PAYNE HICKS BEACH LLP

STANDARD CONTRACTUAL CLAUSES FOR PERSONAL DATA TRANSFERS CONTROLLER TO A PROCESSOR

SECTION I

CLAUSE 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

CLAUSE 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

CLAUSE 3

Third-party beneficiaries

(c) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

(ix) 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 (in the same country as the data importer or in another third country, hereinafter **onward transfer**) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

CLAUSE 9

Use of sub-processors

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under theseClausesto a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) OPTION 2 GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least *[Specify time period]* 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.

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

sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

(e) 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.

(f) 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) [OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body [FN11] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(c) 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.

(d) 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.

(e) 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.

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

(g) 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 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.

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

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

CLAUSE 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

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

CLAUSE 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

CLAUSE 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

CLAUSE 17

Governing law

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

[OPTION 2: 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 _____ (*specify Member State*).]

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 _____ (*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name:	Payne Hicks Beach LLP
Address:	10 New Square Lincoln's Inn London United Kingdom WC2A 3QG
Contact person's name and details:	Jonathan Sewell – Data Protection Officer jsewell@phb.co.uk Payne Hicks Beach LLP 10 New Square Lincoln's Inn London United Kingdom WC2A 3QG
Activities relevant to the data transferred under these Clauses:	Processing of Exporter's clients' data and/or the Exporter's data.
Signature and date:	 6 May 2025
Role:	Controller
Exporter's representative in the European Union:	IT Governance Europe Ltd (Republic of Ireland company number: 590421) 6th Floor South Bank House Barrow Street Dublin 4 Republic of Ireland

Data importer(s):

Name:	Organisations which process personal data on behalf of the Exporter and under the direct instructions of the Exporter.
Address:	As confirmed in the Exporter's engagement letter, terms and conditions of business or letter of instruction addressed to the Importer.
Contact person's name and details:	Importer name as confirmed in the engagement letter, terms and conditions of business or letter of instruction.
Activities relevant to the data transferred under these Clauses:	The processing of personal data.
Signature and date:	In accordance with the engagement, terms and conditions of business or letter of instructions.
Role:	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	• Clients of the Exporter; • Personnel processing personal data for or on behalf of the Exporter; and • Contacts or business associates of the Exporter processing data for or on behalf of the Exporter.
Categories of personal data transferred:	• Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses; • Date of birth; • Gender; • Marital status and dependants; • Family information; • Details from personal or professional online presence; • National Insurance number; • Bank account details; • Employment, pension and tax information; • Nationality and immigration status;

	• Copies of and information from identification documents such as passport and driving licence; • CCTV footage and photographs; • Copies of an information from identification documents such as passport, driving licence and utility bills; • Information relating to the matter in which our advice or representation are sought; • Information to enable us to undertake a credit or other financial check; • Financial details so far as they are relevant to the instructions (such as the source of funds and wealth if we are instructed on a purchase transaction); and • Information about criminal convictions and offences. **Organisations and business contacts personal data:** • may include, organisational name, basic personal contact details such as first and second name, title, addresses, telephone numbers, and personal email addresses and/or business email addresses, date of birth, gender, and marital status; and • copies of and information from identification documents such as passport and driving licence and utility bills Details from personal or professional online presence, CCTV footage and photographs.
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:	• Personal data revealing racial or ethnic origin; • Personal data revealing political opinions; • Personal data revealing religious or philosophical beliefs; • Personal data revealing trade union membership; • Genetic data;

	• Biometric data (where used for identification purposes); • Data concerning health; • Data concerning a person's sex life; and • Data concerning a person's sexual orientation.
Applied restrictions:	There are no applied restrictions/not applicable.
Record of access to the data:	In accordance with the Exporter's data protection policy and data retention policy, procedures and guidelines.
Additional security consists of:	(a) Pseudonymisation of personal data; (b) Encryption of personal data; (c) Segregation of personal data from other networks; (d) Access control and user authentication; (e) Employee and staff training on information security; and (f) Written information security policies and procedures.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	This will be on a continuous transfer basis.
Nature of the processing:	• Personal data will be collected from the Importer and retained and stored in accordance with the Exporter's data retention policy and records of processing. • Authorised employees of the Exporter will have access to the personal data which will be shared with Importers and their authorised representatives and/or third party processors as required. • The Exporter will use processors and sub-processors where required. • The security measures the Exporter has in place to protect personal data are set out below in Annex II. • No new technology or novel types of processing are being used. Data will be

	kept within the UK, unless the Importers live outside of the UK and then data may be required to be sent outside the UK.
Purpose(s) of the data transfer and further processing:	In order to receive legal advice and/or progress legal disputes and for legal claims.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Personal data will be retained in accordance with the Exporter's data retention policy, procedures, records and guidelines and/or in accordance with the Solicitor's Regulation Authority legal requirements.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	This will be the same as set out above. Subject matter – the processing of client data and personal data provided by the Exporter to a processor or the Importer which is to be shared with a sub-processor. Nature and duration of processing – Nature of processing as set out above under ***"Nature of Processing"***. The duration of processing will be for as long as the personal data is retained by the sub-processor in accordance with the Importer's and Exporter's instructions.

C. COMPETENT SUPERVISORY AUTHORITY

Supervisory Authority:	The Information Commission
Address:	Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Tel: 0303 123 1113 Fax: 01625 524 510

ANNEX II

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

Measures include:

Pseudonymisation and encryption of personal data:

The Compliance department ensures that all personnel handling personal data are trained in data protection best practices and pseudonymise personal data when required. We encrypt personal data at rest and in transit, using industry-standard encryption algorithms.

Ongoing confidentiality, integrity, availability and resilience of processing systems and services:

We have implemented strong access control measures, such as multi-factor authentication, to ensure that only authorised personnel can access sensitive data and systems. We regularly monitor and audit systems and services to detect any unauthorised access or malicious activity. We ensure that all systems and services are regularly updated with the latest security patches and software updates. We have implemented a comprehensive backup and disaster recovery plan to ensure that data and systems can be quickly recovered in the event of a disaster. We have implemented encryption technologies to protect data in transit and at rest. We have established and are enforcing policies and procedures to ensure that data is handled securely and in accordance with applicable laws and regulations.

The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident:

We have established a comprehensive backup and recovery plan that includes regular backups of all data and systems. We ensure that all backups are stored securely offsite and are regularly tested to ensure they are up to date. We have implemented a disaster recovery plan that outlines the steps to be taken in the event of a physical or technical incident. We ensure that all systems are regularly monitored and maintained to ensure they are running optimally. We implement a secure authentication system to ensure that only authorised personnel have access to personal data. We ensure that all systems are regularly updated with the latest security patches and software updates. We educate staff on the importance of data security and the need to protect personal data.

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

We routinely employ third party Cybersecurity specialists to review our IT systems and policies. We have established a risk assessment process to identify potential security risks and vulnerabilities. We have developed and are implementing security policies and procedures to address any identified risks. We have Implemented technical measures such as firewalls, encryption, and access control systems. We have

established a system of regular monitoring and auditing to ensure compliance with security policies and procedures. We routinely train staff on security policies and procedures. We have established a system of incident response and reporting.

User identification and authorisation:

We implement strong passwords, two-factor authentication, single sign-on (SSO) systems and user activity monitoring systems.

The protection of data during transmission:

We implement encryption, secure protocols such as TLS, firewalls, intrusion detection systems and network segmentation.

The protection of data during storage:

We implement encryption, access control, endpoint protection, antivirus and malware protection, data backups, firewalls and physical security.

Physical security of locations at which personal data are processed:

We have installed security cameras and access control systems to monitor and restrict access to the premises. We ensure that all personnel have valid identification and authorisation to access the premises. We have stablished a secure perimeter around the premises and restrict access to authorised personnel only. We have installed firewalls and other security measures to protect the premises from unauthorised access. We ensure that all personnel are trained in security protocols and procedures. We regularly inspect the premises for any security breaches or vulnerabilities. We ensure that all data is stored securely and backed up regularly. We implement a policy of regular security audits to identify any potential security risks.

Events logging:

We routinely monitor our systems logs and automate the notification of certain events to the IT department and other relevant staff.

System configuration, including default configuration:

We have stablished a configuration management system to track and document changes to any IT system's configuration. We have implemented a change control process to ensure that all changes to the system configuration are approved and documented. We regularly review the system configuration to ensure that it is up to date and secure. We use automated tools to monitor the system configuration and detect any unauthorised changes. We regularly back up system configurations to ensure that they can be restored in the event of a system failure.

Internal IT and IT security governance and management:

We have established and are continuously enforcing IT policies and procedures, we implement security awareness training, we implement security monitoring and auditing, we have established a risk management program and we have established a disaster recovery plan.

Certification/assurance of processes and products:

We have stablished and are continuously enforcing policies and procedures for the development, implementation, and maintenance of our IT systems. We implement a quality assurance program to ensure that all IT systems meet the required standards. We are enforcing security policies and procedures to protect the confidentiality, integrity, and availability of our IT systems. We implement a risk management program to identify, assess, and mitigate risks associated with our IT systems. We implement a change management program to ensure that changes to our IT systems are properly documented and approved. We implement a disaster recovery plan to ensure that our IT systems can be recovered in the event of a disaster. We implement a system for monitoring and auditing our IT systems to ensure that they are functioning properly. We implement a system for tracking and reporting on our IT systems' performance. We implement a system for training and certifying IT personnel. We implement a system for testing and validating our IT systems.

Data minimisation:

We implement a data minimisation policy, data access controls, monitor data usage, encrypt data and when possible delete any unnecessary data.

Data quality:

We have established data quality standards, implement data quality checks, train staff, utilise data quality tools and have established data governance.

Ensuring limited data retention:

We have a data retention policy, implement data archiving, semi-automate data deletion and monitor data retention.

Ensuring accountability:

We have established clear policies and procedures for IT operations and data access. We have established a system of checks and balances to ensure that all IT operations are conducted in accordance with the established policies and procedures. We have established a system of logging and auditing to track all IT operations and data access. We have established a system of access control to ensure that only authorised personnel have access to sensitive data. We have established a system of user authentication to ensure that only authorised personnel can access the IT systems. We have established a system of encryption to protect sensitive data from unauthorised access. We have established a system of regular security reviews to ensure that all IT operations and data access are conducted in accordance with the established policies and procedures. We have established a system of training and awareness to ensure that all personnel are aware of the importance of IT security and the measures that must be taken to ensure accountability.

Data portability and ensuring erasure:

We have established a data portability policy, implement data encryption, monitor data transfers, implement an erasure policy and implement data destruction.

Transfers to (sub-) processors, describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter:

This is set out in our data sharing arrangements.

We use the following security measures on our website:

We would simply advise the use of 2FA (2 factor authentication) for all admin users.

We use SSL protection and certificates on our login pages and we use cyber security software and virus protection software.

We use a reputable web hosting company WP Engine.

We have a policy of regularly deleting any files, databases, or applications from our website that are no longer in use. During scheduled maintenance windows we ensure the hosting environment is up to date which includes keeping all plugins up to date and removing any which are no longer required or are a security risk.

All data is regularly backed up once every 24 hours.

We run regular web security scans to check for website and server vulnerabilities. These are run daily from WPEngine and also Wordfence which is our preferred Wordpress specific security application. We are currently running the free version of Wordfence.

We seek to use a fraud prevention service on our website.This is usually a process implemented on an eCommerce application, barring the contact form we do not have any functions on the current Payne Hicks Beach site that require users to provide personal details. The contact forms are also maintained by hubspot and we simply embed the form.

PAYNE HICKS BEACH LLP

STANDARD CONTRACTUAL CLAUSES FOR PERSONAL DATA TRANSFERS CONTROLLER-TO-CONTROLLER

SECTION I

CLAUSE 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

CLAUSE 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

CLAUSE 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5(e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

CLAUSE 4

Interpretation

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

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

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

CLAUSE 5

Hierarchy

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

CLAUSE 6

Description of the transfer(s)

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

CLAUSE 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

CLAUSE 8

Data protection safeguards

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

8.1 Purpose limitation

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

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

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

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

8.2 Transparency

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

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

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

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

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

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

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

8.3 Accuracy and data minimisation

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

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

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

8.4 Storage limitation

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

8.5 Security of processing

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

in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

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

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

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

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

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

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

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

8.7 Onward transfers

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

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

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

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

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

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

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

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

8.8 Processing under the authority of the data importer

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

8.9 Documentation and compliance

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

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

CLAUSE 9

Use of sub-processors

N/A.

CLAUSE 10

Data subject rights

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

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

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

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

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

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

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

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

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

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

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

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

CLAUSE 11

Redress

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

(b) [OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body [FN11] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(c) 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.

(d) 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.

(e) 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.

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

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

CLAUSE 12

Liability

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

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data

subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

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

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

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

CLAUSE 13

Supervision

(a) 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.

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

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

CLAUSE 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

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

CLAUSE 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

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

SECTION IV – FINAL PROVISIONS

CLAUSE 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

CLAUSE 17

Governing law

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

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 ……. *(specify Member State).*

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX
ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Data Exporter	
Name:	Payne Hicks Beach LLP
Address:	10 New Square Lincoln's Inn London WC2A 3QG England
Contact person's name, position and contact details:	Jonathan Sewell, Data Protection Officer jsewell@phb.co.uk Payne Hicks Beach LLP 10 New Square Lincoln's Inn London WC2A 3QG England
Activities relevant to the data transferred under these Clauses:	Processing of client data and/or personal data.
Signature and date:	
Role:	Controller
Data Exporter's Representative in the European Union	
Name:	IT Governance Europe Ltd (Republic of Ireland company number: 590421)
Address:	6th Floor South Bank House Barrow Street Dublin 4 Republic of Ireland

Data importer(s):

Name:	Clients of Payne Hicks Beach and/or organisations instructed to act as independent or joint controllers for or on behalf of the Exporter.
Address:	As confirmed in the Exporter's client care letter or instruction letter or terms and conditions of business or an agreement letter.
Contact person's name, position and contact details:	Client name as confirmed in the client care letter or a contact person's name stated in the instruction or terms and conditions of business or an agreement letter.
Activities relevant to the data transferred under these Clauses:	The processing of client data and/or personal data.
Signature and date:	In accordance with the client care letter or instruction letter or terms and conditions of business or an agreement letter.
Role:	Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	Clients of Payne Hicks Beach LLP and/or organisations instructed to act as independent or joint controllers for or on behalf of the Exporter.
Categories of personal data transferred:	• Client data and/or personal data which consists of: (a) from publicly accessible sources such as Companies House or HM Land Registry; (b) directly from a third party such as: • sanctions screening providers; • colleagues, witnesses and family members; • credit reference agencies; and • client due diligence providers. (c) from a third party such as: • bank or building society, another financial institution or advisor; • consultants and other professionals, including legal professionals and accountancy staff, we may engage in relation to a matter;

	• employer and/or trade union, professional body or pension administrators; and • doctors, medical and occupational health professionals; (d) via our website (for more information, please see the cookies policy on our website); (e) via our information technology (IT) systems such as: • case management, document management and time recording systems; • door entry systems, CCTV and access control systems and reception logs; and • automated monitoring of technical systems, such as our computer networks and connections, communications systems, email and instant messaging systems; (f) basic personal contact details such as name, title, addresses, telephone numbers, and personal email addresses, date of birth, gender, family details, family information - such as marital status and details of dependants National Insurance, number bank account details, tax, employment and pension details and records; (g) copies of and information from identification documents such as passport and driving licence and utility bills, details from personal or professional online presence, CCTV footage and photographs; (h) further employment, pension and tax information; (i) nationality and immigration status; (j) information relating to the matter in which our advice or representation are sought;

	(k)information to enable us to undertake a credit or other financial check; and (l) financial details so far as they are relevant to the instructions (such as the source of funds and wealth if we are instructed on a purchase transaction). **Organisations and business contacts personal data:** • may include, organisational name, basic personal contact details such as first and second name, title, addresses, telephone numbers, and personal email addresses and/or business email addresses, date of birth, gender, and marital status; and • copies of and information from identification documents such as passport and driving licence and utility bills Details from personal or professional online presence, CCTV footage and photographs.
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:	• Personal data revealing racial or ethnic origin; • Political opinions; • Religious or philosophical beliefs; • Revealing trade union membership; • Genetic data; • Biometric data (where used for identification purposes); • Health; • A person's sex life; • A person's sexual orientation; and • Information about criminal convictions and offences.
Applied restrictions:	There are no applied restrictions/not applicable.
Record of access to the data:	In accordance with Payne Hicks Beach LLP's data protection policy and data retention policy, procedures and guidelines.
Additional security consists of:	(a) Pseudonymisation of personal data; (b) Encryption of personal data;

	(c) Segregation of personal data from other networks; (d) Access control and user authentication; (e) Employee and staff training on information security; and (f) Written information security policies and procedures.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	This will be on a continuous transfer basis.

Nature of the processing:	• How will the Exporter collect the data - the data will be collected from clients.
	• How will the Exporter store and retain the data – in accordance with Payne Hicks Beach LLP's data retention policy and procedures and records of processing.
	• Who has access to the data and who will the Exporter share it with – authorised staff at Payne Hicks Beach LLP will have access to the data. The data will be shared with clients and their authorised representatives and/ or third party processors as required.
	• Will the Exporter use data processors: yes they will use processors and sub-processors where required.
	• How long will the Exporter retain the data for: data will be retained generally for 7 years or in accordance with the Exporter's data retention policy, procedures, records and guidelines and in accordance with the Solicitor's Regulation Authority legal requirements.
	• What security measures does Payne Hicks Beach LLP have in place to protect data:
	  • Pseudonymisation of personal data;
	  • Encryption of personal data;
	  • Segregation of personal data from other networks;
	  • Access control and user authentication;
	  • Employee and staff training on information security; and

	• Written information security policies and procedures. • The security measures the Exporter has in place to protect personal data are also set out in Annex II. • Is the Exporter using any new technology or novel types of processing - No • What is the nature of transmission/ transfer of the data – the nature will be keeping data in the UK/EEA, unless the client is living outside of the UK/EEA. If this is the case the data will be sent to an adequate country or appropriate safeguards will be put in place such as standard contractual model clauses.
Purpose(s) of the data transfer and further processing:	In order to provide clients with legal advice and/or progress legal disputes and for legal claims purposes.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	In accordance with Payne Hicks Beach LLP's data retention policy.
For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing:	This will be the same as set out above in this Annex I. Nature and duration of processing – The Nature of processing will be as set out above under *"Nature of Processing"*. The duration of processing will be for as long as the data is retained by the sub-processor in accordance with the Exporter's instructions.
Subject matter:	Client data and/or personal data.

C. COMPETENT SUPERVISORY AUTHORITY

Supervisory Authority:	The Information Commission
Address:	Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Tel: 0303 123 1113 (local rate) Fax: 01625 524 510

ANNEX II

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

Measures include:

Pseudonymisation and encryption of personal data:

The Compliance department ensures that all personnel handling personal data are trained in data protection best practices and pseudonymise personal data when required. We encrypt personal data at rest and in transit, using industry-standard encryption algorithms.

Ongoing confidentiality, integrity, availability and resilience of processing systems and services:

We have implemented strong access control measures, such as multi-factor authentication, to ensure that only authorised personnel can access sensitive data and systems. We regularly monitor and audit systems and services to detect any unauthorised access or malicious activity. We ensure that all systems and services are regularly updated with the latest security patches and software updates. We have implemented a comprehensive backup and disaster recovery plan to ensure that data and systems can be quickly recovered in the event of a disaster. We have implemented encryption technologies to protect data in transit and at rest. We have established and are enforcing policies and procedures to ensure that data is handled securely and in accordance with applicable laws and regulations.

The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident:

We have established a comprehensive backup and recovery plan that includes regular backups of all data and systems. We ensure that all backups are stored securely offsite and are regularly tested to ensure they are up to date. We have implemented a disaster recovery plan that outlines the steps to be taken in the event of a physical or technical incident. We ensure that all systems are regularly monitored and maintained to ensure they are running optimally. We implement a secure authentication system to ensure that only authorised personnel have access to personal data. We ensure that all systems are regularly updated with the latest security patches and software updates. We educate staff on the importance of data security and the need to protect personal data.

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

We routinely employ third party Cybersecurity specialists to review our IT systems and policies. We have established a risk assessment process to identify potential security risks and vulnerabilities. We have developed and are implementing security policies and procedures to address any identified risks. We have Implemented technical measures such as firewalls, encryption, and access control systems. We have established a system of regular monitoring and auditing to ensure compliance with security policies and procedures. We routinely train staff on security policies and procedures. We have established a system of incident response and reporting.

User identification and authorisation:

We implement strong passwords, two-factor authentication, single sign-on (SSO) systems and user activity monitoring systems.

The protection of data during transmission:

We implement encryption, secure protocols such as TLS, firewalls, intrusion detection systems and network segmentation.

The protection of data during storage:

We implement encryption, access control, endpoint protection, antivirus and malware protection, data backups, firewalls and physical security.

Physical security of locations at which personal data are processed:

We have installed security cameras and access control systems to monitor and restrict access to the premises. We ensure that all personnel have valid identification and authorisation to access the premises. We have stablished a secure perimeter around the premises and restrict access to authorised personnel only. We have installed firewalls and other security measures to protect the premises from unauthorised access. We ensure that all personnel are trained in security protocols and procedures. We regularly inspect the premises for any security breaches or vulnerabilities. We ensure that all data is stored securely and backed up regularly. We implement a policy of regular security audits to identify any potential security risks.

Events logging:

We routinely monitor our systems logs and automate the notification of certain events to the IT department and other relevant staff.

System configuration, including default configuration:

We have stablished a configuration management system to track and document changes to any IT system's configuration. We have implemented a change control process to ensure that all changes to the system configuration are approved and documented. We regularly review the system configuration to ensure that it is up to date and secure. We use automated tools to monitor the system configuration and detect any unauthorised changes. We regularly back up system configurations to ensure that they can be restored in the event of a system failure.

Internal IT and IT security governance and management:

We have established and are continuously enforcing IT policies and procedures, we implement security awareness training, we implement security monitoring and auditing, we have established a risk management program and we have established a disaster recovery plan.

Certification/assurance of processes and products:

We have stablished and are continuously enforcing policies and procedures for the development, implementation, and maintenance of our IT systems. We implement a

quality assurance program to ensure that all IT systems meet the required standards. We are enforcing security policies and procedures to protect the confidentiality, integrity, and availability of our IT systems. We implement a risk management program to identify, assess, and mitigate risks associated with our IT systems. We implement a change management program to ensure that changes to our IT systems are properly documented and approved. We implement a disaster recovery plan to ensure that our IT systems can be recovered in the event of a disaster. We implement a system for monitoring and auditing our IT systems to ensure that they are functioning properly. We implement a system for tracking and reporting on our IT systems' performance. We implement a system for training and certifying IT personnel. We implement a system for testing and validating our IT systems.

Data minimisation:

We implement a data minimisation policy, data access controls, monitor data usage, encrypt data and when possible delete any unnecessary data.

Data quality:

We have established data quality standards, implement data quality checks, train staff, utilise data quality tools and have established data governance.

Ensuring limited data retention:

We have a data retention policy, implement data archiving, semi-automate data deletion and monitor data retention.

Ensuring accountability:

We have established clear policies and procedures for IT operations and data access. We have established a system of checks and balances to ensure that all IT operations are conducted in accordance with the established policies and procedures. We have established a system of logging and auditing to track all IT operations and data access. We have established a system of access control to ensure that only authorised personnel have access to sensitive data. We have established a system of user authentication to ensure that only authorised personnel can access the IT systems. We have established a system of encryption to protect sensitive data from unauthorised access. We have established a system of regular security reviews to ensure that all IT operations and data access are conducted in accordance with the established policies and procedures. We have established a system of training and awareness to ensure that all personnel are aware of the importance of IT security and the measures that must be taken to ensure accountability.

Data portability and ensuring erasure:

We have established a data portability policy, implement data encryption, monitor data transfers, implement an erasure policy and implement data destruction.

Transfers to (sub-) processors, describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter:

This is set out in our data sharing arrangements.

We use the following security measures on our website:

We would simply advise the use of 2FA (2 factor authentication) for all admin users.

We use SSL protection and certificates on our login pages and we use cyber security software and virus protection software.

We use a reputable web hosting company WP Engine.

We have a policy of regularly deleting any files, databases, or applications from our website that are no longer in use. During scheduled maintenance windows we ensure the hosting environment is up to date which includes keeping all plugins up to date and removing any which are no longer required or are a security risk.

All data is regularly backed up once every 24 hours.

We run regular web security scans to check for website and server vulnerabilities. These are run daily from WPEngine and also Wordfence which is our preferred Wordpress specific security application. We are currently running the free version of Wordfence.

We seek to use a fraud prevention service on our website. This is usually a process implemented on an eCommerce application, barring the contact form we do not have any functions on the current Payne Hicks Beach site that require users to provide personal details. The contact forms are also maintained by hubspot and we simply embed the form.

PAYNE HICKS BEACH LLP

INTERNATIONAL DATA TRANSFER ADDENDUM

CONTROLLER -TO- CONTROLLER

This agreement is between the Exporter and the Importer.

BACKGROUND:

This Addendum has been issued by the Information Commission for the Parties making Restricted Transfers as an Addendum to the Approved EU SCCs. The Information Commission considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

AGREED TERMS:

Table 1: Parties

The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: as set out in the Approved EU SCCs	Full legal name: Payne Hicks Beach LLP
		10 New Square Lincoln's Inn London United Kingdom WC2A 3QG
		Official registration number: OC430964

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum.				
Module	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?
1	Applicable	Applicable	Applicable	-	-	-
2	-	-	-	-	-	-
3	-	-	-	-	-	-
4	-	-	-	-	-	-

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:
Annex 1B: Description of Transfer:
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:
Annex III: List of Sub processors (Modules 2 and 3 only):

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: ☒ Importer ☐ **Exporter** ☐ 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) of the UK GDPR.
>
> **Approved Addendum**: The template Addendum issued by the ICO and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 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 Commission.

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.

This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

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

Hierarchy

Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation ((EU) 2016/679), then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

(a) references to the "Clauses" mean this Addendum, incorporating the Addendum EU SCCs;

(b) in Clause 2, delete the words:

"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";

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

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

(d) Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;";

(e) Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;";

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

(g) references to Regulation (EU) 2018/1725 are removed;

(h) references to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with "the UK";

(i) the reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module 1 is replaced with "Clause 11(c)(i)";

(j) Clause 13(a) and Part C of Annex I are not used;

(k) the "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commission";

(l) in Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

(m) Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

(n) Clause 18 is replaced with:

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

(o) the footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

From time to time, the ICO may issue a revised Approved Addendum which:

(a) makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

(b) reflects changes to UK Data Protection Laws.

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

(a) its direct costs of performing its obligations under the Addendum; and/or

(b) its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative 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 section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

PAYNE HICKS BEACH LLP

INTERNATIONAL DATA TRANSFER ADDENDUM

CONTROLLER -TO- PROCESSOR

This agreement is between the Exporter and the Importer.

BACKGROUND

This Addendum has been issued by the Information Commissioner for the Parties making Restricted Transfers as an Addendum to the Approved EU SCCs. The Information Commission considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

AGREED TERMS:

Table 1: Parties

The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Payne Hicks Beach LLP	Full legal name: as set out in the Approved EU SCCs
	10 New Square Lincoln's Inn London United Kingdom WC2A 3QG	
	Official registration number: OC430964	

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum.				
Module	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?

1	-	-	-	-	-	-
2	Applicable	Applicable	Applicable	General	14 days	-
3	-	-	-	-	-	-
4	-	-	-	-	-	-

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:
Annex 1B: Description of Transfer:
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:
Annex III: List of Sub processors (Modules 2 and 3 only):

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: ☐ Importer ☒ **Exporter** ☐ Neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. 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.

2. 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) of the UK GDPR.
>
> **Approved Addendum**: The template Addendum issued by the ICO and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 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 Commission.
>
> **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.

This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

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

Hierarchy

Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation ((EU) 2016/679), then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

(a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

(b) Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

(c) this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

(a) references to the "Clauses" mean this Addendum, incorporating the Addendum EU SCCs;

(b) in Clause 2, delete the words:

"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";

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

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

(d) Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;";

(e) Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;";

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

(g) references to Regulation (EU) 2018/1725 are removed;

(h) references to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with "the UK";

(i) the reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module 1 is replaced with "Clause 11(c)(i)";

(j) Clause 13(a) and Part C of Annex I are not used;

(k) the "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commission";

(l) in Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

(m) Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

(n) Clause 18 is replaced with:

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

(o) the footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

From time to time, the ICO may issue a revised Approved Addendum which:

(a) makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

(b) reflects changes to UK Data Protection Laws.

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

(a) its direct costs of performing its obligations under the Addendum; and/or

(b) its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative 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 section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.