

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.
- (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;

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.

- (ii) Clause 8 –Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);
 - (iii) Clause 9 –Module Three: Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12 –Module 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 – Module Three: 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.

MODULE THREE: Transfer processor to processor

8.1 Instructions

- (a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
- (b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
- (c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
- (d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

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 rectify or erase 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 controller 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, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union² (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:

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 purposes of these Clauses.

- (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 of Regulation (EU) 2016/679;
- (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 or the controller 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 controller.
- (c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
- (d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
- (e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
- (f) 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.
- (g) 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

MODULE THREE: Transfer processor to processor

- (a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 90 days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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

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

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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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

MODULE THREE: Transfer processor to processor

- (a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
- (b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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.

MODULE THREE: Transfer processor to processor

- (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

MODULE THREE: Transfer processor to processor

- (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

MODULE THREE: Transfer processor to processor

- (a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory

measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE THREE: Transfer processor to processor

- (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 safeguards⁴;
 - (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

⁴ As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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). 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, 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 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 processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

MODULE THREE: Transfer processor to processor

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.

The data exporter shall forward the notification to the controller.

- (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.). The data exporter shall forward the information to the controller.
- (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. The data exporter shall make the assessment available to the controller.
- (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 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 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

MODULE THREE: Transfer processor to processor

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.







Clause 18

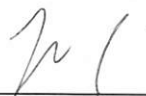





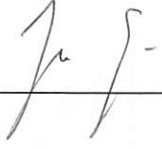
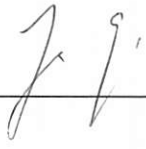
Choice of forum and jurisdiction




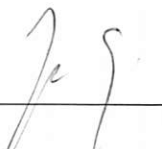

MODULE THREE: Transfer processor to processor

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of the Member State whose law shall apply pursuant to Clause 17.
- (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****MODULE THREE: Transfer processor to processor****Data exporter:**

| County | Name and Address of Processor Data Exporter | Contact Person | Signature | Date |
|---|--|---|---|--------|
| Austria | Abbott Medical Austria GmbH Perfektastrasse 84A 1230 Vienna Austria | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-25 |
| Belgium, Luxembourg, Bulgaria, Croatia, Czech Republic, Slovakia, Slovenia, Romania, Serbia, Belorussia, Kazakhstan | Abbott Medical Belgium The Corporate Village Building Figueras Da Vincilaan 11 Box F1 Zaventem Belgium | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-25 |
| Denmark | Abbott Medical Danmark A/S Produktionsvej 14 2600 Glostrup Denmark | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-25 |
| Estonia | Abbott Medical Estonia OÜ Mõisa 4/Vabaõhumuuseumi tee 3 13522, Tallinn Estonia | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-25 |
| Finland | Abbott Medical Finland Oy Karvaamokuja 2 00380 Helsinki Finland | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-25 |
| France | Abbott Medical France sas 1-3 Esplanade du Foncet 92130 Issy-les- | Jacob Springer, DVP, Global Privacy, Office |  | 2-5-25 |

| County | Name and Address of Processor Data Exporter | Contact Person | Signature | Date |
|----------------------|--|--|---|--------|
| | Moulineaux Cedex France | of Ethics & Compliance | | |
| Germany | Abbott Medical GmbH Helfmann-Park 7 65760 Eschborn Germany | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-25 |
| Greece | Abbott Medical Hellas Ltd. Iroos Matsi & Archaeou Theatrou Str. 17456 Alimos-Athens Greece | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-25 |
| Hungary | Abbott Medical Kft. 1138 Budapest Népfürdő utca 22.B. Hungary | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-25 |
| Ireland | Abbott Medical Ireland Limited Riverside One Sir John Rogerson's Quay Dublin 2 D02 X576 Ireland | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-25 |
| Italy | Abbott Medical Italia S.r.l. Edison Center Viale Thomas Alva Edison, 110 20099 Sesto S. Giovanni (MI) Italy | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-25 |
| Lithuania, Latvia | UAB Abbott Medical Lithuania Seimyniskiu str. 3 LT-09312 Vilnius Lithuania | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-25 |
| Netherlands | Abbott Medical Nederland B.V. Standaardruiter 13 3905 PT Veenendaal Netherlands | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-25 |
| Norway | Abbott Medical Norway AS Gullhaugveien 7 Oslo, 0484 Norway | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-25 |

| County | Name and Address of Processor Data Exporter | Contact Person | Signature | Date |
|----------------|---|---|---|--------|
| Poland | Abbott Medical Sp. z o.o. Postępu 21B 02-676 Warsaw Poland | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-15 |
| Portugal | Abbott Medical (Portugal) Distribuicao de Produtos Medicos, Lda. Estrada de Alfragide 67 Alfragide Edificio D Amadora Portugal | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-15 |
| Spain | Abbott Medical España, S.A. Avda. de Burgos 91 Edificio 4, planta 0 28050, Madrid Spain | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-15 |
| Sweden | Abbott Medical Sweden AB Isafjordsgatan 15 164 07 Kista Sweden | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-15 |
| United Kingdom | Abbott Medical U.K Limited Capulet House Stratford Business & Technology Park, Banbury Road Stratford upon Avon CV37 7GX, England | Jacob Springer, DVP, Global Privacy, Office of Ethics & Compliance |  | 2-5-15 |

Data importer:

Name: Abbott Laboratories ("Abbott")

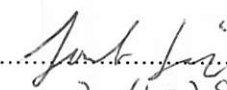
Address: 100 Abbott Park Rd Abbott Park, IL, 60064-3500 USA

Contact person's name, position and contact details:

Jacob Springer,

DVP, Global Privacy, Office of Ethics & Compliance

Signature:



Date: 2-4-15

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred

- (i) Those Controller employees or other authorized users provided with an administrative user ID for the Merlin.net™ Patient Care Network and those authorized users of the Controllers provided with a user ID to the Merlin.net™ Patient Care Network; and
- (ii) Patients enrolled in Merlin.net by a Controller.

Categories of personal data processed

Controller employees or other Authorized Users: name, phone number, email address, Controller name, and Controller country. Additional information, if provided by the Controller, include job title or role and clinic ID.

Patients enrolled in Merlin.net™ by you: Required patient data fields include date of birth, serial number of the implanted device, and information relating to the functioning of the implanted device. The patient's first name and last name may be required depending on whether a Patient ID is provided by the Controller. Depending on the implanted device, a patient's primary phone, email, and/or implant date may be required. Additional patient data, if provided by the Controller, includes gender, preferred language, a clinic assigned patient number or other patient identifier, and an emergency contact for the patient, including their name, phone number, and address.

French Patients enrolled in Merlin.net: The national health identifier ("INS") will be collected in accordance with the standards of the Agence du Numérique en Santé ("ANS").

Specifically, the health data of French patients can be referenced with INS on Merlin.net. We may then collect INS information such as a patient's gender and place of birth if they are based in France.

Sensitive data processed (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.

Additional patient data, if provided by the Controller, includes race, medications, hospitalisations, information about the patient's condition, diagnoses and treatment. **French Patients:** Sensitive data collected includes the national health identifier ("INS").

Nature of the processing

The personal data shall be subject to the following processing operations:

- Receiving data, including collection, accessing, retrieval, recording and data entry;
- Holding data, including storage, organisation and structuring;
- Protecting data, including restricting, encrypting, and security testing;
- Returning data to the data exporter;
- Erasing data, including destruction and deletion;
- Supporting the implanted cardiac devices;

- For devices that support remote programming capabilities, enabling the health care provider to make adjustments to the devices remotely through Merlin.net;
- Training and maintenance of Merlin.net™;
- Data collection and hosting;
- Transmission via electronic transmitters (monitors);
- Information and transmission reporting;
- Upon request by you, assistance with the interpretation or analysis of certain device-related information;
- Technical and clinical support services; and
- Patients implanted with an Abbott implanted cardiac device may send automated transmissions of information collected from their respective implanted medical device to Merlin.net for that patient's clinic (i.e., the Controller) and medical team to receive regular updates on the performance and status of their implanted cardiac device for the remote monitoring of certain aspects of the patient's condition.

Purpose(s) for which the personal data is processed on behalf of the controller

To provide, operate and maintain the Merlin.net™ Patient Care Network, including processing necessary to provide support services in connection with the operation of Devices monitored by the Merlin.net Services.

Duration of the processing

The data importer will continue to store data exporter's patients' personal data for the period that the Controller uses the services, unless Controller chooses to delete their patient personal data sooner. Further, processor may retain personal data in accordance with applicable legal requirements.

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

This is specified in Annex IV.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE THREE: Transfer processor to processor

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

The supervisory authority competent for the data exporter.

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

MODULE THREE: Transfer processor to processor

ABBOTT MERLIN.NET™ PATIENT CARE NETWORK MEASURES

Accreditations/Certifications

1. ISO 27001:

Abbott and Merlin.net is certified with the Information Security Management standard ISO/IEC 27001:2013. The ISO certification recognizes that Merlin.net has established processes and standards that maintain the required levels of confidentiality, integrity and availability for customers. A current copy of the ISO certification for Merlin.net is available upon request.

2. L'Agence du Numérique en Santé (French Customers):

Abbott and Merlin.net is accredited with L'Agence du Numérique en Santé (HDS) for health data hosting. The HDS certification for Abbott Laboratories can be found here: <https://esante.gouv.fr/labels-certifications/hds/liste-des-herbergeurs-certifies> (in French only).

Security Measures

Abbott has implemented the following technical and organisational security measures to ensure the ongoing confidentiality, integrity, availability and resilience of its processing systems and services:

1. Physical access control of processing areas (confidentiality):

Steps taken by Abbott's industry-leading cloud service provider to prevent unauthorized access to data processing equipment (for example, telephones, database and application servers, and associated hardware) in which Personal Data is processed include the following appropriate measures:

- (i) Merlin.net assets are housed within two ISO/IEC 27001:2013 certified computer data centres;
- (ii) Data centres are monitored around the clock by security guards and/or security cameras and other sensors that can detect and track unauthorized persons;
- (iii) Physical access to facilities, including data centres, is granted based on job responsibility and requires management approval;
- (iv) Visitors sign a visitor log prior to entry and must be escorted by Abbott personnel at all times; and
- (v) Physical access rights and authentication controls (for example, card readers) at entry and exit points are implemented, documented and regularly checked.

2. Access control to data processing systems (confidentiality):

Abbott takes appropriate measures to prevent its data processing systems from being used by unauthorized persons. This is achieved by:

- (i) Multi-factor authentication;
- (ii) Restricting access to services through encryption, signature algorithms and secure certificates;
- (iii) Storing data on a secure database that uses disk-level encryption;
- (iv) Using industry standard encryption and password requirements (for example, minimum length, use of special characters, expiration and so on); and
- (v) Locking access following unsuccessful login attempts or inactivity and having a method to reset locked access identifiers.

3. Access control for the use of certain areas of data processing systems by authorized Abbott personnel (confidentiality):

Abbott personnel authorized to use data processing systems may only access Personal Data where they have sufficient access authorisation. To this end, Abbott has implemented the following controls:

- (i) Access is restricted on the basis of roles and responsibilities and is granted to users in accordance with need-to-know and least-privilege principles;
- (ii) Privileged access is granted to authorized administrators, in line with job responsibilities;
- (iii) Access rights are reviewed periodically to ensure that correct access rights are granted; when roles and responsibilities change, access rights are removed, even in the event of termination; and
- (iv) Effective disciplinary action against individuals who access Personal Data without authorization.

4. Clinic setup and security:

Abbott's Remote Care Operations group is responsible for the initial setup of clinics upon enrollment. One clinic administrator account is provided for the purpose of creating, administering and maintaining user IDs. Clinic users, including administrators, are responsible for protecting their Merlin.net credentials. The following controls are implemented:

- (i) Clinicians are restricted from directly accessing the database and infrastructure supporting Merlin.net.
- (ii) For support and troubleshooting purposes, authorized Abbott personnel utilise a designated administrative account.
- (iii) Minimum default password parameter configurations are established.
- (iv) Merlin.net offers two-factor authentication, which customers may elect to implement.

5. Transfer control (integrity):

Abbott takes steps to prevent Personal Data from being read, copied, altered or deleted by unauthorized persons during its transmission or transfer. This is achieved by:

- (i) The transfer of data from external sources to Merlin.net infrastructure is encrypted;
- (ii) Servers use secure network connectivity that is restricted to HTTPS only; and
- (iii) Policies and standards are in place to restrict the use of removable media for transportation purposes and on corporate laptops or other mobile devices.

6. Input control (integrity):

Abbott does not access Personal Data for any purposes other than those set out in the Merlin.net™ PCN Agreement and the Data Processing Agreement (DPA).

Abbott takes appropriate measures to protect personal data against unauthorized access or deletion. This is achieved by:

- (i) Protective measures for reading, changing and deleting stored data;
- (ii) Documentation to control which persons are authorized and responsible for making entries into data processing systems on the basis of their tasks; and
- (iii) Protocols that require the logging of possible entries and / or deletions of Personal Data.

7. Order control:

Abbott takes steps to ensure that, where Personal Data is processed, it is processed strictly in accordance with your instructions. This is achieved by:

- (i) Clear instructions to Abbott on the scope of required Personal Data processing as set out in the Agreement and the DPA.

8. Availability control (availability):

Abbott takes steps to ensure that Personal Data is protected from accidental destruction or loss. This is achieved by:

- (i) Regular data backups and periodic restores;
- (ii) Backup logs are monitored and escalation protocols exist in case of a critical failure;
- (iii) Use of anti-virus/anti-malware software to protect against malicious threats such as viruses, worms and spyware;
- (iv) Conducting internal and external vulnerability scans on a regular basis; and
- (v) Implementation of a Business Continuity Plan, which includes an IT Disaster Recovery Plan, listing the roles, tasks and responsibilities.

9. Separation of processing for different purposes:

Abbott takes steps to ensure that Personal Data is protected from accidental destruction or loss. This is achieved by:

- (i) Ensuring database-driven security by separating production and support and system monitoring databases; and
- (ii) Designing interfaces, batch processes, and reports for specific purposes and functions only, so data collected for specific purposes is processed separately.

10. Resilience:

Abbott has implemented the following technical and organisational security measures, in particular to ensure the reliability of our processing systems and services:

- (i) Data protection management policies and procedures;
- (ii) Incident response policies and procedures;
- (iii) Data protection-friendly pre-settings (as required by GDPR Article 25(1)); and
- (iv) Order control.

ANNEX III**LIST OF SUB-PROCESSORS****MODULE THREE: Transfer processor to processor**

| Sub-processor name | Sub-processor address | Description of services | Location from which services are provided |
|---------------------------|---|--|--|
| Microsoft Azure | 700 Bellevue Way NE - 22nd Floor Bellevue, Washington, 98004 USA | Azure hosting service for encrypted data | Ireland <u>Licensing Documents</u> (microsoft.com) |
| | | | |

ANNEX IV

LOCAL LAW AMENDMENTS FOR DATA EXPORTERS NOT SUBJECT TO THE GDPR

The parties agree to the local law amendments set out below, which are required for full compliance with mandatory requirements regarding the commissioning of processors under the national laws applicable to the data exporter. For the avoidance of doubt, each of the amendments shall only apply if and to the extent the data exporter is located within the jurisdiction set out below:

1. Local Law Amendments for Data Exporters located in Switzerland:

(a) Insofar data transfers are subject to the Swiss Federal Act on Data Protection of June 19, 1992 or as from 1 September 2023 the Federal Act on Data Protection of 25 September 2020 ("FADP"), references to the GDPR shall be interpreted as references to the FADP or any subsequent act, including the relevant amendments and implementing ordinances (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established; for Switzerland i.e. the Federal Data Protection and Information Commissioner, Feldeggweg 1, 3003 Bern); insofar data transfers are subject to cantonal data protection laws, references to the GDPR shall be interpreted as references to the relevant cantonal data protection laws applicable to the data exporter (whereby the "Authority" shall mean the competent cantonal data protection authority in the canton in which the data exporter is established).

(b) The Data Importer acknowledges and agrees that the personal data transferred to the Data Importer by the Data Exporter may include personal data of legal persons and personality profiles of natural persons. The Data Importer shall process personal data of legal persons in the same manner as other personal data and personality profiles in the same manner as special categories of data (the special protection of data from legal persons and from personality profiles will be abolished upon entering into force of the revised Swiss Federal Data Protection Act of 25 September 2020 on 1 September 2023, whereupon the obligations of the Data Importer according to this paragraph (b) shall cease);

(c) The term "Member State" shall be interpreted as including Switzerland;

(d) The term "Member State" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their habitual place of residence (Switzerland) in accordance with Clause 18c.

2. Local Law Amendments for Data Exporters located in United Kingdom:

UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

This Addendum has been issued by the Information Commissioner ("ICO") for Parties making Restricted Transfers. The ICO considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

PART 1: TABLES

1. Table 1: Parties

| | | |
|------------------|--|---|
| Start date | The date of the last signature to the Addendum EU SCCs | |
| The Parties | Exporter (who sends the Restricted Transfer) | Importer (who receives the Restricted Transfer) |
| Parties' details | As set out in Annex 1A to the Addendum EU SCCs | As set out in Annex 1A to the Addendum EU SCCs |

2. Table 2: Selected SCCs, Modules and Selected Clauses

| | |
|------------------|---|
| Addendum EU SCCs | <input checked="" type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information. <input type="checkbox"/> The Standard Contractual Clauses as defined in the DPA. |
|------------------|---|

3. 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:

- Annex 1A: List of Parties: As set out in the Addendum EU SCCs
- Annex 1B: Description of Transfer: As set out in Annex 1B of the Addendum EU SCCs
- Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set out in Annex II of the Addendum EU SCCs
- Annex III: List of Sub processors (Modules 2 and 3 only): As set out in Annex III of the Addendum EU SCCs

4. Table 4: Ending this Addendum when the Approved Addendum Changes

| | |
|---|---|
| Ending this Addendum when the Approved Addendum changes | Which Parties may end this Addendum as set out in Section 19: <input checked="" type="checkbox"/> Importer <input checked="" type="checkbox"/> Exporter <input type="checkbox"/> neither Party |
|---|---|

PART 2: MANDATORY CLAUSES

Entering into this Addendum

- Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
- Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

- Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

| | |
|----------------------|---|
| Addendum | This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs. |
| Addendum EU SCCs | The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information. |
| Appendix Information | As set out in Table 3. |

| | |
|-------------------------|--|
| Appropriate Safeguards | The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR. |
| Approved Addendum | The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18. |
| Approved EU SCCs | The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021. |
| ICO | The Information Commissioner. |
| Restricted Transfer | A transfer which is covered by Chapter V of the UK GDPR. |
| UK | The United Kingdom of Great Britain and Northern Ireland. |
| 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 | As defined in section 3 of the Data Protection Act 2018. |

Part 2 Mandatory Clauses:

| | |
|--------------------------|---|
| Mandatory Clauses | Part 2: 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. |
|--------------------------|---|