Terms and Conditions to comply with the General Data Protection Regulation (GDPR) and UK-GDPR

These terms and conditions shall automatically become an essential part of any contractual arrangement or agreement ("Subscription Agreement") that is concluded between GLMX (in the following "Provider", "Our"), as specified in the imprint of this or on GLMX`s website and/or in the Subscription Agreement, and your company (in the following "Subscriber", "Client") as specified in the Subscription Agreement, or in case the Subscription Agreement is concluded by implicit acts or otherwise, the natural or legal person, agency or other body that is our contractual partner, but only in case processing of personal data is part of or essential to the Subscription Agreement and if data subjects that are subject to processing are based in the EU, EEA or UK or otherwise protected under GDPR or UK-GDPR. Based on the individual business relationship between Subscribers/Clients and GLMX, (1) Exhibit D: "EU Standard Contractual Clauses," and/or (2) Exhibit E: "UK SCCs ADDENDUM" will automatically apply.

EXHIBIT D

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 they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3 ***Third-party beneficiaries***

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

(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 the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and 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[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;

[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.

(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 noncompliance. 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 subprocessors at least five (5) business 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.

(aa) If the data exporter objects to such change, the data exporter may, as its sole and exclusive remedy, terminate the portion of any Agreement relating to the Services that cannot be reasonably provided without the new sub-processor that it objects to by providing 30 days' written notice to the data importer.[3]

(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.[4] 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 subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect

[3] Clause 9 (aa), which does not contradict, directly or indirectly, these Clauses, and which does not prejudice the fundamental rights or freedoms of data subjects, has been added in accordance with clause 2 (a) of these Clauses.

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

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 subprocessor 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) 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).

(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

[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.

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 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 Ireland.

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, these Clauses shall be governed by the law of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 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 Ireland.[6]

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(1) of Regulation (EU) 2016/679, these Clauses shall be governed by the law 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. 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 Ireland.[7]

Where these Clauses are used to comply with article 28 of the UK GDPR, these Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established.[8]

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 Ireland.

(bb) Where these Clauses are used to comply with article 28 of the UK GDPR, any dispute arising from these Clauses shall be resolved by the courts of the country of the United Kingdom in which the data exporter is established.[9]

(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.

[6] This second paragraph of clause 17, which does not contradict, directly or indirectly, these Clauses, and which does not prejudice the fundamental rights or freedoms of data subjects, has been added in accordance with clause 2 (a) of these Clauses.

[7] This third paragraph of clause 17, which does not contradict, directly or indirectly, these Clauses, and which does not prejudice the fundamental rights or freedoms of data subjects, has been added in accordance with clause 2 (a) of these Clauses.

[8] This fourth paragraph of clause 17, which does not contradict, directly or indirectly, these Clauses, and which does not prejudice the fundamental rights or freedoms of data subjects, has been added in accordance with clause 2 (a) of these Clauses.

[9] This clause 18 (bb), which does not contradict, directly or indirectly, these Clauses, and which does not prejudice the fundamental rights or freedoms of data subjects, has been added in accordance with clause 2 (a) of these Clauses.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: Subscriber

Address: is indicated in the preamble of the Agreement.

Contact person's name, position and contact details: are indicated in clause 13.2 of the Agreement.

[*Please include, where applicable, the contact details of the data protection officer and/or representative in the European Union]*

Activities relevant to the data transferred under these Clauses: processing of Subscriber Personal Data by the data importer on behalf of the data exporter in the context of the provision of the Services.

Signature and date: indicated and signed on the signature page of the Agreement.

Role: controller.

2. [*Please provide the identity and contact details of the Subscriber Group entities and, where applicable, of its/their data protection officer and/or representative in the European Union (or at least indicate where such information can be found)*]

Data importer:

1. Name: GLMX

Address: is indicated in the preamble of the Agreement.

Contact person's name, position and contact details: General Counsel; email: legal@glmx.com; phone: (001) 646-948-6704.

Activities relevant to the data transferred under these Clauses: processing of Subscriber Personal Data by the data importer on behalf of the data exporter in the context of the provision of the Services.

Signature and date: indicated and signed on the signature page of the Agreement.

Role: processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Named Users and any other data subjects whose personal data are processed by the data importer as Subscriber Group Personal Data.

Categories of personal data transferred

Contact information of Named Users and any other Subscriber Group Personal Data that are processed by the data importer.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

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

The Subscriber Group Personal Data are transferred to and processed by GLMX with the frequency that is required for the provision of the Services.

Nature of the processing

The provision of the Services, as described in detail in the Agreement.

Purpose(s) of the data transfer and further processing

The provision of the Services, as described in detail in 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 Subscriber Group Personal Data will be retained for as long as required for the provision of the Services.

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

The Subscriber Group Personal Data will only be transferred to sub-processors of the data importer if and insofar as required for the provision of the Services.

C. COMPETENT SUPERVISORY AUTHORITY

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

_____

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

General. The following terms are hereby incorporated into the Agreement and set forth the security requirements for the Services. Capitalized terms used but not defined herein will have the meanings assigned in the Agreement.

1. Unauthorized Disclosure. In the event that GLMX identifies or suspects any unauthorized disclosure of Subscriber's Confidential Information ("**Security Breach**") and unless requested by law enforcement not to do so, GLMX agrees to notify Subscriber in writing within 72 hours of discovery, and in accordance with all laws. GLMX will reasonably assist Subscriber in remediating or mitigating any potential damage, GLMX will issue a report that describes: a) the date of the Security Breach; b) a description of the disclosures involved in the Security Breach; and, c) the steps GLMX has taken to investigate the Security Breach, and to mitigate potential harm. GLMX shall allow Subscriber to perform an IT security review, at Subscriber's expense, upon thirty (30) days prior written notice after notice of a Security Breach.

2. Background Check Requirements. GLMX shall conduct background checks on its employees or contractors who will provide Services under this Agreement in accordance with GLMX's policies.

3. Subcontractors. In the event an affiliate or subcontractor of GLMX is provided access to, develops, or uses Subscriber's Confidential Information, GLMX's agreement with such subcontractor will include provisions equivalent to those in this Agreement with respect to the protection of Confidential Information. GLMX shall be responsible for the acts of its affiliates and subcontractors to the same extent, as if the acts were performed by GLMX. GLMX shall maintain a vendor management program to ensure the requirements of this paragraph.

4. Security Program, Program Requirements & Program Adjustments.

4.1 Security Program. GLMX shall maintain a comprehensive, written information security program ("**Security Program**"), that contains administrative, technical, and physical safeguards that are appropriate to: (i) GLMX's size, scope and type of business; (ii) the amount of resources available to GLMX; (iii) the type of information that GLMX will store or access, (iv) the service provided to Subscriber; and, (v) the need for security and confidentiality of such information.

4.2. Program Requirements.

(a) Program Design. GLMX's represents and warrants that its security program is designed to: (i) protect the confidentiality, integrity, and availability of Confidential Information in GLMX's possession, control and/or to which GLMX has access; (ii) protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Confidential Information; (iii) protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Confidential Information; (iv) protect against accidental loss or destruction of, or damage to, Confidential Information; and, (v) safeguard information as set forth in any local, state or federal regulations by which GLMX may be regulated.

(b) Security Incident Procedures. GLMX represents and warrants that its security program contains a security incident response plan that includes procedures to be followed in the event of any Security Breach or any breach of any application or system directly associated with the accessing, processing, storage, communication or transmission of Confidential Information.

4.3 Program Adjustments. GLMX represents and warrants that it monitors, evaluates, and adjusts, as appropriate, the security program in light of: (i) any relevant changes in technology and any internal or external threats to GLMX or the Confidential Information; (ii) security and data privacy laws and regulations applicable to GLMX; and (iii) GLMX's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

4.4 Security Awareness and Training. GLMX shall conduct a mandatory annual security awareness and training program for all employees or contractors of GLMX's workforce, which includes: (i) training on how to implement and comply with its information security program; and (ii) the promoting of a culture of security awareness through periodic communications from senior management with employees.

5. Access Controls. GLMX's Security Program shall contain policies, procedures, and logical controls designed to: (i) limit access to Confidential Information, GLMX's information systems, and the facility or facilities in which they are housed to properly authorized persons; (ii) prevent those workforce members and others who should not have access from obtaining access; and (iii) remove access on a timely basis in the event of a change in job responsibilities or job status. Access Controls shall include, at a minimum, (a) multi-factor authentication of all GLMX employees and contractors remotely accessing GLMX systems and (b) stateful packet inspection firewalls and Intrusion Prevention for all GLMX networks.

6. Storage and Transmission Controls. GLMX's Security Program will contain storage and technical transmission security measures to guard against unauthorized access to Confidential Information that is being transmitted over a public electronic communications network or stored electronically. Such measures include requiring encryption of any sensitive information stored or transmitted over unsecured networks. It also includes the operation of up-to-date antivirus software on desktops and laptops.

7. Physical and Environmental Security. GLMX will maintain controls that provide reasonable assurance that access to physical servers at the production data centers (and all GLMX facilities), is limited to properly authorized individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes. Controls include video surveillance, badge systems, visitor logs, biometric access controls, and restriction of device removal to authorized ticketed devices.

8. Additional Mandatory Elements, Policies, and Procedures. In addition to the requirements in Section 7.2, GLMX's Security Program will (at a minimum) contain:

(a) "**Audit Controls**" — Meaning hardware, software, and/or procedural mechanisms that record and examine activity in GLMX's information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements.

(b) A "**Secure Disposal Policy**" — Meaning policies and procedures regarding the disposal of tangible property containing Confidential Information, taking into account available technology so that sensitive information cannot be practicably read or reconstructed. The following criteria must be used for media sanitization for media used for processing Subscriber Confidential Information: (i) if the media is rewriteable, then a purge procedure recommended in the NIST Guide must be used on the media; (ii) If degaussing will render the media unusable and destruction is not the intent, then software purge techniques may be used where applicable; and (iii) When software purge is not an available option, then the media must be degaussed or destroyed.

(c) "**Testing**" — Meaning regularly testing of the key controls, systems and procedures of its information security program to validate that they are properly implemented and effective in addressing the threats and risks identified.

(d) An "**Assigned Security Responsibility**" — Meaning GLMX has assigned responsibility for the development, implementation, and maintenance of its information security program, including: (i) designating a security official with overall responsibility, and providing the official's contact details to Subscriber; and (ii) defining security roles and responsibilities for individuals with security responsibilities. The GLMX and Subscriber contacts for security and privacy issues are:
If to GLMX:
Name: General Counsel; email: legal@glmx.com; phone: (001) 646-948-6704

If to Subscriber:
Name: ; email: ; phone:

(e) "**Monitoring**" — Meaning the monitoring of the network and production systems, including error logs on servers, disks and security events for any potential problems. Such monitoring includes: (i) Reviewing changes affecting systems handling authentication, authorization, and auditing and; (ii) Reviewing privileged access to GLMX's production systems.

(f) "**Change and Configuration Management**" Meaning that policies and procedures are maintained for managing changes to GLMX's production systems, applications, and databases. Such policies and procedures include: (i) a process for documenting, testing and approving the promotion of changes into production; (ii) a security patching process that requires patching systems in a timely manner based on a risk analysis according to a documented patching policy; and (iii) a process for GLMX to utilize a third party to conduct web application level security assessments. These assessments generally include testing for: (1) cross-site request forgery, (2) improper input handling (e.g. cross-site scripting, SQL injection, XML injection, cross-site flashing), (3) XML and SOAP attacks, (4) weak session management, (5) data validation flaws and data model constraint inconsistencies, (6) insufficient authentication, and (7) insufficient authorization

9. Independent Penetration Tests. GLMX shall commission an independent penetration test of the service at least annually and will furnish Subscriber with a summary of the report from such tests upon request. GLMX shall use all commercially reasonable efforts to promptly make any necessary changes to secure the service following identification of vulnerabilities in the testing.

10. Audit Report. GLMX shall commit to achieving and maintaining an unqualified report that covers at a minimum the AICPA TSC Confidentiality and Security principles, or equivalent, and make such report available upon request to Subscriber. GLMX shall not materially lessen the controls contained in the most recent report. The report shall be prepared according an equal or greater standard to SOC 2.

11. Software Development. GLMX shall develop software in accordance with a written Software Development Policy, and consistently with industry best practices. These practices shall include, at a minimum, review of developed code, and testing of changes before being deployed to production, and segregation of development and production environments.

12. Vulnerability Scanning. GLMX shall routinely scan developed applications and production networks for known security vulnerabilities using industry standard tools. GLMX shall remediate any discovered vulnerabilities according to a documented vulnerability risk and patching procedure.

13. Continuity and Recovery. GLMX shall maintain a documented plan for business continuity and disaster recovery, including documented Recovery Time and Recovery Point objectives, and shall test the plan at least annually. During the term of the Agreement, GLMX shall use reasonable efforts to protect Client Data behind a firewall system, to conduct daily data backups, and to store weekly full-system backups in a separate, fire-safe facility.

14. Secure Configuration. GLMX shall develop, deploy, and maintain secure system, network and workstation configurations. In particular, removable media use shall be blocked on workstations. GLMX shall maintain an inventory of all systems storing or processing Subscriber's Confidential Data.

EXHIBIT E: UK SCCs ADDENDUM

PART 1: TABLES

Table 1: Parties

Start date	Effective Date	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As indicated in the preamble of the Agreement.	As indicated in the preamble of the Agreement.
Key Contact	As indicated in clause 13.2 of the Agreement.	General Counsel; email: legal@glmx.com; phone: (001) 646-948-6704.
Signature (if required for the purposes of Section 2)	As indicated and signed on the signature page of the Agreement.	As indicated and signed on the signature page of the Agreement.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum SCCs		The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Effective Date Reference (if any): Other identifier (if any):			
Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
2	Applies	Applies	General Authorisation	Five (5) business days	No

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

- List of Parties: as indicated in Annex 1A of the SCCs.
- Description of Transfer: as indicated in Annex 1B of the SCCs.
- Technical and organisational measures including technical and organisational measures to ensure the security of the data: as indicated in Annex II of the SCCs.
- List of Sub processors: as indicated in Annex III of the SCCs.

Table 4: Ending this Addendum when the Approved Addendum Changes

The Importer may end this Addendum as set out in Section **Error! Reference source not found.**.

PART 2: MANDATORY CLAUSES

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses, are incorporated herein by reference.