SHL's Pre-Signed European Standard Contractual Clauses

SECTION I

Clause 1
Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that theydo 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 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c)
and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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.

---

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

Clause 5
Hierarchy

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

Clause 6
Description of the transfer(s)

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

Clause 7 – Optional
Docking clause

(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 the 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 dueaccount 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 forattributing the personal data to a specific data subject shall, where possible, remain under the exclusive controlof 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[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 **Documentation and compliance**

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

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-

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

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) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects[3]. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been 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. The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[4] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph(a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

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

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

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place

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

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

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

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

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental

rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
   (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved, and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
   (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[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). [For Module Three: The data exporter shall forward the notification to the controller.]

(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 [for Module Three:, if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] 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 processingof 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.

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(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 arequest, 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 [for Module Three: and the controller] 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 deletionof 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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

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 Netherlands with the dispute to be heard in English.
(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.

ANNEX I

A. **LIST OF PARTIES**

Data exporter(s):

1. Name (Insert the name of company signing the Order Form):
Address (Insert registered address as per the Order Form):
Contact person's name, position and contact details:
Activities relevant to the data transferred under these Clauses: Data Exporters being supplied with the Data Importer's online assessment products

Signature and date: .....
Role: Controller

Data importer(s):

1. Name: **SHL US LLC**
Address: 111 Washington Avenue South, Suite 500, Minneapolis, MN 55401 USA
Contact person's name, position and contact details: Emmy Hackett, Global Data Protection Officer & General Counsel, dpo@shl.com
Activities relevant to the data transferred under these Clauses: Maintenance and support of Data importer's online assessment platforms

Signature and date: DocuSigned by: Emmy Hackett F824F46BEA71411... 23 April 2023
Role: processor

2. Name: **SHL (India) Private Limited**
Address: 9th Floor, Tower 10-B, DLF Cyber City, Phase-II, Gurgaon 122 002, India
Contact person's name, position and contact details: Emmy Hackett, Global Data Protection Officer & General Counsel, dpo@shl.com
Activities relevant to the data transferred under these Clauses: Maintenance and support of SHL's online assessment platforms

Signature and date: DocuSigned by: Emmy Hackett F824F46BEA71411... 23 April 2023
Role: processor

3. Name: **SHL Saville & Holdsworth (Proprietary) Limited**
Address: Ground Floor, Block D, Southdowns Office Park, CNR of John Voster Road and Karee Road, Iren Ext 54, Centurion 0157, South Africa
Contact person's name, position and contact details: Emmy Hackett, Global Data Protection Officer & General Counsel, dpo@shl.com
Activities relevant to the data transferred under these Clauses: Maintenance and support of SHL's online assessment platforms

Signature and date: DocuSigned by: Emmy Hackett F824F46BEA71411... 23 April 2023
Role: processor

4. Name: **SHL Group Limited**
Address: The Pavilion, 1 Atwell Place, Thames Ditton, Surrey, KT7 0NE, United Kingdom.
Contact person's name, position and contact details: Emmy Hackett, Global Data Protection Officer & General Counsel, dpo@shl.com
Activities relevant to the data transferred under these Clauses: Maintenance and support of SHL's online assessment platforms

Signature and date: DocuSigned by: Emmy Hackett F824F46BEA71411... 23 April 2023
Role: processor

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred
Data exporter's employees and prospective employees.

Categories of personal data transferred

Name, Email Address, Gender, Language, Data Exporter ID, employee demographic information, responses to assessments or survey, audio recordings, visual images and any other data requested by the Data Exporter.

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

Nature of the processing

For the purpose of SHL to provide SHL talent assessment products and services to Data exporter

Purpose(s) of the data transfer and further processing

SHL affiliates to provide support and maintenance to the SHL online assessment platforms

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 will be deleted or returned at the request of and as instructed by Data Exporter

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

For the purposes described in Annex III.

C. **COMPETENT SUPERVISORY AUTHORITY MODULE**

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

Where Company is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Company with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

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

Where Company is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office shall act as competent supervisory authority.

Where Company is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

ANNEX II

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

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

Data importer operates under the principles of data minimisation, processing only those categories of personal information required for the delivery of its products and services.

All data is encrypted by Data importer to industry leading standards when at rest (256-bit AES) and in transit (TLS 1.2). Data utilised in major third party suppliers such as AWS (for hosting) and Microsoft (email and productivity) is encrypted with keys maintained by Data importer so as to render the data inaccessible to the third party.

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

Data importer proactively manages, maintains, and measures the confidentiality, integrity, and availability of all systems and services used in the processing of data through ISO-accredited management systems.

Data importer's integrated management system (IMS) incorporates information security (ISMS), data protection (PIMS), and business continuity (BCMS) to provide effective protection of data and assurance to its clients and stakeholders. Data importer holds ISO accreditations in these three key areas, meaning they are subject to regular internal and external assessment for suitability, discovery and management of risks, and continuous improvement.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Data importer operates a business continuity and disaster recovery plan which is subject to ongoing testing and verification to ensure its suitability. The use of multiple data hosting sites in geographically disparate locations provides effective disaster recovery and service continuity in the event of an incident or outage.

Data importer systems run weekly full backups with incremental daily backups which are encrypted and then transferred securely within the relevant AWS region. Backups are stored for 45 days before being deleted from S3 buckets.

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

As part of its ISO-accredited integrated management system, Data importer conducts an internal audit programme to measure the effectiveness of its policies, procedures, and controls. Re-certification against ISO standards and other assurance initiatives provides external verification of the effectiveness of the IMS.

Regular vulnerability testing is conducted across all internal systems and externally-facing platforms to identify weaknesses and opportunities for improvement. This is supported by assessment against the OWASP Top Ten security risks, and annual external penetration testing of systems and web applications by a CREST-accredited supplier.

Measures for user identification and authorisation

All Data importer employees are assigned unique user IDs and login credentials to ensure proper identification and accountability of all users. Access is provisioned on the basis of least privilege and role-based access control, validated by monthly review and audit of user system access lists.

Authorisation of access to Data importer systems is provided through multi-factor authentication and single sign-on services. Data importer utilises Zscaler Private Access to provide secure zero trust access to users of its applications.

Measures for the protection of data during transmission

Data importer utilises TLS 1.2 for email services to provide encryption of data in transit. The transfer of any files containing personal inforamtion is facilitated through approved secure link services, password protection, and/or the encryption of data files to 256-bit AES.

Measures for the protection of data during storage

Data at rest is subject to 256-bit AES encryption, utilising keys operated entirely by Data importer to ensure no third-party access to data.

Stored data is provisioned to staff utilising role-based access control, with full system and OS logs to verify and hold accountable users to their actions.

All Data importer endpoints are subject to full-desk encryption, utilise host-based intrusion prevention systems, and prevent the use of physical storage media by default.

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

Data importer monitors access to its facilities using Closed-Circuit Television (CCTV) cameras, security personnel, automated access control systems (e.g. badge-activated door locks), and other available control mechanisms dependent on site. All employees and approved third party individuals are issued ID/security badges in order to gain entry to Data importer facilities, which dependent on role provide access to specific areas within a locale.

AWS and other third party suppliers processing personal data are required to provide contractual agreement to and evidence of similar physical levels of protection provided by security controls and logging of access.

Measures for ensuring events logging

Data importer utilises Rapid7's InsightIDR for for incident detection and response, authentication monitoring, and endpoint visibility. InsightIDR is a Software as a Service (SaaS) tool that collects data from existing network security tools, authentication logs, and endpoint devices, aggregating the data at an on-premises centralised Collector.

Logs are stored for all systems through InsightIDR for a period of 12 months from the point of collection.

Measures for ensuring system configuration, including default configuration

Through the use of centralised tools (InTune and ManageEngine), Data importer is able to implement and enforce the use of default configurations for end points. This includes the restriction of software to named and managed assets, web filtering, and ensuring the use of security tools.

Updates and patching are managed through these systems to provide protection against vulnerabilities. The logging and monitoring of end points, along with the visibility of installed software packages and versions, ensures the consistent use of secure system configurations across the Data importer userbase.

Measures for internal IT and IT security governance and management

Data importer's integrated management system provides visibility and control of business practices relating to information technology, information security, business continuity, and data protection. This is achieved through comprehensive use of compliance documentation, audit, risk management and treatment, improvement identification and tracking, and externally-assessed accreditations.

Further governance is achieved through quarterly management review meetings by the Compliance Board to ensure that the integrated management system remains suitable, adequate and effective, and meets the requirements of the organisation. The Compliance Board consists of leaders across the organisation, including the group managing director, and heads of IT, legal, and HR.

Measures for certification/assurance of processes and products

To provide validation and assurance of the security of Data importer's products and services, the organisation holds a number of external certifications in the areas of information security and data protection.

These include:

ISO 20000 – Service Management System
ISO 22301 – Business Continuity Management System
ISO 27001 – Information Security Management System
ISO 27701 – Privacy Information Management
ISO 27018 – Protection of personally identifiable information (PII) in public clouds acting as PII processor
Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) Security Programme
Cyber Security Essentials Plus

All AWS regions utilised for data hosting are both ISO 27001 and SSAE 16/SOC 2 Type II certified.

Measures for ensuring data minimisation

Data importer's products and services follow the principles of privacy-by-default and -by-design throughout their development and use lifecycles. A key part of this is ensuring only those categories of personal information are processed as required to ensure the provision of products and services.

Data importer ensures it understands and utilises only those data categories that are essential for purpose through the use of internal assessments such as PIAs and DPIAs across project lifecycles, and a pod system which sees a member of the information security team embedded in all projects from conception to delivery.

As Data importer acts as a data processor for its clients, it advises controllers and works with them closely during onboarding to ensure that data minimisation is configured and enforced throughout the use of its systems.

Measures for ensuring data quality
Measures for ensuring limited data retention

Data importer operates and measures through audits against its Data Retention Policy to ensure that personal data is deleted or anonymised at the end of its lifecycle or retention period.

Where Data importer is operating as a data controller, it works with clients to establish and implement appropriate retention periods for personal data across projects and categories of personal information.

Measures for ensuring accountability

Through the use of staff awareness education and compliance training, Data importer ensures that its employees understand their responsibilities around information security and data protection, and accountability for their actions.

This is underpinned through the use of role-based access controls, confidentiality agreements, staff disciplinary processes, and full system logs.

Measures for allowing data portability and ensuring erasure

Formal processes for data deletions and subject access requests are documented and shared with clients in order to facilitate the delivery of data subjects' rights. These are managed and tracked through a formal ticketing system with approvals, to ensure accurate and timely delivery
For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III

LIST OF SUB-PROCESSORS

Most current list of subprocessors can be found at the following link: https://www.shl.com/en/documents/security-compliance/platforms-sub-processors/. Data exporter can subscribe for updates using the 'Subscribe Now' feature.
The controller has authorised the use of the following sub-processors:

CRM – Salesforce – Store of marketing contacts and technical support cases

1. **Name: SALESFORCE.COM, INC.**
   Address: 415 Mission Street 3rd Floor San Francisco, CA 94105 United States
   Contact person's name, position and contact details: contact via dpo@shl.com .
   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):
   Store of marketing contacts and technical support cases

Email – Microsoft Office 365 – Emails to and from SHL (doesn't include emails from SHL Online Applications)

2. **Name: Microsoft Corp**
   Address: 1 Microsoft Way Redmond, WA 98052 United States
   Contact person's name, position and contact details: contact via dpo@shl.com .
   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):
   Emails to and from SHL as well as Office 365 system

Customer Contact Centre – Voice – New Voice Media – Phone system used for SHL Customer Support Center

3. **Name: Vonage Business Limited**
   Address: 25 Canada Square Level 37, London, England E14 5LQ
   Contact person's name, position and contact details: contact via dpo@shl.com .
   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):
   Phone system used for SHL Customer Support Center

CSAT Tool – Qualtrics – Customer satisfaction survey data.

4. **Name: Qualtrics LLC**
   Address: 333 West River Park Drive Provo, UT 84604 United States
   Contact person's name, position and contact details: contact via dpo@shl.com .
   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):
   Customer satisfaction survey data.

Marketing tool – Eloqua - Sending marketing emails to contacts who have requested information

5. **Name: Eloqua Corporation (doing business as Oracle Marketing Cloud**
   Address: 1921 Gallows Rd Ste 250 Vienna, VA, 22182-3994, United States
   Contact person's name, position and contact details: contact via dpo@shl.com .
   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):
   Sending marketing emails to contacts who have requested information

Hosting – AWS – Hosting of SHL systems

6. **Name: Amazon Web Services, Inc**
   Address: 10 Terry Avenue North, Seattle, WA 98109-5210
   Contact person's name, position and contact details: contact via dpo@shl.com .
   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):
   Hosting of SHL systems. SHL holds the encryption keys, not AWS

ADDITIONAL SUB-PROCESSORS DEPENDENT ON THE SHL PRODUCTS AND SERVICES PURCHASED

7. **Name: ZOOM VIDEO COMMUNICATIONS, INC -** If video conferencing tools purchased. For example, SmartMeet or VADC purchases. Alternative platform for video interviews.
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Access to the EU server for the purposes of providing online maintenance and support.
Data Storage location: APAC Server - Australia CN Server - China EU Server - Netherlands US Server - USA
Categories of Personal Information: Name, Email Address , audio recordings and visual images

8. **Jio Haptik Technologies Limited** – If Customer/Candidate Chatbot used
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Access to the EU server for the purposes of providing online maintenance and support.
Data Storage location: Singapore
Categories of Personal Information: Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Technical support - Name, Email Address, Country of residence, preferred language, telephone number, account log in details, browser types, operating systems, IP addresses and Date / time stamps. Chatbot transcripts

9. **Nylas, Inc.** - If Calendar Scheduling integration tool use
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Access to the EU server for the purposes of providing online maintenance and support.
Data Storage location: EU (SHL EU Server customers), US (SHL US Server Customers)
Categories of Personal Information: Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Name, email address and where calendar sync turned on by user all calendar details including any shared calendars

ANNEX IV

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

UK Addendum to the EU Commission Standard Contractual Clauses

Date of this Addendum:

1. The Clauses are dated as of the same date as the Addendum.

Background:

2. The Information Commissioner considers this Addendum provides appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors. This Addendum forms part of and supplements the Clauses to which it is attached. If personal data originating in the United Kingdom is transferred by data exporter to data importer in a country that has not been found to provide an adequate level of protection under UK Data Protection Laws, the Parties agree that the transfer shall be governed by the Clauses as supplemented by this Addendum.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Annex those terms shall have the same meaning as in the Annex. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Clauses
The Annex	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021
UK Data Protection Laws	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.
UK GDPR	The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
UK	The United Kingdom of Great Britain and Northern Ireland

4. This Addendum shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 UK GDPR.

5. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.

6. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

7. In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

Incorporation of the Clauses

8. This Addendum incorporates the Clauses which are deemed to be amended to the extent necessary so they operate:

    a. for transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that transfer; and

    b. to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.

9. The amendments required by Section 8 above, include (without limitation):

    a. References to the "Clauses" means this Addendum as it incorporates the Clauses

    b. Clause 6 Description of the transfer(s) is replaced with:

    "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer."

    c. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.

    d. References to Regulation (EU) 2018/1725 are removed.

    e. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK"

    f. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner;

    g. Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".

    h. Clause 18 is replaced to state:

    "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."

ANNEX V – Data Transfer Impact Assessment Questionnaire

1. What countries will Data importer Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom be stored in or accessed from? If this varies by region, please specify each country for each region.
    a. **Answer:** United States, South Africa and India.
    b. **Purposes of such transfer?** Support and maintenance to Data importer's online systems.
    c. **By which entities?** Data Importers as listed in the Standard Contractual Clauses.
2. What are the categories of data subjects whose Candidate Personal Data will be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?
    a. **Answer:** Data exporter's current and/or prospective employees
3. What are the categories of Candidate Personal Data transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?
    a. **Answer:** Candidate Personal Data that is processed includes Name, Email Address, Gender, Language, Data Exporter ID, employee demographic information, responses to assessments or survey, audio recordings, visual images and any other data requested by the Data Exporter.
4. Will any Candidate 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 be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom? If so, are there any 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?

   a. **Answer:** No, not applicable.

5. What business sector is SHL involved in?
   a. **Answer:** Technology, assessment products (Software as a Service)
6. Broadly speaking, what are the services to be provided and the corresponding purposes for which Candidate Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?
   a. **Answer:** Candidate Personal Data may be accessible from staff within the United States, India, South Africa to provide support and maintenance of the SHL online assessment systems.
7. What is the frequency of the transfer of Candidate Personal Data outside of the European Economic Area, Switzerland, and/or the United Kingdom? E.g., is Candidate Personal Data transferred on a one-off or continuous basis?
   a. **Answer:** Continuous as required to provide support and maintenance to the SHL online assessment platforms. Customer data is logically segregated by unique client ID.
8. When Candidate Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom to SHL, how is it transmitted to SHL? Is the Candidate Personal Data in plain text, pseudonymized, and/or encrypted?
   a. **Answer:** Data importer utilises TLS 1.2 for email services to provide encryption of data in transit. The transfer of any files containing personal information is facilitated through approved secure link services, password protection, and/or the encryption of data files to 256-bit AES.
9. What is the period for which the Candidate Personal Data will be retained, or, if that is not possible, the criteria used to determine that period?
   a. **Answer:** SHL will retain Candidate Personal Data in accordance with the contractual agreement between the parties.
10. Please list the Subprocessors that will have access to Candidate Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom:
   a. **Answer:** See list of authorised Subprocessors within the SCCs above
11. Is SHL subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where Candidate Personal Data is stored or accessed from that would interfere with SHL fulfilling its obligations under the attached Standard Contractual Clauses? For example, FISA 702 or U.S. Executive Order 12333. If yes, please list these laws.
   a. **Answer:** As 02nd December 2021, no court has found SHL to be eligible to receive process issued under the laws contemplated by Question 11, including FISA Section 702 and no such court action is pending.
12. Has SHL ever received a request from public authorities for information pursuant to the laws contemplated by Question 11 above (if any)? If yes, please explain.
   a. **Answer:** As 02nd December 2021, SHL has not received any national security orders of the type described in Paragraphs 150-202 of the judgment in the CJEU Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, nor is SHL aware of any such orders in progress.
13. Has SHL ever received a request from public authorities for Candidate Personal Data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain.
   a. **Answer:** No, not as 02nd December 2021,
14. What safeguards will SHL apply during transmission and to the processing of Candidate Personal Data in countries outside of the European Economic Area, Switzerland, and/or the United Kingdom that have not been found to provide an adequate level of protection under applicable Data Protection Laws?
15. **Answer:** Those safeguards set forth in the SCCs (including Annex II to the Standard Contractual Clauses).