Data Processing Agreement

This Data Processing Agreement ("**Agreement**", "**DPA**", "**Principal Agreement**") is an agreement between you and the entity you represent ("**Customer**", "**you**" or "**your**") and The VDOC under the Agreement ("**VDOC**", "**The VDOC**", "**Data Processor**"). Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 1 of this DPA.

This document seeks to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "Scope and Roles" This DPA applies when Customer Data is processed by VDOC. In this context, VDOC will act as "processor" to Customer who may act either as "controller" or "processor" with respect to Customer Data (as each term is defined in the GDPR).

1.1.2 "Agreement" means this Data Processing Agreement and all Schedules;

1.1.3 "Company Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.4 "Contracted Processor" means a Subprocessor;

1.1.5 "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.6 “EEA” means the European Economic Area;

1.1.7 “EU Data Protection Laws” means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.8 “GDPR” means EU General Data Protection Regulation 2016/679;

1.1.9 “Data Transfer” means:

1.1.9.1 a transfer of Customer Personal Data from the Company to a Contracted Processor; or

1.1.9.2 an onward transfer of Customer Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.10 “Services” means the services that we offer through our website (thevdoc.com)

1.1.11 “Subject Matter” also known as “Services” of this DPA consists of the appointment of the Processor by the Controller and the provision of instructions for the processing of personal data. The processing activities that the Processor shall carry out are strictly limited to those necessary to fulfil the scope of the main contract.

1.1.12 The Processor shall carry out one or more of the following processing activities on behalf of the Controller :

i. Processing payments and financial information (including refunds, subscriptions and membership fees)

ii. Providing you with the services you purchase (including club management, team information and player assignments, player management, portal access etc)

iii. Providing you with support including customer service, technical support and billing support

iv. Complying with laws, regulations and other compliance requirements (including complying with all local, state, federal and international laws, complying with anti-fraud regulations and money laundering regulations)

1.1.13 "Subprocessor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Customer in connection with the Agreement.

1.1.14 The Customer wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

1.1.15 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.2 **Compliance with Laws.** Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR

2. Customer Instructions

The parties agree that this DPA and the Agreement (including the provision of any goods and services) constitute Customer's documented instructions regarding VDOC's processing of Customer Data ("Documented Instructions").

VDOC will process Customer Data only in accordance with Documented Instructions. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between VDOC GDPR Data Processing Addendum 2 and Customer, including agreement on any additional fees payable by Customer to VDOC for carrying out such instructions.

Customer is entitled to terminate this DPA and the Agreement if VDOC declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA.

3 Processing of Customer Personal Data

3.1. Processor shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

3.1.2 not Process Company Personal Data other than on the relevant Customer's documented instructions.

3.2 The Customer instructs Processor to process Customer Personal Data.

4. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, VDOC shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

5.2 In assessing the appropriate level of security, VDOC shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

6. Security Breach Notification.

6.1 **Security Incident**. VDOC will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

6.2 **VDOC Assistance**. To assist Customer in relation to any personal data breach notifications Customer is required to make under the GDPR, VDOC will include in the notification under section 5.1(a) such information about the Security Incident as VDOC is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to VDOC, and any restrictions on disclosing the information, such as confidentiality.

6.3 **Unsuccessful Security Incidents**. Customer agrees that:

i. an unsuccessful Security Incident will not be subject to this Section 5. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of VDOC's equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and

ii. VDOC's obligation to report or respond to a Security Incident under this Section 5 is not and will not be construed as an acknowledgement by VDOC of any fault or liability of VDOC with respect to the Security Incident.

6.4 **Communication**. Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means VDOC selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information is delivered securely to VDOC.

7. Subprocessing

7.1. **Authorised Sub-processors**.

Customer agrees that VDOC may use sub-processors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf, such as providing support, marketing, website, seo or other such services that we provide.

Our lists sub-processors that are currently engaged by VDOC to carry out processing activities on Customer Data on behalf of Customer are listed below:

Third Party Entity	Location
Nubble Media	United Kingdom
1&1 IONOS	Germany

VDOC will update the list as applicable as and when new sub processors are on boarded.

If Customer objects to a new sub-processor, then without prejudice to any termination rights Customer has under the Agreement and subject to the applicable terms and conditions, the customer must email info@thevdoc.com without any undue delay. However the Customer acknowledges that we rely on our sub-processors in order to provide our services and that any objection may impact the level of service that we can provide to the Customer.

Except as set forth in this Section, or as Customer may otherwise authorize, VDOC will not permit any sub-processor to carry out processing activities on Customer Data on behalf of Customer.

7.2 **Sub-processor Obligations**.

Where VDOC authorises any sub-processor as described in Section 7.1:

i. VDOC will restrict the sub-processor's access to Customer Data only to what is necessary to maintain the Services or to provide the Services to Customer and any End Users in accordance with the Documentation and VDOC will prohibit the sub-processor from accessing Customer Data for any other purpose;

ii. VDOC will enter into a written agreement with the sub-processor and, to the extent that the sub-processor is performing the same data processing services that are being provided by VDOC under this DPA, VDOC will impose on the subprocessor the same contractual obligations that VDOC has under this DPA; and

iii. VDOC will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the sub-processors that cause VDOCto breach any of VDOC's obligations under this DPA.

8. Data Subject Rights

8.1 Taking into account the nature of the Processing, VDOC shall assist the Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

8.2 VDOC shall

8.2.1 promptly notify Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

8.2.2 ensure that it does not respond to that request except on the documented instructions of Customer or as required by Applicable Laws to which the VDOC is

subject, in which case VDOC shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before the Contracted Processor responds to the request.

9. Personal Data Breach

9.1 VDOC shall notify Customer without undue delay upon VDOC becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

9.2 VDOC shall co-operate with the Customer and take reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

10. Termination of the DPA.

This DPA shall continue in force until the termination of the Agreement (the "Termination Date").

11. Data Protection Impact Assessment

11.1 Data Protection Impact Assessment and Prior Consultation Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted

Processors.

12. Deletion or return of Company Personal Data

12.1 Customer may request to retrieve or delete Customer Data as described in the Documentation. Up to the Termination Date, Customer will continue to have the ability to request the retrieval or deletion Customer Data in accordance with this Section.

12.2 For 14 days following the Termination Date, Customer may retrieve or delete any remaining Customer Data from the Services, subject to the terms and conditions set out in the Agreement, unless prohibited by law or the order of a governmental or regulatory body or it could subject VDOC or its Affiliates to liability.

12.3 No later than the end of this 14 day period, Customer will close all VDOC accounts. VDOC will delete Customer Data when requested by Customer by using the Service controls provided for this purpose by VDOC.

13. Duties to Inform

Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by VDOC, VDOC will inform Customer without undue delay. VDOC will, without undue delay, notify all relevant parties in such action (e.g. creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer's property and area of responsibility and that Customer Data is at Customer's sole disposition.

14. Entire Agreement; Conflict

Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the parties including the Agreement and this

DPA, the terms of this DPA will control, except that the Service Terms will control over this DPA.

15. Audit rights

15.1 Subject to this section 15, VDOC shall make available to the Customer on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by the Contracted Processors.

15.2 Information and audit rights of the Customer only arise under section 15.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

16. Data Transfer

16.1 The Processor **undertakes** not to transfer any personal data abroad (i.e. outside the EEA territory) without the prior written authorization of the Data Controller. Any data transfer abroad, and processing activities thereof, will be carried out in strict compliance with the Controller's documented and specific instructions.

16.2 Such processing activities, which are hereby specifically authorized by the Controller, will take place in the states listed below and in strict compliance to the legal bases for data transfer set forth in articles. 45 and ss. GDPR, as applicable to each processing activity.

Third Party Entity	**Location**	**Legal Basis For Transfer**

The main legal bases for transfer pursuant to the GDPR are:

- an adequacy decision issued by the European Commission (Article 45 Paragraph 3 GDPR);
- binding corporate rules (Article 46 Paragraph 2 Point b in conjunction with Article 47 GDPR);
- Standard Contractual Clauses (Article 46 Paragraph 2 Points c and d GDPR);
- Codes of Conduct (Article 46 Paragraph 2 Point e in conjunction with Article 40 GDPR);
- Certification Mechanism. (Article 46 Paragraph 2 Point f in conjunction with Article 42 GDPR).

17. General Terms

17.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

a. disclosure is required by law;
b. the relevant information is already in the public domain.

17.2 Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified

from time to time by the Parties changing address.

18. Governing Law and Jurisdiction

18.1 This Agreement is governed by the laws of the State of Tennessee and is subject to the exclusive jurisdiction of the courts of the State of Tennessee.

18.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of the State of Tennessee, subject to possible appeal to the Federal court in Nashville.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the start of the contract "**Agreement**" between VDOC and the customer.

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity identified as "Customer" in the DPA

(the "data exporter")

And

The VDOC LLC

813 HARRIS DR

GALLATIN, TN 37066-3419 USA. (the "data importer")

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

a. 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

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 ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

d. 'the 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 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 Member State in which the data exporter is established;

f. 'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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

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.

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. The data subject can enforce against the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

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:

(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 relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(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;

(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;

(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;

(e) that it will ensure compliance with the security measures;

(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 providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(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 subprocessing 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;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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; and

(j) that it will ensure compliance with Clause 4(a) to (i)

Clause 5

Obligations of the data importer*

**Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, 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.*

The data importer agrees and warrants:

(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;

(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;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(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 authorized to do so;

(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 supervisory authority with regard to the processing of the data transferred;

(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 supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, 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;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

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 subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

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 subprocessor 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 subprocessor of its obligations in order to avoid its own liabilities.

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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

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, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is

established.

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

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, 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.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, 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 Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. 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.

2. The prior written contract between the data importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing 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 data exporter's data protection supervisory authority.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter

The data exporter is the entity identified as “Customer” in the DPA

Data importer

The data importer is The VDOC LLC “The Virtual DOC Coaching Platform”.

Data subjects

Data subjects are defined in Section 1.3 of the DPA.

Categories of data

The personal data is defined in Section 1.3 of the DPA.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The processing operations are defined in Section 1.3 of the DPA.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The technical and organizational security measures implemented by the data importer are as described in the DPA.