

CLEARY GOTTLIB

**Transfers of
Personal Data Outside
the UK/EEA**



This Restricted Transfer Addendum (“**RTA**”) is entered into by and between:

1. the Client (“**Client**” or “**you**”); and
2. Cleary Gottlieb Steen & Hamilton LLP, a New York limited liability partnership; Cleary Gottlieb Steen & Hamilton LLP, an English limited liability partnership; Cleary Gottlieb Steen & Hamilton Studio Legale, an Italian partnership; Cleary Gottlieb Steen & Hamilton Consultores em Direito Estrangeiro; and Cleary Gottlieb Steen & Hamilton (Hong Kong) (“**Cleary**”, “**we**” or “**us**”)

(each a “**Party**”, and together the “**Parties**”).

The parties agree as follows:

- A. This RTA supplements Cleary’s Terms and Conditions and Engagement Letters (together the “**Agreement**”) under which the Client instructs Cleary to provide it with services (the “**Services**”).
- B. It applies where there is one or more Restricted Transfers between the Parties and in such cases is intended by the Parties to comply with the International Transfer Requirements in respect of such Restricted Transfer(s).

1. Definitions and Interpretation

- 1.1. Unless otherwise defined in this RTA, words and expressions used in this RTA shall have the meanings given in the Agreement.
- 1.2. In this RTA the following words should have the following meanings:

“**Data Protection Laws**” means:

- a. the UK Data Protection Laws;
- b. 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 (the “**GDPR**”);
- c. all local laws or regulations of jurisdictions in the EEA implementing or supplementing the GDPR;
- d. codes of practice and guidance relating to Restricted Transfers that are issued by national supervisory authorities, regulators or institutions of competent jurisdictions relating to the laws and regulations referred to in (a)-(c),

in each case as amended, superseded or replaced from time to time;

“**EEA**” means the European Economic Area;

“**Effective Date**” means the date upon which the Parties entered into the Agreement (and in doing so, this RTA);

“**ICO**” means the Information Commissioner’s Office;

“**International Transfer Requirements**” means the requirements of Chapter V of the GDPR (Transfers of personal data to third countries or international organisations);

“**Restricted Country**” means a country, territory or jurisdiction which is not considered by the EU Commission (or in respect of personal data transfers caught by the requirements of UK Data Protection Laws, the relevant UK governmental or regulatory body as applicable) to offer an adequate level of protection in respect of the processing of personal data pursuant to Article 45(1) of the GDPR;

“**Restricted Transfer**” means a transfer of personal data to a Restricted Country which is subject to the International Transfer Requirements;

“**Standard Contractual Clauses**” or “**SCCs**” means the standard contractual clauses set out in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance) C/2021/3972 (as set out in Schedule 1 of this RTA);

“**UK**” means the United Kingdom of Great Britain and Northern Ireland;

“**UK Addendum**” means the International Data Transfer Addendum to the European Commission Standard Contractual Clauses issued by the ICO under or pursuant to section 119A(1) of the Data Protection Act 2018 (as may be amended by the ICO from time to time pursuant to its terms);

“**UK Data Protection Laws**” means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018; and

“**UK GDPR**” has the meaning given to it in the Data Protection Act 2018 (as amended from time to time).

- 1.3. References in this RTA to “controller”, “personal data”, “processor”, and “processing” shall have the same meaning as defined in the GDPR.
- 1.4. Unless the context otherwise requires, a reference to a “clause” is a reference to a clause of the main body of this RTA.
- 1.5. A reference to the GDPR and/or an Article or Chapter of the GDPR shall, where the context so requires and insofar as the Data Protection Law is that of the UK be construed as a reference to the UK GDPR and/or the equivalent Article or Chapter of the UK GDPR.

- 1.6. References to legislation (or specific provisions of legislation) mean that legislation (or specific provision) as amended from time to time.

2. Applicability and Effect of this RTA

- 2.1. This RTA will be deemed to have taken effect on the Effective Date and will remain in effect for the duration of the Agreement.
- 2.2. This RTA shall be deemed incorporated into, and to form a part of, the Agreement and shall amend and/or supersede any existing clauses or schedules relating to compliance with the International Transfer Requirements. Any provision of the Agreement that does not relate to compliance with the International Transfer Requirements shall be unaffected by this RTA and shall remain in full force and effect.
- 2.3. In the event of any conflict or inconsistency between the Agreement, the main body of the RTA and/or the SCCs, the provisions which provide the most protection to data subjects shall prevail. In the absence of any provision providing more protection to data subjects than any other provision, in the event of any conflict or inconsistency:
- a. between this RTA and the Agreement, this RTA shall prevail;
 - b. between the SCCs and the main body of this RTA, the SCCs shall prevail; and
 - c. Between the SCCs and the UK Addendum, the UK Addendum shall prevail, except where (for the purposes of the conflicting terms) the SCCs provide greater protection for data subjects, in which case the SCCs will override the UK Addendum.
- 2.4. For the avoidance of doubt, nothing in this RTA is intended to vary, modify or contradict the provisions of the SCCs – save for clause 4 (UK Interpretation of the SCCs).

3. International Transfer Requirements

- 3.1. The Agreement specifies each Party's status as a controller and/or a processor in respect of personal data that is processed under or in connection with the Agreement.
- 3.2. Subject to clause 4, where there is a Restricted Transfer, the Parties agree to rely on the Standard Contractual Clauses to comply with the International Transfer Requirements and, accordingly, to the extent that such transfer is:
- a. on a controller to controller basis, Module 1 in Schedule 1 will apply;
 - b. on a controller to processor basis, Module 2 in Schedule 1 will apply.
- 3.3. Each Party agrees that by entering into this RTA, the SCCs are incorporated into this RTA and deemed executed by each of the Parties acting on their own behalf and on behalf of their affiliates (where applicable) without the need for any further signature from either Party.

- 3.4. The SCCs shall cease to apply to the processing of personal data if and to the extent that the relevant transfer of the personal data ceases to be a Restricted Transfer.

4. UK Interpretation of SCCS

- 4.1. Where the UK GDPR applies to the data exporter's processing when making a Restricted Transfer, the SCCs shall be deemed to be amended (and/or insofar as possible will be interpreted) so that they operate to provide appropriate safeguards to the transfer(s) in accordance with Article 46 of the UK GDPR and shall be read mutatis mutandis as appropriate.
- 4.2. The Parties agree that this clause 4 incorporates the UK Addendum to the European Commission Standard Contractual Clauses issued by the ICO under or pursuant to section 119A(1) of the Data Protection Act 2018 and that, by entering into this RTA, the requirements of the UK Addendum are binding on the parties in accordance with Clause 1 of the UK Addendum. Pursuant to Clause 19 and Table 4 of the UK Addendum, the parties agree that both the data exporter and the data importer may end the UK Addendum as set out in Clause 19 of the UK Addendum.

5. Invalidity of the SCCS

- 5.1. If the SCCs relied upon by the Parties pursuant to clause 3.2 cease to exist or are no longer considered by either Party to be a lawful method of complying with the International Transfer Requirements for any reason, the data importer shall cease (and procure that any relevant third party ceases) all substantive processing of such personal data until such time as the Parties have entered into an alternative transfer mechanism and/or put in place such supplementary measures and/or safeguards to comply with the International Transfer Requirements.
- 5.2. Subject to clause 5.3, if the data exporter determines (acting reasonably) that it is not feasible to put in place such an alternative transfer mechanism and/or supplementary measures and/or safeguards to enable compliance with the International Transfer Requirements, the data exporter shall be entitled to require the data importer to:
- a. process (and/or procure that any relevant third party processes) the personal data within a jurisdiction which is not a Restricted Country; and/or
 - b. delete (or procure the deletion of) and/or destroy the personal data such that it is no longer processed in the relevant Restricted Country.
- 5.3. Where the data importer is unable to comply with clause 5.2 because of local laws applicable to the data importer that prohibit such compliance, the data importer warrants that it will continue to ensure compliance with this RTA and will only process the relevant personal data to the extent and for as long as required under that local law.

6. Rights and Remedies

- 6.1. The rights and remedies provided under this RTA are in addition to, and not exclusive of, any rights or remedies provided by law.

7. Liability

- 7.1. The exclusions and limitations of liability set out in (or that otherwise apply to) the Agreement, including in particular in clause 18 (Limitation of Liability), shall apply to this RTA.

8. Third Party Rights

- 8.1. Except as otherwise expressly stated in this RTA, this RTA does not confer any rights on any person or party (other than the Parties) under the Contracts (Rights of Third Parties) Act 1999 or otherwise.

9. Further Assurance

- 9.1. Each Party shall, at the request of the other Party, execute such additional documents and perform or procure the performance of such other acts or things that may reasonably be required by the other Party in order to give full effect to this RTA.

10. Entire Agreement

- 10.1. This RTA and the documents referred to or incorporated in it constitute the entire agreement between the Parties relating to the subject matter of this RTA and supersede and extinguish any prior drafts, agreements, undertakings, representations, warranties and arrangements of any nature whatever, whether or not in writing, between the Parties in relation to the subject matter of this RTA.

11. Severance

- 11.1. If any provision of this RTA is held to be invalid or unenforceable by any judicial or other competent authority, all other provisions of this RTA will remain in full force and effect and will not in any way be impaired.
- 11.2. If any provision of this RTA is held to be invalid or unenforceable but would be valid or enforceable if some part of the provision were deleted, or the period of the obligation reduced in time, or the range of activities or area covered reduced in scope, the provision in question will apply with the minimum modifications necessary to make it valid and enforceable.

12. Governing Law and Jurisdiction

- 12.1. This RTA and any dispute or claim arising out of or in connection with it or its subject matter, whether of a contractual or non-contractual nature, shall:
- a. where the GDPR applies to the data exporter's processing when making a Restricted Transfer, be governed by and construed in accordance with the laws of Belgium; and
 - b. where the UK GDPR applies to the data exporter's processing when making a Restricted Transfer, be governed by and construed in accordance with the laws of England and Wales.

12.2. The Parties irrevocably agree that:

- a. where clause 12.1(a) applies, the courts of Belgium shall have exclusive jurisdiction to settle any dispute which may arise out of or in connection with this RTA; and
- b. where clause 12.1(b) applies, the courts of England and Wales shall have exclusive jurisdiction to settle any dispute which may arise out of or in connection with this RTA,

provided in each case that a data subject whose personal data is subject to the GDPR (or as the case may be the UK GDPR) may also bring legal proceedings before the courts of the Member State in which that data subject has their habitual residence (or, as the case may be, the courts of England and Wales).

Execution

This RTA will be deemed to have been executed by the Parties on the Effective Date.

This RTA was last updated on 4 November 2022.

Schedule 1 (Standard Contractual Clauses)

Module 1

Controller to Controller

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) 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)I 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 - Clause 8.5 (e) and Clause 8.9(b);
 - iii. Clause 9 - N/A;
 - iv. Clause 12 - Clause 12(a) and (d);
 - v. Clause 13;
 - vi. Clause 15.1(c), (d) and (e);
 - vii. Clause 16(e);
 - viii. Clause 18 - Clause 18(a) and (b).
- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

- a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Purpose limitation

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

- i. where it has obtained the data subject's prior consent;
- ii. where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- iii. where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

- a. In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
 - i. of its identity and contact details;
 - ii. of the categories of personal data processed;
 - iii. of the right to obtain a copy of these Clauses;
 - iv. where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
- b. Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
- c. On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
- d. Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

- a. Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
- b. If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
- c. The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

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

8.5 Security of processing

- a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- b. The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- c. The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- d. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
- e. In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate

number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

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

8.6 Sensitive data

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

8.7 Onward transfers

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

- i. it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- iii. the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

- iv. it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- v. it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- vi. where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

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

8.9 Documentation and compliance

- a. Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
- b. The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

N/A

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. 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 11(c)(i);
 - ii. rectify inaccurate or incomplete data concerning the data subject;
 - iii. erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.
- c. Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
- d. The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:
 - i. inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
 - ii. implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.
- e. Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
- f. The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
- g. If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

- a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- 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;
 - iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
 - d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
 - e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
 - f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data

requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

- b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - ii. the data importer is in substantial or persistent breach of these Clauses; or
 - iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

- d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or

returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

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

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 Belgium.
- 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.

Schedule 1 (Standard Contractual Clauses)

Module 2

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) for the transfer of personal data to a third country.
- b. The Parties:
 - i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
 - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679,

provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

- a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
- i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - ii. Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);
 - iii. Clause 9 - Clause 9(a), (c), (d) and (e);
 - iv. Clause 12 - Clause 12(a), (d) and (f);
 - v. Clause 13;
 - vi. Clause 15.1(c), (d) and (e);
 - vii. Clause 16(e);
 - viii. Clause 18 - Clause 18(a) and (b).
- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

- a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 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 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 organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- 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 (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 authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) working 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. 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 authorised 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 organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

- 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 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;
 - iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request)

indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

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

Clause 15

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

15.1 Notification

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

- d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

- i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
- ii. the data importer is in substantial or persistent breach of these Clauses; or
- iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

- d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

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

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 Belgium.

- 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 Annex I

A. List of Parties

Data exporter(s):

- Name:** The Client, as set out in the Agreement.

Address: The address of the Client as set out in the Agreement.

Contact person's name, position and contact details: The person responsible for instructing Cleary in relation to the Services, as set out in the Agreement or the Engagement Letter

Activities relevant to the data transferred under these Clauses: Recipient of Services under the Agreement.

Signature and date: This Annex is deemed completed as of the Effective Date.

Role (controller/processor): Controller

Data importer(s):

- Name:** Cleary Gottlieb Steen & Hamilton LLP, a New York limited liability partnership

Address: One Liberty Plaza, New York, NY 10006, United States of America

Contact person's name, position and contact details: Sonya Foulds, Chief Risk Officer (email: sfoulds@cgsh.com)

Activities relevant to the data transferred under these Clauses: the provision of Services to Client under the Agreement.

Signature and date: This Annex is deemed completed as of the Effective Date.

Role (controller/processor): Cleary is primarily a data controller in terms of the provision of its Services, however it is acknowledged that it may at times be a data processor depending on the particulars of the service in question.
- Name:** Cleary Gottlieb Steen & Hamilton LLP, an English limited liability partnership

Address: 2 London Wall Place, London EC2Y 5AU, England

Contact person's name, position and contact details: Sonya Foulds, Chief Risk Officer (email: sfoulds@cgsh.com)

Activities relevant to the data transferred under these Clauses: the provision of Services to Client under the Agreement.

Signature and date: This Annex is deemed completed as of the Effective Date.

Role (controller/processor): Cleary is primarily a data controller in terms of the provision of its

Services, however it is acknowledged that it may at times be a data processor depending on the particulars of the service in question.

4. **Name:** Cleary Gottlieb Steen & Hamilton Studio Legale, an Italian partnership

Address: Via San Paolo 7 20121 Milan, Italy
Piazza di Spagna 15 00187 Rome, Italy

Contact person's name, position and contact details: Sonya Foulds, Chief Risk Officer (email: sfoulds@cgsh.com)

Activities relevant to the data transferred under these Clauses: the provision of Services to Client under the Agreement.

Signature and date: This Annex is deemed completed as of the Effective Date.

Role (controller/processor): Cleary is primarily a data controller in terms of the provision of its Services, however it is acknowledged that it may at times be a data processor depending on the particulars of the service in question.

5. **Name:** Cleary Gottlieb Steen & Hamilton Consultores em Direito Estrangeiro

Address: Rua Professor Atilio Innocenti, 165, 14th Floor
São Paulo, SO 04538-000, Brazil

Contact person's name, position and contact details: Sonya Foulds, Chief Risk Officer (email: sfoulds@cgsh.com)

Activities relevant to the data transferred under these Clauses: the provision of Services to Client under the Agreement.

Signature and date: This Annex is deemed completed as of the Effective Date.

Role (controller/processor): Cleary is primarily a data controller in terms of the provision of its Services, however it is acknowledged that it may at times be a data processor depending on the particulars of the service in question.

6. **Name:** Cleary Gottlieb Steen & Hamilton (Hong Kong)

Address: Hysan Place, 37th Floor
500 Hennessy Road Causeway Bay Hong Kong

Contact person's name, position and contact details: Sonya Foulds, Chief Risk Officer (email: sfoulds@cgsh.com)

Activities relevant to the data transferred under these Clauses: the provision of Services to Client under the Agreement.

Signature and date: This Annex is deemed completed as of the Effective Date.

Role (controller/processor): Cleary is primarily a data controller in terms of the provision of its Services, however it is acknowledged that it may at times be a data processor depending on the particulars of the service in question.

B. Description of Transfer

Categories of data subjects whose personal data is transferred

- Client (if an individual) and personnel of Client;
- Parties to disputes, litigations, arbitration, transactions, negotiations or other legal matters involving Client, including personnel of those parties;
- Personnel of Client's partners, advisors and other entities with whom it has a relationship, so far as those personnel are relevant to or involved with the Services provided by the data importer.

Categories of personal data transferred

These vary depending on the nature of the Services but may include:

- Name and title (such as position, seniority, department and description of responsibilities/duties);
- Contact information (such as address, email address, fax number and phone number);
- Client communications;
- Client preferences (such as mailing lists signed up to for marketing and events);
- Client matter information and instructions;
- "Know your client" information (such as passport details and other identifying documents);
- Other information such as billing information and details of paid invoices, signatures, evidential documents supplied by Client in the course of the Services, tax identifier or VAT number);
- Data included in emails and files (including electronic files) sent from and received with corporate email;
- Technical information (such as username and passwords, IP address, domain, browser type, operating system, click-stream data and system logs); and
- Other information provided by or obtained on behalf of Client as part of the Services.

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.

- Information regarding criminal offences;
- Health or medical information; and

— Other special category data provided by or obtained on behalf of Clients as part of the Services.

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

Continuous for the duration of the Services.

Nature of the processing

The provision of the Services to Client as per the Agreement.

Purpose(s) of the data transfer and further processing

The provision of the Services to Client as per 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

The data importer will retain data processed as part of Client matters for the duration of the matter, plus a further period for legal purposes (normally six years from matter closure or the date of the last invoice sent to Client)

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

The provision of the Services to Client as per the Agreement, on a continuous basis for the duration of the Services.

C. Competent Supervisory Authority

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

For UK data exporters, the ICO.

Where there is a sole EU data exporter, the appropriate Supervisory Authority.

Where there are multiple EU data exporters, the Belgian Data Protection Authority.

Annex II - Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data

Please email dataprivacy@cgsh.com for details of the data importer's technical and organisational measures to ensure the security of the data.

Annex III – List of Sub-Processors

Please email dataprivacy@cgsh.com for a list of the sub-processors the data importer uses to process the data.



clearygottlieb.com

© Cleary Gottlieb Steen & Hamilton LLP, 2022. All rights reserved.

This memorandum was prepared as a service to clients and other friends of Cleary Gottlieb to report on recent developments that may be of interest to them. The information in it is therefore general, and should not be considered or relied on as legal advice. Throughout this memorandum, "Cleary Gottlieb" and the "firm" refer to Cleary Gottlieb Steen & Hamilton LLP and its affiliated entities in certain jurisdictions, and the term "offices" includes offices of those affiliated entities.