing and fee arrangements) arising in connection with this Agreement;

(d) communicating with Subscriber and the Data Subjects that work for Licensee in relation to matters arising under or in connection with the Agreement and in connection with services that Ovid may offer from time to time;

(e) to ensure compliance with applicable conditions of use (as set forth in the Master Subscription Agreement), laws, and/or regulations,

(f) establishing, exercising and defending legal rights and claims;

(g) client relationship management purposes;

(h) to provide support for data exporter and its Authorized Users,

(i) risk management and quality reviews;

(j) to improve or modify the Online Tools and to create derivative or new products and services; marketing; advertising; sending reports to data exporter and its Authorized Users, or conducting research; and

(k) Ovid's internal financial accounting, information technology, system administration, and other administrative support services

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 is processed to the extent necessary for the performance of data importer’s obligations, and for the time necessary to achieve the purposes for which the personal data is collected, in accordance with the data importer’s data retention policies and the applicable data protection laws. When the data importer no longer needs personal information, the data importer takes all reasonable steps to remove it from its systems and records or take steps to properly anonymize it.

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

Service providers or processors who perform certain functions on data importer’s behalf, such as for managing or hosting services and/or underpinning technology for the Online Tools we are providing; to provide analytics and site usage information, process transactions and payments; provide outsourced help with the operations of the Online Tools, provide marketing and promotional assistance, and provide other services related to the operation of the data importer’s business.

Marketing partners and vendors to develop, deliver and report on targeted advertising of our services either online or in emails sent by the data importer, or data importer’s marketing partners to the data exporter

Affiliates of data importer who support the data importer’s products and services and with whom data importer shares certain back-office functions.

C. COMPETENT SUPERVISORY AUTHORITY

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

The competent supervisory authority is the supervisory authority of the EU Member State where the data exporter is established

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Wolters Kluwer N.V. ("Wolters Kluwer") Global Information Security Program

1. Security Program & Governance

1.1. Security Program. Wolters Kluwer (Ovid Technologies, Inc.'s ultimate parent) maintains a written global information security program of policies, procedures and controls aligned to NIST CSF, ISO27001, and other equivalent standards, governing the processing, storage, transmission and security of data (the "Security Program"). The Security Program mandates industry-standard practices designed to protect data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to data transmitted, stored or otherwise processed. Wolters Kluwer updates the Security Program to address (i) new and evolving security threats, (ii) changes to industry standards, (iii) technological advances in security tools, and (iv) amendments required following risk assessments undertaken pursuant to 1.3 below. Additionally, all security policies and standards governing the Security Program are reviewed, updated, and approved annually by the Wolters Kluwer Security Council ("Security Council"), which is comprised of executive representation from each of the Wolters Kluwer commercial divisions and corporate functions.

1.2. Security Organization. Wolters Kluwer has implemented a three-tiered information security management structure to facilitate the management, architecture, and operations of security functions. The Security Council oversees the management of this structure. Members of the Security Council include leadership representatives including commercial division CTOs, Legal, Internal Audit, Internal Controls, the Global Information Security team, and Risk Management. Wolters Kluwer has a Chief Information Security Officer who is responsible for oversight, management, and monitoring of Wolters Kluwer's Security Program.

1.3. Risk Assessments. Wolters Kluwer performs information security risk assessments as part of a risk governance program that is established with the objective to regularly assess and evaluate the effectiveness of the Security Program. Such assessments are designed to identify and assess potential risks impacting confidentiality, integrity, availability, and/or privacy of the information and data processed, stored or transmitted by the organization, resulting from any changes in the business or technology environments. The Wolters Kluwer Security Program is audited annually by an independent third-party in accordance with 2.2 below.

2. Certifications and Audits

2.1. Certifications and Standards. Wolters Kluwer has established and maintains sufficient controls to meet certification and attestation requirements for the objectives stated in ISO 27001, SOC 1 and SOC 2 Type 2 (or equivalent standards) for the Security Program.

2.2. Audits. At least once per calendar year, Wolters Kluwer obtains an assessment against the referred standards and audit methodologies by an independent third-party auditor. For select systems, applications and services, Wolters Kluwer annually receives third party audits for compliance with SOC 2 Type 2.

3. Physical and organizational measures

3.1. Facilities. Offices and data center facilities that are owned or leased by Wolters Kluwer include physical access restrictions and fire detection and fire suppression systems both localized and throughout the building. The implemented controls are commensurate with the risk exposure of each facility. Controls include access by authorized personnel only, visitor access controls, secure areas which are physically separated from other workspaces, and systems, machines and devices including physical protection mechanisms and entry controls to limit physical access.

3.2. Asset Management. Wolters Kluwer maintains an inventory of its assets used within Wolters Kluwer and by any third parties authorized to act on its behalf, and an inventory of all media and equipment where data is stored. An asset is anything that has value to Wolters Kluwer, which includes hardware, software, information, infrastructure, outsourced services and even resources with specific skills and knowledge ("Asset").

3.3. Personnel Security. Users who are given access to Assets must abide by the Wolters Kluwer Acceptable Use Policy. Wolters Kluwer performs background screening on employees and all contractors who have access to Wolters Kluwer information and customers' information, subject to applicable laws and regulations.

3.4. Endpoint Security. Wolters Kluwer implements and maintains security mechanisms on endpoints, including firewalls, automated locking of devices after a specified period of inactivity, updated anti-virus, an advanced endpoint detection and response (EDR) solution, and full disk encryption. Wolters Kluwer restricts personnel from disabling security mechanisms.

3.5. Training and Awareness. Wolters Kluwer maintains a security and privacy awareness program that includes both regularly scheduled and unannounced training and education of its personnel, including any contractors or other third parties working on its behalf with access to data or Assets. Such training is conducted at time of hire and at least annually. In addition, Wolters Kluwer offers role-based security training for critical roles such as application developers to enhance security awareness throughout the organization. Tabletop exercises are scheduled on at least an annual basis for all commercial divisions and involve a cross-functional team from across the organization.

3.6. Vendor Risk Management. Wolters Kluwer maintains a vendor risk management program that assesses all vendors that access, store, process, or transmit Wolters Kluwer information and customers' information for appropriate security and privacy controls and business disciplines. Before Wolters Kluwer provides a vendor with access to personal information or any other sensitive information of Wolters Kluwer employees or customers, or critical Assets, it is required that appropriate security controls are in place. Access by vendors is required to be limited to only the access required to provide the contracted-for services. Security controls are required to be implemented to ensure that vendor access is limited appropriately. Periodic reviews of vendors, including third-party security audits, may be used to confirm whether vendors are adhering to their obligations and maintaining appropriate security measures.

3.7. Laws and Regulations. Changes to the Security Program are undertaken in compliance with applicable laws and regulations.

4. Technical measures

4.1. Access and Authentication. Access to Assets by Wolters Kluwer employees and contractors is protected by authentication, authorization, and identity management mechanisms. User authentication is required to gain access to production and development environments. Individuals are assigned a unique user account. Sharing of individual user accounts is prohibited. Access privileges are based on job requirements using the principle of least privilege, are modified upon any applicable changes in job requirements, and are revoked upon termination of employment or contract. Infrastructure access is established using appropriate user account and authentication controls, which include the required use of VPN connections, complex passwords, enabling of account lock-out, and a multi-factor authenticated connection.

4.2. Separation of Duties. Wolters Kluwer implements and maintains a formal separation of duties, including those managed by third-parties or otherwise outsourced.

4.3. Separation of Environments. For Wolters Kluwer critical Assets, Wolters Kluwer deploys separate development, QA, and production environments. Wolters Kluwer does not use customer data in development and maintains controls to prevent such use.

4.4. Vulnerability Management. The Wolters Kluwer vulnerability management program is focused on the collection, analysis, summarization, tracking and reporting of identifiable vulnerabilities in applications, infrastructure, endpoint systems and networks. This process is vital for providing accurate visibility of risk across the organization. Monthly vulnerability scans are conducted, and third-party penetration tests are performed annually, which follow the remediation schedule in accordance with established vulnerability management standards.

4.5. Encryption. Wolter Kluwer uses industry standard encryption to encrypt data in transit over public networks to the Wolters Kluwer environment and data at rest for systems, applications and services that involve or impact sensitive data.

4.6. Encryption Management. Encryption keys are created and protected with at least the same level of security and access control as the data being protected. The encryption strength is based on industry standards for strong encryption and does commensurate with the data classification.

4.7. Firewall System. Industry standard firewalls are installed and managed to protect Wolters Kluwer systems by monitoring all entry connections routed to the Wolters Kluwer environment. Firewall rules are reviewed periodically.

4.8. Software Development. Wolters Kluwer implements and maintains secure application development policies and procedures aligned with industry standard practices such as the OWASP Top Ten (or a substantially equivalent standard). All personnel responsible for secure application design and development receive a minimum of 8 hours of related training per year regarding Wolters Kluwer's secure application development practices.

4.9. Endpoint Security. See Section 3.4, above.

4.10. Disposal of Information. Wolters Kluwer maintains procedures ensuring secure disposal of information. Secure disposal of data requires, at minimum, secure erasure of media and secure disposal of records so that the information cannot be read or reconstructed.

5. Business Continuity & Disaster recovery

5.1. Data Backup. Wolters Kluwer maintains a backup plan to ensure all critical data is backed up without affecting system operations. The type and frequency of backup and type of backup media used takes into consideration the volume of data, criticality of data and recovery time constraints.

5.2. Business Continuity. Wolters Kluwer maintains business continuity plans ("BCP") which include processes for protecting personnel and assets and restoring functionality in accordance with the time frames outlined therein. Such BCP is tested annually and updated based on any deficiencies identified during such tests.

5.3. Disaster Recovery. Wolters Kluwer (i) maintains an IT disaster recovery plan ("DR"); (ii) tests the DR plan at least once every year; (iii) makes available summary test results which will include the actual recovery point and recovery times; and (iv) documents any action plans within the summary test results to promptly address and resolve any deficiencies, concerns, or issues that prevented or may prevent the services from being recovered in accordance with the DR plan.

6. Security Operations Center

6.1. Incidents. Wolters Kluwer has a cross-functional global information security incident response team that provides 24/7, 365 days a year proactive security monitoring, management, and response, in accordance with Wolters Kluwer's established corporate incident management plan. Wolters Kluwer's security team will promptly analyze potential security incidents to assess the impact, determine if immediate risk exists, and take immediate action to mitigate such damage.

6.2. Notification. Wolters Kluwer provides notification of security incidents in accordance with applicable laws and regulations and contractual commitments.

6.3. Logging & Monitoring. Wolters Kluwer utilizes a Security Incident Event Monitoring (SIEM) tool which feeds event notification into the Security Operations Center. Events are reviewed, prioritized, and tracked to remediation according to the established service level agreements.