MediGuide

Privacy Policy and Standard Contractual Clauses for the EU, EEA, UK and Switzerland

MediGuide International, LLC (hereinafter MediGuide) has established a comprehensive privacy program, including a global privacy office, supervised by a Chief Privacy Officer in the person of Kristyn D'Angelo (260 Chapman Road, Suite 203 Newark, DE 19702, USA; 302.425.5900; privacy@mediguide.com). This privacy program has been designed to help us respect and protect your data privacy rights.

This statement and agreement includes the Standard Contractual Clauses for the EU and EEA, the UK and Switzerland and the Website Privacy Statement.

GENERAL PRIVACY POLICY

Privacy is very important to the management of MediGuide, especially with respect to personal data processed as part of our Medical Second Opinion Programs and other related business activities.

In order for MediGuide to provide services to its members, we collect PHI and PII with our member's written consent, which includes the following data: full legal name, date of birth, gender, address, email, telephone number, insurance information, medical information, medical records and diagnostics.

Definitions

"Personal information" means any information that: (i) relates to an individual and (ii) identifies or can be used to identify an individual.

Such information may include an individual's name, postal address, email address, telephone number, Social Security (or like) number, and/ or other unique identifier.

"Sensitive personal data/sensitive information" defined as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions.

"Agent" or "Data Processor" means a third party that processes personal data solely on behalf of and under the instructions MediGuide.

Scope

This MediGuide Privacy Policy ("Policy") sets forth the privacy principles that MediGuide follows with respect to personal information.

Since MediGuide provides services to its members all over the world we work with third party administrators in countries where our members reside, help us gather PHI and PII (as listed above) in our members native language. These third party administrators work on the behalf and under the direction of MediGuide. MediGuide also shares PHI/PII with world leading medical centers and translation services in order to facilitate our service of medical second opinions. All of this is done with our members signed consent.

Standard Contractual Clauses

For personal information of MediGuide members, policyholders, insureds, consumers, healthcare professionals, medical research subjects and medical patients, investors, government officials (and others who entrust us), that MediGuide receives from the European Union, European Economic Area, United Kingdom or Switzerland, MediGuide has committed to handling such personal information in accordance with the respective laws and based on the respective Standard Contractual Clauses that apply for these jurisdictions, that you as a business partner or insurance company agree to by accepting this Privacy Policy.

MediGuide is based in the United States of America. Therefore, the EU Standard Contractual Clauses (APPENDIX 1) shall govern the relationship between MediGuide and the data exporter from the EU or EEA exclusively in regards to the processing of any Personal Data from Data Subjects that are based or resident in countries where GDPR applies ("EU Personal Data Processing"), and shall prevail over any conflicting or inconsistent provisions pertaining to EU Personal Data Processing in any commitment, obligation, arrangement, contract or Agreement between the parties, unless and until the EU Standard Contractual Clauses are superseded by any new laws or regulations enacted by the European legislators (collectively, the "New EU Laws"), wherein such New EU Laws shall, from the date of their enforcement, apply automatically in place of the EU Standard Contractual Clauses to EU Personal Data Processing between MediGuide and the business partner or insurance company, unless either party notifies the other party in writing of its objection thereto within 30 days from the official publication date of the New EU Laws.

The Swiss Transborder Data Flow Agreement (APPENDIX 2) shall govern the relationship between the MediGuide data exporter from Switzerland exclusively in regards to the processing of any Personal Data from Data Subjects that are based or resident in Switzerland ("Swiss Personal Data Processing"), and shall prevail over any conflicting or inconsistent provisions pertaining to Swiss Personal Data Processing in any commitment, obligation, arrangement, contract or Agreement between the parties, unless and until the Swiss Transborder Data Flow Agreement is superseded by any new laws or regulations enacted by the Swiss legislators (collectively, the "New Swiss Laws"), wherein such New Swiss Laws shall, from the date of their enforcement, apply automatically in place of the Swiss Transborder Data Flow Agreement to Swiss Personal Data Processing between MediGuide and the business partner or insurance company, unless either party notifies the other party in writing of its objection thereto

within 30 days from the official publication date of the New Swiss Laws.

The Standard Contractual Clauses for International Transfers from Controllers to Processors for the United Kingdom (APPENDIX 3) shall govern the relationship between MediGuide and the data exporter from the UK exclusively in regards to the processing of any Personal Data from Data Subjects that are based or resident in the United Kingdom ("UK Personal Data Processing"), and shall prevail over any conflicting or inconsistent provisions pertaining to UK Personal Data Processing in any commitment, obligation, arrangement, contract or Agreement between the parties, unless and until the Standard Contractual Clauses for International Transfers from Controllers to Processor for the United Kingdom is superseded by any new laws or regulations enacted by the UK legislators (collectively, the "New UK Laws"), wherein such New UK Laws shall, from the date of their enforcement, apply automatically in place of the Standard Contractual Clauses for International Transfers from Controllers to Processors for the United Kingdom to UK Personal Data Processing between MediGuide and the business partner or insurance company, unless either party notifies the other party in writing of its objection thereto within 30 days from the official publication date of the New UK Laws.

Notice

MediGuide informs individuals in the EU, EEA, UK and Switzerland that the only purpose for which it collects and uses their personal information is to comply with the request of said individual that MediGuide secure a Medical Second Opinion for him/her, how to contact MediGuide, the type Agent/Data Processor third party with whom, at the direction of said individual, MediGuide shares their personal information, and the choice and means MediGuide offers for limiting the use and disclosure of their personal information.

Where MediGuide receives personal information directly from individuals in the EU, EEA, UK or Switzerland, it informs them about the types of personal information collected, the purposes for which it collects and uses the personal information, and the types of Agent/Data Processor to which the Company discloses or may disclose that information, and the choices and means, if any, the Company offers individuals for limiting the use and disclosure of their personal information.

Notice will be provided in a clear and conspicuous language when individuals are first asked to provide personal information, or as soon as practicable thereafter, and in any event before the Company uses or discloses the information for a purpose other than that for which it was originally collected. However, in no event or circumstance will MediGuide or its Agents or any Data Controller ever receive any personal information unless and until said individual authorizes MediGuide in writing signed by said individual to receive his/her personal information.

Choice

MediGuide, in addition to first having received a signed authorization from the individual to receive the individual's personal information, also offers an individual the opportunity to choose (opt out) whether personal data are (a) to be disclosed to a non-agent third party or (b) used for a purpose other than that for which the information were originally collected or subsequently authorized by the individual. In point of fact, MediGuide never uses the personal information for any purpose other than to secure a Medical Second Opinion, as originally requested by said individual. For sensitive personal information, MediGuide requires individuals to affirmatively and explicitly (opt in) by a signed writing to consent to the disclosure of the information to an Agent/Data Processor.

Accountability for Onward Transfers

MediGuide will only transfer personal data to an Agent/Data Processor where they provided assurances that they provide at least the same level of privacy protection as is required by these privacy principles. Where MediGuide has knowledge that an Agent/Data Processor to whom it has provided personal information is processing that information in a manner contrary to this Policy, MediGuide will take reasonable steps to prevent or stop the processing.

MediGuide will only transfer personal data to a non-agent third party in a manner that is consistent with the written authorization provided by the individuals who are the subject of the data and any consent that those individuals have given.

Security

MediGuide will take reasonable precautions to protect personal information in its possession from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Data Integrity and Purpose Limitation

MediGuide will only use and share personal data about individuals in a way that is consistent with the purposes for which the data were collected and authorized in writing by those individuals. To the extent necessary for those purposes, MediGuide will take reasonable steps to ensure that the data is reliable for intended use, accurate, complete, and current.

Access

MediGuide acknowledges the right of data subjects to access their personal data. Subject to limitations set forth by law. MediGuide will provide individuals with complete access to personal information about them and they may request the correction or amendment of personal information. Please apply to MediGuide's Privacy Office. Directed to Kristyn D'Angelo at 260 Chapman Road, Suite 203 Newark, DE 19702, USA, 302.425.5900 or privacy@mediguide.com.

The caller can trust that this will be a private conversation treated with confidentiality to whatever extent the caller requests.

Recourse, Enforcement and Liability

In compliance with law, MediGuide commits to resolve complaints about your privacy and our collection or use of your personal information. Please apply to MediGuide's Privacy Office. Directed to Kristyn D'Angelo at 260 Chapman Road, Suite 203 Newark, DE 19702, USA, 302.425.5900 or privacy@mediguide.com.

Limitation on Scope of Principles

MediGuide may be required to disclose an individual's personal information in response to a lawful request by public authorities, including to meet national security or law enforcement requirements.

This Policy may be amended from time to time, consistent with the requirements of MediGuide and the law.

MEMBERSHIP IN THE DATA PRIVACY FRAMEWORKS

MediGuide International, LLC complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. MediGuide International, LLC has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. MediGuide International, LLC has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/

The other U.S. entities or U.S. subsidiaries of our organization that are also adhering to the EU-U.S. DPF Principles, including as applicable under the UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF Principles and that are covered are: MediGuide Insurance Services International LLC, 260 Chapman Road, Suite 203 Newark, DE 19702, USA, email: info@mediguide.com

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, MediGuide International, LLC commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF.

We hereby inform data subjects about the relevant European Data Protection Authorities designated to address complaints concerning our organization's handling of personal data and that we provide appropriate recourse free of charge to the affected individual:

1. The EU Lead Data Protection Supervisory Authority (Responsible for EU/EEA Data Subjects) is: Bayerisches Landesamt fur Datenschutzaufsicht (BayLDA), Promenade 18, 91522 Ansbach, Germany.
2. The Data Protection Authority of Switzerland (Responsible for Data Subjects from Switzerland) is: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Feldeggweg 1, 3003 Bern, Switzerland.
3. The UK Data Protection Supervisory Authority (Responsible for Data Subjects from the UK) is: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, United Kingdom.

We inform all data subjects that our organization is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

Data subjects have the possibility, under certain conditions, to invoke binding arbitration. Our organisation is obligated to arbitrate claims and follow the terms as set forth in Annex I of the DPF Principles, provided that the data subject has invoked binding arbitration by delivering notice to our organization and following the procedures and subject to conditions set forth in Annex I of Principles. We hereby inform all data subjects about our organization's liability in cases of onward transfers to third parties. In particular, MediGuide International, LLC remains responsible and liable under the EU-U.S. DPF Principles, the UK extension to the EU-U.S. DPF, and/or the Swiss-U.S. DPF Principles if third-party agents that it engages to process the personal data on its behalf do so in a manner inconsistent with the Principles unless MediGuide International, LLC proves that it is not responsible for the event giving rise to the damage.

For any questions by data subjects or Data Protection Supervisory Authorities we designated the following local representatives:

Identity and contact details of the EU representative (Article 27 GDPR): Prof. Dr. h.c. Heiko Maniero, Franz-Joseph-Str. 11, 80801 Munchen, Bayern, Germany, E-Mail: info@dg-datenschutz.de

Identity and contact details of controller's UK representative (Article 27 UK-GDPR):

Prof. Dr. h.c. Heiko Maniero, 120 High Road, East Finchley, N2 9ED, London, England, United Kingdom, E-Mail: info@dg-datenschutz.de

Identity and contact details of controller's representative in Switzerland (Art. 14 FDPA): Prof. Dr. h.c. Heiko Maniero, c/o Cancellarius AG, Pflanzschulstrasse 3, 8400 Winterthur, Switzerland, E-Mail: info@dg-datenschutz.de. *Last Updated: September 2026*

HIPAA

To view HIPAA Compliance document, click here.

APPENDIX 1

To view GDPR Terms and Conditions, click here. To view List of (Sub-) Processors, click here.

APPENDIX 2 (SWISS TRANSBORDER DATA FLOW AGREEMENT) SWISS TRANSBORDER DATA FLOW AGREEMENT

by and between the

Business Partner or Insurance Company (hereinafter Data Exporter) and the MediGuide International, LLC 260 Chapman Road, Suite 203 Newark, DE 19702, USA (hereinafter Data Importer)

§ 1 Purpose

This Swiss Transborder Data Flow Agreement (the Agreement) is entered into by and between the Data Exporter and the Data Importer to provide adequate protection for Personal Data in situations in which such data is transferred from the Data Exporter established in Switzerland to the Data Importer established in another country for the purposes of processing such data on behalf of the Data Exporter. The purposes of the transfer to, and processing by, the Data Importer are described in Annex 1 to this Agreement. Annex 1 forms an integral part of this Agreement and may be amended by the Data Exporter from time to time.

§ 2 Scope

This Agreement applies to all Personal Data relating to Third Parties that is transferred (which shall include making it available for access) from the Data Exporter to the Data Importer; or processed by the Data Importer on behalf of the Data Exporter. The catalogue of the Personal Data to be transferred and/or processed is found in Section 1 of Annex 1 to this Agreement.

§ 3 Definitions

Unless defined otherwise herein, all terms shall have the same meaning as defined in the Swiss Federal Act of 19 June 1992 on Data Protection (FADP). Any reference to the FADP shall always also include a reference to the Ordinance to the FADP (the OFADP) and any other provision of the substantive Swiss Data Protection law. For the purposes of this Agreement: 'Data Exporter' means the natural or legal person, public authority, agency or any other body established in Switzerland which alone or jointly with others determines the purposes and means of the processing of Personal Data and which transfers such data to another country for the purposes of its processing on his behalf. 'Data Importer' means a natural or legal person, public authority, agency or any other body established in another country which agrees to receive Personal Data from the Data Exporter for the purposes of processing such data on behalf of the latter after the transfer in accordance with his instructions. 'Subprocessor' means any processor engaged by the Data Importer (or by any other Subprocessor of the Data Importer) who agrees to receive from the Data Importer (or from any other Subprocessor of the Data Importer) Personal Data exclusively intended for processing on behalf of the Data Exporter after the transfer in accordance with his instructions and the terms of the written subcontract.

§ 4 Obligations of the Data Exporter

The Data Exporter warrants that the Personal Data to be transferred has been collected and processed in accordance with the requirements of the FADP. The Data Exporter further warrants that the transfer of the Personal Data and the processing of such data by the Data Importer as set forth in this Agreement is admissible under the FADP and the Data Exporter undertakes that the transfer is made in accordance with the FADP. The Data Exporter shall verify that the Technical and Organizational Measures, as required by Art. 7 para. 1 FADP and Art. 8 et seq. OFADP, undertaken by the Data Importer (that are known to the data exporter) are sufficient to protect the transferred Personal Data from any unauthorized processing. The Technical and Organizational Measures form an integral part of this Agreement and may be amended by the Data Exporter from time to time.

§ 5 Obligations of the Data Importer

The Data Importer undertakes and warrants that it will process any and all Personal Data received from or made available by the Data Exporter or derived from such data (1) solely on behalf and solely for the purposes of the Data Exporter as set forth in Section 2 of Annex 1 or as otherwise expressly provided for by the Data Exporter or agreed with the Data Exporter; (2) in accordance with the instructions of the Data Exporter which may be given by any means, including e-mail; and (3) in compliance with this Agreement. The Data Importer undertakes, prior to any processing, appropriate Technical and Organizational Measures as defined by the FADP (particularly Art. 7 para. 1 FADP and Art. 8 et seq. OFADP) to protect the transferred Personal Data from unauthorized processing, including any processing not expressly authorized by this Agreement and including accidental loss or destruction of, or damage to, such Personal Data. The Data Importer will promptly inform, and cooperate with, the Data Exporter

(1) if it believes that it may no longer be able, or no longer is able, to comply with this Agreement, particularly in case it receives or must reasonably expect to receive a request or order of a competent authority requiring it to disclose, or refrain from further processing, some or all Personal Data to which this Agreement applies; or

(2) if any accidental or unauthorized access has occurred. The Data Importer shall not subcontract any of its processing operations performed on behalf of the Data Exporter under this Agreement without the prior written consent of the Data Exporter. In the event of subprocessing, the Data Importer undertakes that

(1) it has previously informed the Data Exporter and obtained its prior written consent;

(2) the subcontracting of the processing of Personal Data may only consist of the processing operations agreed in this Agreement;

(3) Data Importer and Subprocessor shall sign an Agreement which will impose the same obligations on the Subprocessor as those imposed on the Data Importer under this Agreement;

(4) it will promptly send a copy of any Subprocessor Agreement it concludes under this Agreement to the Data Exporter. Where the Subprocessor fails to fulfil its Data Protection obligations under such written agreement, the Data Importer shall remain fully liable to the Data Exporter for the performance of the Subprocessor's obligations under such agreement.

§ 6 Rights of Persons Affected

The Data Exporter is responsible that the Persons Affected are provided with their right of information (right of access), correction, blocking, suppression or deletion, as available under the FADP. The Data Importer (and any Subprocessor) will fully and without delay cooperate with the Data Exporter in, and provide to the Data Exporter the necessary services for, fulfilling such requests or inquiries of Persons Affected.

§ 7 Term and Termination

This Agreement shall be binding between the parties upon execution by both parties and shall remain in place for an indefinite period of time. Each party may terminate this Agreement at any time with immediate effect by providing a written notice. The Data Exporter may also suspend the transfer of Personal Data and/or its processing at any time. Upon termination of this Agreement for whatever reason, the Data Importer (and any Subprocessor) shall,

(1) immediately return any Personal Data and copies thereof to which this Agreement applies, including the Personal Data transferred by the Data Exporter; and, to the extent this is not possible,

(2) destroy such Personal Data and copies thereof, and certify to the Data Exporter in writing that it has done so; unless legislation imposed upon the Data Importer prevents it from returning or destroying all or parts of the Personal Data to which this Agreement applies, in which case the Data Importer informs the Data Exporter and undertakes to keep such Personal Data confidential and not actively process it anymore.

Upon termination of this Agreement, any other contract signed by the Data Importer and the Subprocessor for the purposes of processing and transferring Personal Data under this Agreement shall be terminated automatically. This, however, does not concern any other contract signed by the Data Exporter and Data Importer for other purposes.

§ 8 Miscellaneous

Each party will provide any court or supervisory agency, and the Data Exporter will provide any Person Affected, a copy or the content of this Agreement upon its request or if required by law. The rights and obligations of each party to this Agreement are without prejudice and notwithstanding to any other rights and obligations the parties may or may not have under other agreements. This Agreement does not regulate the consequences that the execution of a right and performance of an obligation under this Agreement may have under another relationship among the parties. Persons Affected may raise damages and other claims pursuant to the FADP relating to the transfer and/or processing of their Personal Data under this Agreement against either party. This Agreement may only be modified in writing. The parties shall not assign this Agreement or any rights or obligations hereunder to any Third Party without the prior written consent of the other party. This Agreement (and any Agreement signed by the Data Importer and any Subprocessor for the purposes of processing and transferring Personal Data under this Agreement) shall be governed by and construed in accordance with the substantive laws of Switzerland. Any dispute arising out of or in connection with this Agreement (or any subprocessor Agreement signed by the Data Importer and any Subprocessor for the purposes of processing and transferring Personal Data under this Agreement) or breach thereof, shall be exclusively settled by the ordinary courts at the seat of the Data Exporter in Switzerland.

ANNEX 1 TO THE SWISS TRANSBORDER DATA FLOW AGREEMENT

Description of the Transfer and Processing

1. Catalogue of Personal Data to be transferred and processed: Data Subjects: Employees, Employees of Third Parties, Business Partners, Suppliers, Communication Participants, Contractual Partners, Service Providers,

Consultants, Freelancers, Authorized Agents, Data Protection Officers Insured Persons, Patients, Medical Second Opinion Users.

2. Purpose(s) of the transfer and processing: Provision and use of SaaS Application(s).

3. Categories of the Persons Affected: Employees, Employees of Third Parties, Business Partners, Suppliers, Communication Participants, Contractual Partners, Service Providers, Consultants, Freelancers, Authorized Agents, Data Protection Officers, Contact Persons, Names, Address Data, Contact Information, Location data, Identification numbers, Online identifiers, Security identifiers, Other Identifiers, Insurance Numbers.

4. Persons who may access or receive the Personal Data: Employees of the Subscriber. Employees of the Provider and its subsidiaries. Subprocessors.

5. Data Protection registration information of the Data Exporter: None.

6. Additional useful information: None.

7. Contact Information for Data Protection Inquiries: Kristyn D'Angelo, MediGuide, 260 Chapman Road, Suite 203 Newark, DE 19702, USA; 302.425.5900; privacy@mediguide.com

APPENDIX 3 (STANDARD CONTRACTUAL CLAUSES FOR INTERNATIONAL TRANSFERS FROM CONTROLLERS TO PROCESSORS FOR THE UNITED KINGDOM)

Parties	
Name of the data exporting organisation:	Business Partner or Insurance Company
	(the data exporter")
	And
Name of the data importing organisation:	MediGuide International, LLC
Address	260 Chapman Road, Suite 203 Newark, DE 19702, USA
Telephone	302.425.5900
Email	privacy@mediguide.com
	(the data importer")
Clause 1. Definitions	For the purposes of the Clauses: (a)'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'Commissioner' shall have the same meaning as in the UK GDPR;
	(b) 'the data exporter' means the controller who transfers the personal data;
	(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;
	(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
	(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK;
	(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
Clause 2. Details of the transfer	The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.
Clause 3. Third-party beneficiary clause	
3(1)	The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
3(2)	The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3(3)	The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3(4)	The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.
Clause 4. Obligations of the data exporter	The data exporter agrees and warrants:
4(a)	that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the Commissioner) and does not violate the applicable data protection law;
4(b)	that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
4(c)	that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
4(d)	that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
4(e)	that it will ensure compliance with the security measures;
4(f)	that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;
4(g)	to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner if the data exporter decides to continue the transfer or to lift the suspension;
4(h)	to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
4(i)	that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses;
4(j)	that it will ensure compliance with Clause 4(a) to (i).
Clause 5. Obligations of the data importer1	The data importer agrees and warrants:
5(a)	to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend

	the transfer of data and/or terminate the contract;
5(b)	that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
5(c)	that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
5(d)	that it will promptly notify the data exporter about: (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation; (ii) any accidental or unauthorised access; and (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
5(e)	to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the Commissioner with regard to the processing of the data transferred;
5(f)	at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Commissioner;
5(g)	to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
5(h)	that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
5(i)	that the processing services by the sub-processor will be carried out in accordance with Clause 11;
5(j)	to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.
Clause 6. Liability	
6(1)	The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
6(2)	If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
6(3)	If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-

	processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.
Clause 7. Mediation and jurisdiction	
7(1)	The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject: (a) to refer the dispute to mediation, by an independent person or, where applicable, bythe Commissioner; (b) to refer the dispute to the UK courts.
7(2)	The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.
Clause 8. Cooperation with supervisory authorities	The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law.
8(2)	The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
8(3)	The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).
Clause 9. Governing law	The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established, namely England.
Clause 10. Variation of the contract	The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause.
Clause 11. Sub-processing	
11(1)	The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses2. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
11(2)	The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
11(3)	The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK where the exporter is established.

11(4)	The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Commissioner.
Clause 12. Obligation after termination	
12(1)	The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
12(2)	The data importer and the sub-processor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.
Indemnification	Liability The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred. Indemnification is contingent upon: (a) the data exporter promptly notifying the data importer of a claim; and (b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.
Priority of standard contractual clauses	The Standard Contractual Clauses take priority over any other agreement between the parties, whether entered into before or after the date these Clauses are entered into. Unless the Clauses are expressly referred to and expressly amended, the parties do not intend that any other agreement entered into by the parties, before or after the date the Clauses are entered into, will amend the terms or the effects of the Clauses, or limit any liability under the Clauses, and no term of any such other agreement should be read or interpreted as having that effect.

1 Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

2 This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.