Willing & Able

SaaS Subscription and Data Processing Agreement

This SaaS Subscription and Data Processing Agreement (the "**Agreement**") is concluded between Willing & Able Licensing LLC, a company incorporated in the Republic of Georgia, having its registered office at Geronti Kikodze Street 11, 1st Floor, 0105 Tbilisi (the "**Provider**") and your company which is named with its details in the "Subscriber Address Details" in APPENDIX 1 (the "**Subscriber**").

1. Definitions

In the context of this Agreement, the following definitions and rules of interpretation shall apply:

"**Account**" means an account enabling one single named natural person to access and use the Hosted Services, including both administrator accounts and user accounts.

"Administrator Account" means an account enabling one single named natural person to administer the Hosted Services.

"**Agreement**" means this Agreement including any Appendices, and any amendments to this Agreement from time to time.

"**Appendix**" means any Appendix attached to the main body of this Agreement.

"**Business Day**" means any weekday other than a bank or public holiday in the Republic of Georgia.

"**Business Hours**" means the hours of 8:00 to 17:00 GMT +04:00 on a Business Day.

"**Charges**" means the subscription fee, rental fee or amount charged for the Account, Accounts and/or additional Services.

"**Content**" means any text, data or information, pictures, videos, infographics, graphics, graphs, and every other digital data that is transmitted, stored or processed by the Hosted Services or over the Platform.

"**Contractor**" or "**Business Partner**" means any company or person that act, based on an agreement or contract, on behalf of the Subscriber, Provider, FranchisePartner or SubscriptionPartner, or together with them.

"**Data Protection Laws**" means all applicable laws relating to the processing of Personal Data including but not limited to, while they are in force and applicable to Personal Data, the General Data Protection Regulation (Regulation (EU) 2016/679, GDPR) and/or national laws of EU Member States, the Swiss Federal Law on Data Protection (FDPA), UK GDPR and UK Data Protection Act (DPA 2018), California Consumer Privacy Act (CCPA), New York Privacy Act (S5642), Massachusetts Data Privacy Law (S-120), Hawaii Consumer Privacy Protection Act (SB 418), Maryland Online Consumer Protection Act (SB 613) and North Dakota Privacy Law (HB 1485).

"**Date of Subscription**" means the first or last day of subscription of a Hosted Service.

"**Documentation**" means the documentation for the Hosted Services produced by the Provider and delivered or made available by the Provider to the Subscriber.

"**Force Majeure Event**" means any event, or a series of related events, that is outside the reasonable control of the party affected, including but not limited to failures of the internet, servers, applications or any public telecommunications network, hacker attacks, denial of service attacks, virus or other malicious software attacks or infections, power failures, industrial disputes affecting any Partner or Third Party, changes to the law, disasters, explosions, hardware defects, fires, floods, riots, pandemics, diseases, terrorist attacks and wars.

"**FranchisePartner**" means a company that signed a Franchise Partner Agreement with the Provider and offers the Platform to its clients under its own brand or logo, or under the Providers trademark.

"**Free Subscriber**" means a Non-Profit Organisation that was approved by the Provider and that uses the Hosted Services without exception for Non-Profit purposes.

"**Hosted Services**" means SaaS Services which will be made available by the Provider to the Subscriber as a service via the internet in accordance with this Agreement.

"**Hosted Services Defect**" means any defect, error or bug in the Platform having an adverse effect or a material adverse effect on the appearance, operation, functionality or

performance of the Hosted Services, but excluding any defect, error or bug caused by or arising as a result of:

(a) any act or omission of the Subscriber or any person authorized by the Subscriber to use the Platform or Hosted Services;

(b) any use of the Platform or Hosted Services contrary to the Documentation, whether by the Subscriber or by any person authorized by the Subscriber;

(c) a failure of the Subscriber to perform or observe any of its obligations from this Agreement; or

(d) an incompatibility between the Platform or Hosted Services and any other system, network, application, program, hardware or software not specified as compatible in the Hosted Services Specification.

"**Hosted Services Specification**" means the specification for the Platform and Hosted Services set out in the Documentation.

"**Intellectual Property Rights**" means all intellectual property rights wherever in the world, whether registrable or unregistrable, registered or unregistered, including any application or right of application for such rights, including but not limited to copyright and related rights, database rights, confidential information, business secrets, trade secrets, specifications, know-how, inventions, technological innovations, discoveries, designs, formulas, processes, business methods, computer software, software code (including object code, intermediate code and source code), ideas, documents, drawings, creations, writings, illustrations, photographs, scientific and mathematical models, specifications, drawings, sketches, models, samples, business names, trade names, trademarks, service marks, passing off rights, unfair competition rights, patents, petty patents, utility models, wireframes, semi-conductor topography rights, rights in designs, rights on logos, any kind of materials defining, describing, or illustrating the SaaS Applications, commercial and operational information concerning the SaaS Applications and other information whether in hard copy or electronic form, as well as the functionalities designed for or implemented into the SaaS Applications."

"**Joint Controller**" means the natural or legal person, public authority, agency or other body which jointly with others, determines the purposes and means of the processing of Personal Data.

"**Maintenance Services**" means the general maintenance of the Platform and Hosted Services, and the application of Updates and Upgrades.

"**Mobile App**" means any mobile application that is made available by the Provider in relation to the Platform.

"**Partner**" means a company, person or integrator that is in a contractual relationship with the Provider.

"**Party**" or "**Parties**" shall mean the respective parties referred to in the section of the agreement.

"**Personal Data**" means any information relating to an identified or identifiable natural person (`**Data Subject'**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Platform**" means the Platform managed by the Provider and used by the Provider to provide the Hosted Services, including the application and database software for the Hosted Services, the system and server software used to provide the Hosted Services, and the computer hardware on which applications, databases, systems and server software are installed.

"**Services**" means any services that the Provider provides to the Subscriber, or has an obligation to provide to the Subscriber under this Agreement.

"Subscriber" means the natural or legal person, public authority, agency or other body which has an active Subscription to the Hosted Services, including the Free Subscriber. The term **"Subscriber"** may include, based on contractual circumstances and/or when referring to the conclusion of Standard Contractual Clauses all of the **"Subscribers Subsidiaries"**.

"**Subscriber Confidential Information**" means any information disclosed by the Subscriber that at the time of disclosure was marked as "confidential".

"**Subscriber Data**" means all data, works and materials, uploaded to or stored on the Platform by the Subscriber; transmitted by the Platform at the instigation of the Subscriber; supplied by the Subscriber to the Provider for uploading to, transmission by or storage on the Platform; or generated by the Platform as a result of the use of the Hosted Services by the Subscriber but excluding any Personal Data.

"Subscription" means an active Subscription to the Hosted Services, whether payed or free.

"**SubscriptionPartner**" means a company that signed a Subscription Partner Agreement with the Provider and offers the Platform to subscribers under its own brand or logo, or under the Providers trademark.

"**Subscription Period**" means one twelfth of the term.

"**Subsidiary**" means any company or person that is part of a group of companies to which the Subscriber, Provider, FranchisePartner or SubscriptionPartner are part.

"**Support Services**" means support in relation to the use of, and the identification and resolution of errors in the Hosted Services but shall not include the provision of Trainings.

"**Supported Web Browser**" means the current release of Google Chrome, or any other web browser that the Provider agrees in writing shall be supported.

"**Term**" means the subscription time or term of the Agreement.

"**Third Party**" means any company or person that is not a subsidiary or Contractor of the Provider, Subscriber, FranchisePartner or SubscriptionPartner.

"**Trial Period**" means the time before the Term begins and before any Charges are due.

"**Update**" means a hotfix, patch or minor version update to any Platform software.

"**Upgrade**" means a major version upgrade of any Platform software.

"**User**" means a natural person that has accepted the User Agreement.

"**User Agreement**" means the rules the Users need to comply with, and which is attached to this Agreement as APPENDIX 2.

2. Term and Trial Period

2.1 Hosted Services can be tested free of charge during the Trial Period that is mentioned on the respective website.

2.2 A Term is one year (365 days). The initial Term begins on Date of Subscription and after the Trial Period ends.

2.3 The Subscription will renew at the end of every Term for an additional Term (“Renewal Term”) at the prevailing list price unless the Agreement is terminated by either of the parties.

2.4 This Agreement is subject to termination in accordance with the clauses stipulated in this Agreement.

3. Hosted Services

3.1 The Provider shall ensure that the Platform will automatically generate Accounts for the Subscriber and for its Users, or that the Subscriber can create Accounts, and provide the Subscriber or its Users with login details for the Accounts.

3.2 The Provider hereby grants to the Subscriber a worldwide, revocable, nontransferable, non-exclusive user-based and/or terms-based license to use the Hosted Services by means of a supported Web Browser for internal business purposes of the Subscriber in accordance with the Documentation and during the Term.

3.3 The license granted by the Provider to the Subscriber under Clause 3.2 is subject to the following limitations:

(a) the Hosted Services may only be used by the officers, employees, agents, Subsidiaries and Contractors of the Subscriber;

(b) the Hosted Services may only be used by the named users providing that the Subscriber may change, add or remove a designated named ulause 10ser in accordance with the procedure set out by the Provider; and

(c) the Hosted Services shall not be used at any point in time by more than the number of concurrent users that was subscribed for, providing that the Subscriber may add or remove concurrent user licenses in accordance with the procedure set out by the Provider.

3.4 Except to the extent expressly permitted in this Agreement or required by law on a non-excludable basis, the license granted by the Provider to the Subscriber under Clause 3.2 is subject to the following prohibitions:

(a) the Subscriber shall not modify, create derivative works from, distribute, publicly display, publicly perform or sub-license its right to access and use the Hosted Services or the Hosted Services;

(b) the Subscriber shall not use the Hosted Service for service bureau or time-sharing purposes and the Subscriber shall not permit any unauthorized person to access, use or otherwise exploit the Hosted Services;

(c) the Subscriber shall not use the Hosted Services to provide services to or for Third Parties;

(d) the Subscriber shall not copy, republish or redistribute any Content or material from the Hosted Services;

(e) the Subscriber shall not reverse engineer, decompile, disassemble, or otherwise attempt to derive any of the Hosted Services source code or functionality;

(f) the Subscriber shall not make any alteration to the Platform, except as permitted by the Documentation; and

(g) the Subscriber shall not conduct or request that any person conduct any load testing or penetration testing on the Platform or Hosted Services without prior written consent of the Provider.

3.5 The Subscriber shall use reasonable endeavors, including reasonable security measures relating to Administrator Account access details, to ensure that no unauthorized person may gain access to the Hosted Services using an Administrator Account.

3.6 The Provider shall use all reasonable endeavors to maintain the availability of the Hosted Services to the Subscriber at the gateway between the public internet and the network of the hosting services provider for the Hosted Services but does not guarantee 100% availability.

3.7 For the avoidance of doubt, downtime caused directly or indirectly by any of the following shall not be considered a breach of this Agreement:

(a) a Force Majeure Event;

(b) a fault or failure of the internet or any public telecommunications network;

(c) a fault or failure of the Subscriber's or Providers computer systems, networks, servers or applications;

(d) any breach by the Subscriber of this Agreement; or

(e) scheduled maintenance carried out in accordance with this Agreement.

3.8 The Subscriber shall comply with APPENDIX 2 (User Agreement) and shall ensure that all persons using the Hosted Services with the authority of the Subscriber, on his behalf or by means of an Administrator Account will comply with APPENDIX 2 (User Agreement).

3.9 The Subscriber shall not use the Hosted Services in any way that causes, or may cause, damage to the Hosted Services or Platform or impairment of the availability or accessibility of the Hosted Services.

3.10 The Subscriber shall not use the Hosted Services

(a) in any way that is unlawful, illegal, fraudulent or harmful; or

(b) in connection with any unlawful, illegal, fraudulent or harmful purpose or activity.

3.11 For the avoidance of doubt, the Subscriber has no right to access the software code (including object code, intermediate code and source code) of the Platform, either during or after the Term.

3.12 The Provider may suspend the provision of the Hosted Services if any amount due to be paid by the Subscriber to the Provider under this Agreement is overdue, and the Provider has given to the Subscriber at least 7 days prior written notice, following the amount becoming overdue, of its intention to suspend the Hosted Services on this basis.

4. Maintenance Services

4.1 The Provider shall provide Maintenance Services to the Subscriber during an active subscription.

4.2 The Provider shall where practicable give to the Subscriber at least one Business Day prior written notice of scheduled Maintenance Services that are likely to affect the availability of the Hosted Services or are likely to have a material negative impact upon the Hosted Services, without prejudice to the Provider's other notice obligations under the main body of this Agreement.

4.3 The Provider shall give to the Subscriber at least one Business Day prior written notice of the application of an Upgrade to the Platform.

4.4 The Provider shall give to the Subscriber written notice of the application of any security Update to the Platform and at least one Business Day prior written notice of the application of any non-security Update to the Platform.

4.5 The Provider shall provide the Maintenance Services with reasonable skill and care.

4.6 The Provider may suspend the provision of the Maintenance Services if any amount due to be paid by the Subscriber to the Provider under this Agreement is overdue, and the Provider has given to the Subscriber at least 7 days written notice, following the amount becoming overdue, of its intention to suspend the Maintenance Services on this basis.

5. Support Services

5.1 The Provider shall provide Support Services to the Subscriber during an active subscription.

5.2 The Provider shall make available to the Subscriber a helpdesk in accordance with the provisions of the main body of this Agreement.

5.3 The Provider shall provide the Support Services with reasonable skill and care.

5.4 The Subscriber may use the helpdesk for the purposes of requesting and, where applicable, receiving the Support Services and the Subscriber shall not use the helpdesk for any other purpose.

5.5 The Provider shall respond to all requests for Support Services made by the Subscriber through the helpdesk.

5.6 The Provider may suspend the provision of the Support Services if any amount due to be paid by the Subscriber to the Provider under this Agreement is overdue, and the Provider has given to the Subscriber at least 7 days written notice, following the amount becoming overdue, of its intention to suspend the Support Services on this basis.

6. Subscriber Data

6.1 The Subscriber hereby grants to the Provider a non-exclusive free-of-charge license to use, copy, re-use, reproduce, store, distribute, publish, export, adapt, edit and translate the Subscriber Data to the extent reasonably required for the performance of the Provider's services or obligations and the exercise of the Provider's rights under this Agreement. The Subscriber grants to the Provider a non-exclusive free-of-charge right to license and/or sub-license the Subscriber Data except for Personal Data protected under Data Protection Laws. The Subscriber grants to the Provider a non-exclusive free-of-charge license to copy, use, reproduce, store, make publicly available and publish the Subscriber´s company logo (which stays the sole Intellectual Property or Trademark of the Subscriber) on websites and in marketing materials (flyers etc.) of the Provider in relations to its rights under this Agreement or marketing activities during the Term or an active subscription and afterwards, if used already before end of subscription.

6.2 The Subscriber warrants to the Provider that the Subscriber Data when used by the Provider in accordance with this Agreement will not infringe the Intellectual Property Rights or other legal rights of any person, and will not breach the provisions of any law, statute or regulation in any jurisdiction and under any applicable law.

6.3 The Subscriber shall create a back-up copy of the Subscriber Data at least daily. The Subscriber shall ensure that each such copy is sufficient to enable the Provider to restore the Hosted Services to the state they were in at the time the back-up was taken, and shall retain and securely store each such copy at least for one year or for the applicable statutory retention period.

6.4 Within the period of 7 Business Days following receipt of a written request from the Subscriber, the Provider shall use all reasonable endeavors to restore to the Platform the Subscriber Data stored in any back-up copy. The Subscriber acknowledges that this process will overwrite the Subscriber Data stored on the Platform prior to the restoration.

7. Mobile App

The parties acknowledge and agree that the use of the Mobile App, the parties' respective rights and obligations in relation to the Mobile App and any liabilities of either party arising out of the use of the Mobile App shall be governed by this SaaS Subscription and Data Processing Agreement.

8. No Assignment of Intellectual Property Rights

Nothing in this Agreement shall operate to assign or transfer any Intellectual Property Rights from the Provider to the Subscriber.

9. Charges

9.1 The Subscriber shall pay Charges to the Provider in accordance with this Agreement and/or the Subscription-Plans or Fees published on the respective website of the Provider.

9.2 If the Charges are based in whole or in part upon the time spent by the Provider performing the Services, the Provider shall obtain the Subscriber's written consent before performing Services that result in any estimate of time-based Charges given to the Subscriber being exceeded or any budget for time-based Charges agreed by the parties being exceeded; and unless the Subscriber agrees otherwise in writing, the Subscriber shall not be liable to pay to the Provider any Charges in respect of Services performed in breach of this Clause.

9.3 All amounts in or in relation to this Agreement and/or on pricing pages of the Provider’s websites are, unless the context requires otherwise, stated exclusive of any tax, tariff, duty, or assessment imposed by any government authority (national, state, provincial, or local), including without limitation any sales, use,

excise, ad valorem, property, withholding, or value added tax withheld at the source. If applicable law requires withholding or deduction of such taxes or duties, Subscriber shall separately pay Provider the withheld or deducted amount.

9.4 The Provider may elect to vary any element of the Charges by giving to the Subscriber not less than 30 days' written notice.

9.5. The Free Subscriber shall not pay Charges to the Provider.

10. Payments

10.1 The Provider shall issue invoices for the Charges to the Subscriber in advance of the period to which they relate.

10.2 The Subscriber shall pay the Charges mentioned in the order submitted by the Subscriber – and use the automated means published by the Provider on the Provider's website for its order submission – to the Provider for each Subscription Period, within 7 days following the issuance of the invoice for the said Subscription Period.

10.3 The Subscriber shall pay the Charges by supported online payment systems or wire transfer. The Subscriber may allow and/or authorize automatic online payments to the Provider by supported payment applications.

10.4 If the Subscriber does not pay any amount promptly due to the Provider under this Agreement in accordance to payment terms stipulated in this Agreement, the Provider may:

(a) charge the Subscriber interest on the overdue amount at the rate of 9% per annum from time to time (which interest will accrue daily until the date of actual payment and be compounded at the end of each calendar month); and

(b) suspend the account(s) of the Subscriber.

11. Provider's Confidentiality Obligations

11.1 The Provider shall

(a) keep the Subscriber Confidential Information strictly confidential;

(b) not disclose the Subscriber Confidential Information to any unauthorized person without the Subscriber's prior written consent; and

(c) use the same degree of care to protect the confidentiality of the Subscriber Confidential Information as the Provider uses to protect the Provider's own

Confidential Information of a similar nature, being at least a reasonable degree of care.

11.2 The Provider may disclose the Subscriber Confidential Information to the Provider's officers, employees, lawyers, professional advisers, insurers, agents and Contractors, and to other companies or persons who are bound by a written Agreement or professional obligation to protect the confidentiality of the Subscriber Confidential Information.

11.3 This Clause imposes no obligations upon the Provider with respect to Subscriber Confidential Information that:

(a) is known to the Provider before disclosure under this Agreement and is not subject to any other obligation of confidentiality;

(b) is or becomes publicly known through no act or default of the Provider;

(c) is obtained by the Provider from a Third Party in circumstances where the Provider has no reason to believe that there has been a breach of an obligation of confidentiality; or

(d) was or is licensed to the Provider.

11.4 The restrictions of this Clause do not apply to the extent that any Subscriber Confidential Information is required to be disclosed by any law or regulation, by any judicial or governmental order or request, or pursuant to disclosure requirements relating to the listing of the stock of the Provider on any recognized stock exchange.

11.5 The provisions of this Clause shall continue in force for a period of 3 years following the termination of this Agreement.

12. Data Protection

12.1 Each party shall comply with the Data Protection Laws with respect to processing of Personal Data.

12.2 The Subscriber warrants to the Provider that it has the legal right to disclose all Personal Data that it does in fact disclose to the Provider under or in connection with this Agreement or the use of the Hosted Services.

12.3 The Subscriber shall only supply to the Provider, and the Provider shall only process, in each case under or in relation to this Agreement, the Personal Data of Data Subjects falling within the categories and the types specified in APPENDIX 3 (Data Processing Information) and the Provider shall only process the Subscriber

Personal Data for the purposes specified in APPENDIX 3 (Data Processing Information).

12.4 The Provider shall process the Subscriber Personal Data during the contractual period and after that period only if the Provider needs to comply with an applicable statutory retention period, laws or regulations.

12.5 The Provider shall only process the Subscriber Personal Data on documented instructions of the Subscriber, including transfers of the Subscriber Personal Data to any place outside of the European Union or the European Economic Area, if applicable under laws or regulations that the Subscriber is subject to or need to comply with.

12.6 The Subscriber acknowledges that the Provider and Subsidiaries of the Provider are based outside the European Union (EU) and the European Economic Area (EEA) but understands that processing of Personal Data is mainly managed by using servers and sub-processors based within the EU or EEA.

12.7 The Provider shall promptly inform the Subscriber if, in the opinion of the Provider, an instruction of the Subscriber relating to the processing of the Subscriber Personal Data infringes Data Protection Laws.

12.8 Notwithstanding any other provision of this Agreement, the Provider may process the Subscriber Personal Data if and to the extent that the Provider is required to do so by applicable law. In such case, the Provider shall inform the Subscriber of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

12.9 The Provider shall ensure that employees authorized to process the Subscriber Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

12.10 The Provider and the Subscriber shall each implement appropriate Technical and Organizational Measures to ensure an appropriate level of security for the Subscriber Personal Data, including those measures specified for the Provider in APPENDIX 3 (Data Processing Information).

12.11 The Provider shall not engage any Third Party to process the Subscriber Personal Data without the prior specific or general written authorization of the Subscriber. As at the Effective Date, the Provider is hereby authorized by the Subscriber to engage sub-processors with respect to Subscriber Personal Data (general written authorization). The Provider shall inform the Subscriber at least 30 days in advance, by means of public announcement on the website of the Provider, about

any intended changes concerning the addition or replacement of any processors, and if the Subscriber objects to any such changes before their implementation, then the Subscriber or the Provider may terminate this Agreement with a 7 days written notice, providing that such notice shall be given within the period of 30 days after the initial public announcement on the website of the Provider. The Provider shall ensure that each processor is subject to equivalent or similar contractual obligations as those imposed on the Provider by this Agreement.

12.12 The Provider shall, insofar as possible and taking into account the nature and scope of processing, implement appropriate Technical and Organizational Measures to assist the Subscriber with the fulfilment of the Subscriber's obligation to respond to requests exercising Data Subject's rights under Data Protection Laws.

12.13 The Provider shall assist the Subscriber in ensuring compliance with the obligations relating to the security of processing of Personal Data, the notification of Personal Data breaches to the supervisory authority, the communication of Personal Data breaches to the Data Subject, Data Protection Impact Assessments and prior consultation in relation to high-risk processing under the Data Protection Laws. The Provider shall report any Personal Data breach relating to the Subscriber Personal Data to the Subscriber without undue delay following the Provider becoming aware of the breach. The Provider may charge the Subscriber at its standard time-based charging rates for any work performed by the Provider at the request of the Subscriber pursuant to this Clause.

12.14 The Provider shall make available to the Subscriber all information necessary to demonstrate compliance of the Provider with its obligations under Data Protection Laws. The Provider may charge the Subscriber at its standard time-based charging rates for any work performed by the Provider at the request of the Subscriber pursuant to this Clause.

12.15 The Provider shall, at the choice of the Subscriber, delete or return all of the Subscriber Personal Data to the Subscriber after the provision of services relating to the processing, and shall delete existing copies saved to the extent that applicable law does not require storage of the Personal Data.

12.16 The Provider shall allow for and contribute to audits, including inspections, conducted by the Subscriber or another auditor mandated by the Subscriber in respect of the compliance of the Provider's processing of Subscriber Personal Data with Data Protection Laws and this Agreement. The Provider may charge the Subscriber at its standard time-based charging rates for any work performed by the Provider at the request of the Subscriber pursuant to this Clause.

12.17 If any changes or prospective changes to the Data Protection Laws result or can result in one or both parties not complying with Data Protection Laws in relation to processing of Personal Data carried out under this Agreement, then the parties shall use their best endeavors promptly to agree such variations to this Agreement as may be necessary to remedy such non-compliance.

12.18 If the Provider is based outside of the European Union or the European Economic Area, the respective EU Standard Contractual Clauses (APPENDIX 4, SECTIONS B, C, D and/or E) shall govern the relationship between the Provider and the Subscriber 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 applicability, apply automatically in place of the EU Standard Contractual Clauses to EU Personal Data Processing between the Provider and the Subscriber, 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.

12.19 If the Provider is based outside of Switzerland, the Swiss Transborder Data Flow Agreement (APPENDIX 5) shall govern the relationship between the Provider (PARTY 2) and the Subscriber (PARTY 1) 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 applicability, apply automatically in place of the Swiss Transborder Data Flow Agreement to Swiss Personal Data Processing between the Provider and the Subscriber, 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.

12.19 If the Provider is based outside of the United Kingdom, the Standard Contractual Clauses for International Transfers from Controllers to Processors for the United

Kingdom (APPENDIX 8) shall govern the relationship between the Provider (PARTY 2) and the Subscriber (PARTY 1) 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 applicability, 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 the Provider and the Subscriber, 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.

13. Warranties

13.1 The Provider warrants to the Subscriber and/or its Subsidiary and/or its User that the Provider has the legal right and authority to enter into this Agreement and to perform its obligations under this Agreement.

13.2 The Subscriber and/or its Subsidiary warrants to the Provider that the Subscriber has the legal right and authority to enter into this Agreement and to perform its obligations under this Agreement.

13.3 The Subscriber and/or its Subsidiary warrants to the Provider that every User has the legal right and authority to enter into the User Agreement and to perform its obligations under the User Agreement, and is of full age and competent under the law of the country where he or she resides.

13.4 All of the parties' warranties and representations in respect of the subject matter of this Agreement are expressly set out in this Agreement. To the maximum extent permitted by applicable law, no other warranties or representations concerning the subject matter of this Agreement will be implied into this Agreement or any related contract.

14. Acknowledgements and Warranty Limitations

14.1 The Subscriber acknowledges that Hosted Services are never wholly free from defects, errors and bugs, and subject to the other provisions of this Agreement,

the Provider gives no warranty or representation that the Hosted Services will be wholly free from defects, errors and bugs.

14.2 The Subscriber acknowledges that Hosted Services are never entirely free from security vulnerabilities, and subject to the other provisions of this Agreement, the Provider gives no warranty or representation that the Hosted Services will be entirely secure.

14.3 The Subscriber acknowledges that the Hosted Services are designed to be compatible only with that software, browsers and those systems mentioned on the Provider's website; and the Provider does not warrant or represent that the Hosted Services will be compatible with any other software, browsers or systems.

14.4 The Subscriber acknowledges that the Provider will not provide any legal, financial, accountancy or taxation advice under this Agreement or in relation to the Hosted Services; and, except to the extent expressly provided otherwise in this Agreement, the Provider does not warrant or represent that the Hosted Services or the use of the Hosted Services by the Subscriber will not give rise to any legal liability on the part of the Subscriber or any other person.

15. Limitations and Exclusions of Liability

15.1 Nothing in this Agreement will:

(a) limit or exclude any liability for death or personal injury resulting from negligence;

(b) limit or exclude any liability for fraud or fraudulent misrepresentation;

(c) limit any liabilities in any way that is not permitted under applicable law; or

(d) exclude any liabilities that may not be excluded under applicable law.

15.2 The limitations and exclusions of liability set out in this clause and elsewhere in this Agreement:

(a) are subject to this clause; and

(b) govern all liabilities arising under this Agreement or relating to the subject matter of this Agreement, including liabilities arising in contract, in tort (including negligence) and for breach of statutory duty, except to the extent expressly provided otherwise in this Agreement.

15.3 Neither party shall be liable to the other party in respect of any losses arising out of a Force Majeure Event.

15.4 Neither party shall be liable to the other party in respect of any loss of profits or anticipated savings.

15.5 Neither party shall be liable to the other party in respect of any loss of revenue or income.

15.6 Neither party shall be liable to the other party in respect of any loss of use or production.

15.7 Neither party shall be liable to the other party in respect of any loss of business, contracts or opportunities.

15.8 Neither party shall be liable to the other party in respect of any loss or corruption of any data, database or software.

15.9 Neither party shall be liable to the other party in respect of any special, indirect or consequential loss or damage.

15.10 The liability of each party to the other party under this Agreement in respect of any event or series of related events shall not exceed the total amount paid and payable by the Subscriber to the Provider under this Agreement in the 3 month period preceding the commencement of the event or events.

15.11 The aggregate liability of each party to the other party under this Agreement shall not exceed the total amount paid and payable by the Subscriber to the Provider under this Agreement.

16. Force Majeure Event

16.1 If a Force Majeure Event gives rise to a failure or delay in either party performing any obligation under this Agreement (other than any obligation to make a payment), that obligation will be suspended for the duration of the Force Majeure Event.

16.2 A party that becomes aware of a Force Majeure Event which gives rise to, or which is likely to give rise to, any failure or delay in that party performing any obligation under this Agreement, shall

(a) notify the other party; and

(b) inform the other party of the period for which it is estimated that such failure or delay will continue.

16.3 A party whose performance of its obligations under this Agreement is affected by a Force Majeure Event shall take reasonable steps to mitigate the effects of the Force Majeure Event.

17. Termination

17.1 Either party may terminate this Agreement by giving to the other party at least 90 days prior written notice before the end of every Term.

17.2 Either party may terminate this Agreement immediately and unilaterally by giving written notice of termination to the other party if the other party commits a material breach of this Agreement.

17.3 Either party may terminate this Agreement immediately and unilaterally by giving written notice of termination to the other party if:

(a) the other party:

(i) is dissolved;

(ii) ceases to conduct all (or substantially all) of its business;

(iii) is or becomes unable to pay the Charges as they fall due, in accordance to payment terms stipulated in this Agreement;

(iv) is or becomes insolvent or is declared insolvent; or

(v) convenes a meeting or makes or proposes to make any arrangement or composition with its creditors;

(b) an administrator, administrative receiver, liquidator, receiver, trustee, manager or similar is appointed over any of the assets of the other party; or

(c) an order is made for the winding up of the other party, or the other party passes a resolution for its winding up, other than for the purpose of a solvent company reorganization where the resulting entity will assume all the obligations of the other party under this Agreement.

18. Effects of Termination

18.1 Upon the termination of this Agreement, all of the provisions of this Agreement shall cease to have effect, save that the following provisions of this Agreement shall survive and continue to have effect, in accordance with their express terms or otherwise indefinitely: Clauses 1, 3.11, 6.1, 6.2, 8, 9, 10.2, 10.4, 11, 12, 15, 18, 21, 29 and 30.

18.2 Except to the extent that this Agreement expressly provides otherwise, the termination of this Agreement shall not affect the accrued rights of either party.

18.3 Within 30 days following the termination of this Agreement for any reason

(a) the Subscriber shall pay to the Provider any Charges in respect of Services provided to the Subscriber before the termination of this Agreement without prejudice to the Provider's other legal rights; and

(b) the Provider shall refund to the Subscriber any Charges paid by the Subscriber to the Provider in respect of Services that were to be provided to the Subscriber after the termination of this Agreement without prejudice to the Provider's other legal rights.

19. Notices

19.1 Any notice from one party to the other party under this Agreement shall be given by one of the following methods, and using the relevant contact details:

(a) delivered personally or sent by courier, in which case the notice shall be deemed to be received upon delivery; or

(b) sent by recorded signed-for post, in which case the notice shall be deemed to be received 10 Business Days following posting; or

(c) sent by e-mail to the Subscribers or Providers general e-mail-address, in which case the notice shall be deemed to be received 3 Business Days following the sending of the e-mail; or

(d) in case of general notices to more or all Subscribers of the Provider, published on the website of the Provider, in which case the notice shall be deemed to be received 30 days after its publication,

providing that, if the stated time of deemed receipt is not within Business Hours, then the time of deemed receipt shall be when Business Hours next begin after the stated time.

19.2 The Provider's contact details for notices under this Clause are as follows:

Willing & Able Operations LLC

Shop 141, Building 25, 1st Floor

Norashen, Ajapnyak

Yerevan, 0036

Republic of Armenia

E-Mail: info@willing-able.com

19.3 The addressee and contact details set out may be updated from time to time.

20. Subcontracting by the Provider

20.1 Subject to any express restrictions elsewhere in this Agreement, the Provider may subcontract any of its obligations under this Agreement.

20.2 The Provider shall remain responsible to the Subscriber for the performance of any subcontracted obligations.

20.3 Notwithstanding the provisions of this Clause but subject to any other provision of this Agreement, the Subscriber acknowledges and agrees that the Provider may subcontract to any reputable Contractor hosting business the hosting of the Platform and the provision of services in relation to the support and maintenance of elements of the Platform.

21. Arbitration Clause

21.1 All disputes arising out of or in connection with this SaaS Subscription and Data Processing Agreement, the User Agreement (accepted by Users of the Subscriber), or any other agreement between the parties, including Data Processing Agreements and Standard Contractual Clauses, or their validity, shall be finally settled in accordance with the Arbitration Rules of the German Arbitration Institute (DIS) without recourse to the ordinary courts of law.

21.2 The arbitral tribunal shall be comprised of a sole arbitrator.

21.3 The seat of the arbitration shall be in Munich, Germany. For economic reasons, both parties agree to online arbitration and will use any online meeting system provided by the arbitrator.

21.4 The language of the arbitration shall be German.

21.5 The rules of law applicable to the merits shall be German Law.

21.6 Provider and Subscriber jointly nominate the following Attorney at Law to act as the arbitrator:

Ulrich Baumann

c/o CORPLEGAL

Prinzregentenstr. 22

80538 Munich (Germany)

Telephone: +49 (0)89 / 23 23 73 6-0

Telefax: +49 (0)89 / 23 23 73 6-91

E-Mail: mail@corplegal.global

21.7 The arbitrator can assign the case to another arbitrator without obtaining consent of the parties.

21.8 The arbitrator and contact details set out may be updated from time to time. The Subscriber hereby agrees that the Provider may change the arbitrator on its own discretion, if such changes are published as a general notice and will apply to all Subscribers. Clause 19.1 (d) is applicable. The Provider may transfer pending cases from the old to the new arbitrator on its own discretion.

22. Integrated Works

The web applications and software products of the Provider may contain materials of all kind, for example pictures, texts, source codes, functions, applications, services, programming languages and programming frameworks, or they work on servers and/or operate on operating systems or they use Third Party services that are licensed under one of the following terms:

a) Apache Software License (Apache):

Version 2: http://www.apache.org/licenses/LICENSE-2.0.txt

Version 1.1: http://www.apache.org/licenses/LICENSE-1.1

b) Server-Side Public License (MongoDB)

Version 1: https://www.mongodb.com/licensing/server-side-public-license

c) GNU General Public License (GPL):

Version 3: https://www.gnu.org/licenses/gpl-3.0.html

Version 2: https://www.gnu.org/licenses/gpl-2.0.html

Version 1: https://www.gnu.org/licenses/gpl-1.0.html

d) GNU Lesser General Public License (LGPL):

Version 3: https://www.gnu.org/licenses/lgpl-3.0.html

Version 2.1: https://www.gnu.org/licenses/lgpl-2.1.html

e) GNU Affero General Public License (AGPL):

Version 3: https://www.gnu.org/licenses/agpl-3.0.html

f) GNU Free Documentation License (FDL):

Version 1.3: https://www.gnu.org/licenses/lfdl-1.3.html

Version 1.2: https://www.gnu.org/licenses/fdl-1.2.html

Version 1.1: https://www.gnu.org/licenses/fdl-1.1.html

g) CC License:

Creative Commons: https://creativecommons.org/licenses/

h) EU Public License (EUPL):

European Union Public License (EUPL): https://eur-lex.europa.eu/

i) Python:

License of Python: https://docs.python.org/3/license.html

j) MIT License (e.g. React, Ruby on Rails, Laravel):

MIT License: https://opensource.org/licenses/mit-license.php

k) Mozilla:

Mozilla Public License: https://www.mozilla.org/en-US/MPL/

l) PHP:

PHP License: https://www.php.net/license/index.php

The Subscriber agrees to comply with the respective license. We hereby recognize the work of the respective developers and copyright owners. Thanks for your contribution!

23. Partners and Marketing

The Provider conducts its own marketing activities and works with Partners to offer a variety of deals, products and services (e.g. discounts etc.). The Subscriber instruct the Provider to find deals, products and services for the User and to inform him about these deals, products and services by email, SMS or in other ways (e.g. a method used by a User to sign-up or verify an account). In order to notify the User and provide him with the information needed to participate, as instructed by the Subscriber under the terms of this clause, the Provider may process the Personal Data of the User in order to send or publish such information. Without being able to process the Personal Data of the Users for this purpose, the Provider would not be able to perform the services agreed to with the Subscriber. The User agrees to such processing of its Personal Data by accepting the User Agreement. Therefore, the processing of such Personal Data is required to carry out the services of the Provider to which the legal basis is Art. 6 (1) (b) and Art. 6 (1) (f) GDPR or similar provisions from other Data Protection Laws.

24. Interpretation

24.1 In this Agreement, a reference to a law, regulation, statute or statutory provision includes a reference to:

(a) that law, regulation, statute or statutory provision as modified, consolidated and/or re-enacted from time to time; and

(b) any subordinate legislation made under that law, regulation, statute or statutory provision.

24.2 The Clause headings shall not affect the interpretation of this Agreement.

24.3 References in this Agreement to "calendar months" are to the 12 named periods (January, February and so on) into which a year is divided.

24.4 In this Agreement, general words shall not be given a restrictive interpretation by reason of being preceded or followed by words indicating a particular class of acts, matters or things.

25. SubscriptionPartner and FranchisePartner, Joint Controllership

25.1 If the Subscriber concluded this Agreement over a proxy or website of another party (SubscriptionPartner or FranchisePartner) that other party shall not become a party to this agreement.

25.2 SubscriptionPartners or FranchisePartners do not host the Platform, the Account, Subscriber Data or Personal Data saved on or in relation to the Platform. If the Subscriber has subscribed by a website operated or published by a SubscriptionPartner or FranchisePartner, that party has restricted access to Accounts, Subscriber Data and/or Personal Data for purposes of Support, Services, Invoicing and Verification. For such processing operations, Provider and SubscriptionPartner or Provider and FranchisePartner act together as Joint Controllers (Art. 26 GDPR).

25.3 The "Joint Controllership Agreement between the Provider and FranchisePartner or Subscription Partner" (APPENDIX 6) applies to the relationship between the Provider and the FranchisePartner or the relationship between the Provider and the SubscriptionPartner, and therefore also to the Subscriber, if the Subscriber had received its Account and/or access to the Platform, Hosted Services, Services or Support Services by or from a FranchisePartner or SubscriptionPartner.

26. Purchase and Sale of the Provider or Purchase and Sale of Platform

The Subscriber hereby agrees with the transfer of this entire Agreement, including Rights and Obligations, Account, Charges, Documentation, Hosted Services, Intellectual Property Rights, Maintenance Services, Mobile App, Personal Data, Platform, Services, Subscriber Confidential Information, Subscriber Data, Support Services, Term and every other Functionality, Source Code, Data or Database in relation to the Platform, in whole or in part, in case the Provider concludes a sale of business, shares or stocks, applications or other assets, transfer or restructure of its business, that may or may not result in the performance of this Agreement under the same or a new Provider, legal form or company name.

27. Execution

The parties have indicated their acceptance of this Agreement by executing it online.

28. Agreements with Contractors, Business Partners and Subsidiaries of the Subscriber (EU and EEA, UK, and Switzerland)

28.1 If the Subscriber or a Subscribers Subsidiary provides an Account, access to the Platform, Hosted Services, Services or Support Services to a Contractor or Business Partner,

a) and both, the Subscriber and Contractor or Business Partner are based in the European Union or the European Economic Area, these Parties conclude, by acceptance of this SaaS Subscription and Data Processing Agreement and/or the User Agreement, the "STANDARD CONTRACTUAL CLAUSES 2021/915 BETWEEN CONTROLLERS AND PROCESSORS" (APPENDIX 4, SECTION A) with each other;

b) and both, the Subscriber (PARTY 1) and Contractor or Business Partner (PARTY 2) are based in Switzerland, these Parties conclude, by acceptance of this SaaS Subscription and Data Processing Agreement and/or the User Agreement, the "Swiss Transborder Data Flow Agreement" (APPENDIX 5) with each other, which should be interpreted in accordance with Swiss FDPA and for country internal data flows;

c) and both, the Subscriber and Contractor or Business Partner are based in the United Kingdom, these Parties conclude, by acceptance of this SaaS Subscription and Data Processing Agreement and/or the User Agreement, the "STANDARD CONTRACTUAL CLAUSES 2021/915 BETWEEN CONTROLLERS AND

PROCESSORS" (APPENDIX 4, SECTION A) with each other, which should be interpreted in accordance with UK GDPR and DPA 2018 and be valid until the UK government has published new Standard Contractual Clauses for the United Kingdom and such are incorporated into this Agreement;

d) and if the Contractor or Business Partner is based outside the European Union or European Economic Area, these Parties conclude, by acceptance of this SaaS Subscription and Data Processing Agreement and/or the User Agreement, the applicable "Standard Contractual Clauses" (APPENDIX 4, SECTION B, C, D and/or E) with each other;

e) and if the Subscriber (PARTY 1) is based in Switzerland but the Contractor or Business Partner (PARTY 2) is not, these Parties conclude, by acceptance of this SaaS Subscription and Data Processing Agreement and/or the User Agreement, the "Swiss Transborder Data Flow Agreement" (APPENDIX 5) with each other; and/or

f) and if the Subscriber (PARTY 1) is based in the United Kingdom but the Contractor or Business Partner (PARTY 2) is not, these Parties conclude, by acceptance of this SaaS Subscription and Data Processing Agreement and/or the User Agreement, the Standard Contractual Clauses for "International Transfers from Controllers to Processors for the United Kingdom" (APPENDIX 8) with each other.

28.7 The EU Standard Contractual Clauses (APPENDIX 4, SECTION A, B, C, D and/or E) shall govern the relationship between all parties that accepted this SaaS Subscription and Data Processing Agreement and/or the User Agreement 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 legislator (collectively, the "New EU Laws"), wherein such New EU Laws shall, from the date of their applicability, apply automatically in place of the EU Standard Contractual Clauses to EU Personal Data Processing between the Parties, unless either party notifies one or more other parties in writing of its objection thereto within 30 days from the official publication date of the New EU Laws.

28.8 If the Contractor is based outside of Switzerland, the Swiss Transborder Data Flow Agreement (APPENDIX 5) shall govern the relationship between the Subscriber and

the Contractor 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 are superseded by any new laws or regulations enacted by the Swiss legislator (collectively, the "New Swiss Laws"), wherein such New Swiss Laws shall, from the date of their applicability, apply automatically in place of the Swiss Transborder Data Flow Agreement to Swiss Personal Data Processing between the Parties, unless either party notifies one or more other parties in writing of its objection thereto within 30 days from the official publication date of the New Swiss Laws.

28.9 If the Contractor is based outside of the United Kingdom, the Standard Contractual Clauses for International Transfers from Controllers to Processors for the United Kingdom (APPENDIX 8) shall govern the relationship between the Subscriber and the Contractor 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 Processors for the United Kingdom are superseded by any new laws or regulations enacted by the UK legislator (collectively, the "New UK Laws"), wherein such New UK Laws shall, from the date of their applicability, 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 the Parties, unless either party notifies one or more other parties in writing of its objection thereto within 30 days from the official publication date of the New UK Laws.

28.10 If the Subscriber provides an Account, access to the Platform, Hosted Services, Services or Support Services to a Subsidiary, these Parties conclude, by acceptance of this SaaS Subscription and Data Processing Agreement and/or the User Agreement, the "Joint Controllership Agreement between the Subscriber and a Subsidiary in accordance with Art. 26 GDPR" (APPENDIX 7) and/or the applicable "Standard Contractual Clauses" (APPENDIX 4, SECTION A, B, C, D and/or E) and/or the Swiss Transborder Data Flow Agreement (APPENDIX 5) and/or the

Standard Contractual Clauses for International Transfers from Controllers to Processors for the United Kingdom (APPENDIX 8) with each other.

29. Factoring

29.1 The Provider may sell Receivables to a Third Party. The Subscriber grants permission to the Provider to disclose the provisions of this Agreement to purchasers and prospective purchasers of Receivables, or their Affiliates and their respective agents, attorneys, auditors, rating agencies, and other advisors.

30. Severability Clause and General Provisions

30.1 If any provision of this Agreement is determined by any court or other competent authority to be unlawful and/or unenforceable, the other provisions of this Agreement will continue in effect. If any unlawful and/or unenforceable provision would be lawful or enforceable if part of it were deleted, that part will be deemed to be deleted, and the rest of the provision will continue in effect, unless that would contradict the clear intention of the parties, in which case the entirety of the relevant provision will be deemed to be deleted.

30.2 If the parties disagree on a provision that is to be supplemented and necessary, they shall appeal to the Arbitral Tribunal.

30.3 This Agreement may not be varied except by a written document signed by or on behalf of each of the parties.

30.4 Neither party may without the prior written consent of the other party assign, transfer, charge, license or otherwise deal in or dispose of any contractual rights or obligations under this Agreement, exempt otherwise agreed on in this Agreement.

30.5 This Agreement is made for the benefit of the parties and is not intended to benefit any Third Party or be enforceable by any Third Party. The rights of the parties to terminate, rescind, or agree any amendment, waiver, variation or settlement under or relating to this Agreement are not subject to the consent of any Third Party.

30.6 This Agreement and its Appendices shall constitute the entire Agreement between the parties in relation to the subject matter of this Agreement, and shall supersede all previous agreements, arrangements and understandings between the parties in respect of that subject matter.

APPENDIX 1 (Subscriber Address Details)

Company Name: _____

Address: _____

ZIP Code: _____

City: _____

Country: _____

State: _____

Phone: _____

Fax: _____

E-Mail: _____

Website: _____

APPENDIX 2 (User Agreement)

This User Agreement is concluded between the Willing & Able Licensing LLC, Geronti Kikodze Street 11, 1st Floor, 0105 Tbilisi, Republic of Georgia and you as a natural person. It contains general rules and obligations you need to comply with when using our SaaS Applications.

1. General Terms

1.1 This User Agreement sets out the rules governing:

(a) the use of the Account, Platform or Hosted Services (in the following "Hosted Services"); and

(b) the transmission, storage and processing of Content and Personal Data by you, or by any person on your behalf, when using the Hosted Services.

1.2 References in this User Agreement to "you" and/or to the Subscriber for the Hosted Services and/or any individual user of the Hosted Services should mean you and shall be construed accordingly; references to "us" or the "Provider" means the Willing & Able Licensing LLC and shall be construed accordingly.

1.3 We will ask for your acceptance to the terms of this User Agreement before you first register, upload or submit any Content or otherwise use the Hosted Services. By continuously using the Hosted Services, you continuously agree to the rules set out in this User Agreement.

1.4 You shall be at least of age in your jurisdiction to use the Hosted Services; and by using the Hosted Services, you warrant and represent to us that you are of age and fully competent under the law in your jurisdiction.

2. General Usage Rules

2.1 You shall not use the Hosted Services in any way that causes, or may cause, damage to the Hosted Services or impairment of the availability or accessibility of the Hosted Services.

2.2 You shall not use the Hosted Services:

(a) in any way that is unlawful, illegal, fraudulent, deceptive or harmful;

(b) in connection with any unlawful, illegal, fraudulent, deceptive or harmful purpose or activity.

2.3 You shall ensure that all Content complies with the provisions of this User Agreement.

3. Unlawful Content

3.1 Content shall not be illegal or unlawful, shall not infringe any person's legal rights, and shall not be capable of giving rise to legal action against any person, in each case in any jurisdiction and under any applicable law.

3.2 Your Content, and the use of Content by us in any manner licensed or otherwise authorized by you, shall not

(a) be libelous or maliciously false;

(b) be obscene or indecent;

(c) infringe any copyright, moral right, database right, trademark right, design right, right in passing off, or other Intellectual Property Rights;

(d) infringe any right of confidence, right of privacy or right under Data Protection Laws;

(e) constitute negligent advice or contain any negligent statement;

(f) constitute an incitement to commit a crime, instructions for the commission of a crime or the promotion of criminal activity;

(g) be in contempt of any court, or in breach of any court order;

(h) constitute a breach of racial or religious hatred or discrimination legislation;

(i) be blasphemous;

(j) constitute a breach of official secrets or business secrets legislation; or

(k) constitute a breach of any contractual obligation owed to any person.

3.3 You shall ensure that Content is not and has never been the subject of any threatened or actual legal proceedings or other similar complaint.

4. Graphic Material

4.1 Content shall be appropriate for all persons who have access to or are likely to access the Content in question, and in particular for children.

4.2 Content shall not depict violence in an explicit, graphic or gratuitous manner.

4.3 Content shall not be pornographic or sexually explicit.

5. Factual Accuracy

5.1 Content shall not be untrue, false, inaccurate or misleading.

5.2 Statements of fact contained in Content and relating to persons (legal or natural) shall be true; and statements of opinion contained in Content and relating to persons (legal or natural) shall be reasonable, be honestly held and indicate the basis of the opinion.

6. Negligent Advice

6.1 Content shall not consist of or contain any legal, financial, investment, taxation, accountancy, medical or other professional advice, and you shall not use the Hosted Services to provide any legal, financial, investment, taxation, accountancy, medical or other professional advisory services unless you are a member of a special profession which allow you to use or publish such Content (e.g. lawyer, solicitor, medical doctor, tax advisor etc.).

6.2 Content shall not consist of or contain any advice, instructions or other information that may be acted upon and could, if acted upon, cause death, illness or personal injury, damage to property, or any other loss or damage.

7. Etiquette

7.1 Content shall be appropriate, civil and tasteful, and in accordance with generally accepted standards of etiquette and behavior on the internet.

7.2 Content shall not be offensive, deceptive, threatening, abusive, harassing, menacing, hateful, discriminatory or inflammatory.

7.3 Content shall not be liable to cause annoyance, inconvenience or needless anxiety.

7.4 You shall not use the Hosted Services to send any hostile communication or any communication intended to insult, harass, threaten, or defame any person or entity, including such communications directed at a particular person or group of people.

7.5 You shall not use the Hosted Services for the purpose of deliberately upsetting or offending others.

7.6 You shall not unnecessarily flood the Hosted Services with material relating to a particular subject or subject area, whether alone or in conjunction with others.

7.7 You shall ensure that Content does not duplicate other Content available through the Hosted Services.

7.8 You shall ensure that Content is appropriately categorized and organized.

7.9 You should use appropriate and informative titles for all Content.

7.10 You shall always be courteous and polite to other users of the Hosted Services.

8. Marketing and Spam

8.1 You shall not without our written permission use the Hosted Services for any purpose relating to marketing, advertising, promotion, sale or supply of any product, service or commercial offering, unless the Hosted Services are intended only or mainly for this purpose.

8.2 Content shall not constitute or contain spam, and you shall not use the Hosted Services to store or transmit spam, which for these purposes shall include all unlawful marketing communications and unsolicited commercial communications.

8.3 You shall not send any spam or other marketing communications to any person using any email address or other contact details made available through the Hosted Services or that you find using the Hosted Services.

8.4 You shall not use the Hosted Services to promote, host or operate any chain letters, ponzi schemes, pyramid schemes, matrix programs, multi-level marketing schemes, "get rich quick" schemes or similar letters, schemes or programs.

8.5 You shall not use the Hosted Services in any way which is liable to result in the blacklisting of any of our IP addresses.

9. Regulated Businesses

9.1 You shall not use the Hosted Services for any purpose relating to gambling, gaming, betting, lotteries, sweepstakes, prize competitions or any gambling-related activity.

9.2 You shall not use the Hosted Services for any purpose relating to the offering for sale or distribution of drugs or pharmaceuticals, unless you are a member of a special profession which allow you to use or publish such Content (e.g. medical doctor or member of a state regulated pharmaceutical company).

9.3 You shall not use the Hosted Services for any purpose relating to the offering for sale or distribution of guns or other weapons, unless you are a member of a

special profession which allow you to use or publish such Content (e.g. state licensed manufacturer of guns or other weapons, state authority etc.).

9.4 You shall not use the Hosted Services for any purpose relating to the offering for sale or distribution of illegal material, radical right-wing propaganda or rabble-rousing.

10. Monitoring and Checks

You acknowledge that we may actively monitor or check the Content and your use of the Hosted Services when we are informed or gain knowledge that you infringe this User Agreement.

11. Data Mining

You shall not conduct any systematic or automated data scraping, data mining, data extraction or data harvesting, or other systematic or automated data collection activity, by means of or in relation to the Hosted Services.

12. Hyperlinks

You shall not link to any material by means of the Hosted Services that would, if it were made available through the Hosted Services, breach the provisions of this User Agreement.

13. Harmful software

13.1 The Content shall not contain or consist of, and you shall not promote, distribute or execute by means of the Hosted Services, any viruses, worms, spyware, adware or other harmful or malicious software, programs, routines, applications or technologies.

13.2 The Content shall not contain or consist of, and you shall not promote, distribute or execute by means of the Hosted Services, any software, programs, routines, applications or technologies that will or may have a material negative effect upon the performance of a computer or introduce material security risks to a computer.

14. Purchase and Sale of our Company or Purchase and Sale of Platform

You confirm that you understand that we may transfer the entire Agreement with the Subscriber (e.g. your employer), including Rights and Obligations, Account, Charges, Documentation, Hosted Services, Intellectual Property Rights, Maintenance Services,

Mobile App, Personal Data, Platform, Services, Subscriber Confidential Information, Subscriber Data, Support Services, Term and every other functionality, Source Code, Data or Database in relation to the Platform, in whole or in part, in case we conclude a sale of business, shares or stocks, applications or other assets, transfer or restructure our business, that may or may not result in the performance of this Agreement under the same or a new Provider, legal form or company name.

15. Partners and Marketing

We conduct our own marketing activities and work with Partners to offer a variety of deals, products and services (e.g. discounts etc.). You instruct us to find deals, products and services for you and to inform you about these deals, products and services by email, SMS or in other ways (e.g. a method used by you to sign-up or verify an account). In order to notify you and provide you with the information you need to participate, we process your Personal Data. Without being able to process your Personal Data for this purpose, we would not be able to perform the services agreed on with you. Therefore, the processing of such Personal Data is required to carry out our services to which the legal basis is Art. 6 (1) (b) and Art. 6 (1) (f) GDPR, or similar provisions of other Data Protection Laws.

16. SaaS Subscription and Data Processing Agreement

You confirm that you fully reviewed the SaaS Subscription and Data Processing Agreement and that you agree to and will comply with all terms set out in that Agreement that was concluded with the Subscriber (e.g. your employer).

17. Privacy Policy and Transparency Document

You confirm that you reviewed the Privacy Policy and Transparency Document and that you know all rights that you have as a Data Subject.

18. Data Protection: Your Consent

18.1 By registering and using the Platform you give us consent to process any Personal Data you provide to us.

18.2 We inform you that you have the right to withdraw your consent at any time with effect for the future. It shall be as easy to withdraw as to give consent. Therefore, you can withdraw your consent by deleting your account at any time.

18.3 We inform you, that the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

19. Data Protection: General Obligations

19.1 You shall keep all Personal Data that you process or access by using the Hosted Services strictly confidential. You are strictly prohibited to process Personal Data unauthorized, in particular but not limited to unauthorized collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data.

19.2 You shall process Personal Data always in accordance with applicable law and observe the Principles of Processing of applicable law.

19.3. If GDPR is applicable to the processing of Personal Data, you shall process only in accordance with the Principles of GDPR, which means Personal Data shall be

a) processed lawfully and in a comprehensive manner for the data subject;

b) collected with the defined, explicit and legitimate purpose and shall not be processed in other way, that is not associated with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimization’);

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data are processed;

f) processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’).

20. Business and Trade Secrets, other Secrets, Intellectual Property Rights, Designs, Wireframes and SaaS Application Functionality

20.1 You shall keep Business and Trade Secrets, other Secrets, Intellectual Property Rights, Designs, Wireframes and SaaS Application Functionality that are property

of the Provider, Subscriber or Third Parties, strictly confidential and shall not process and/or copy, examine, analyze, explore, research, study, investigate, document, catalogue, log, note, register, report, write down, screen, recreate, reproduce, clone, duplicate, emulate, imitate, mirror, photocopy, portray, print, replicate, photograph, record, print screen, duplicate, inspect, and/or make them available to any Third Party, your employer or use them in any way without explicit approval of the owner of the respective Business or Trade Secret, other Secret, Intellectual Property Right, Design, Wireframe or SaaS Application Functionality.

20.2 Business and/or Trade Secrets are (at least) all information that are

a) neither in general nor in their precise arrangement or composition generally known or otherwise available to the persons in circles, who usually handle such type of information and are therefore of economic value;

b) subject to reasonable confidentiality measures by its lawful owner; and

c) all information in regards to or about our SaaS Applications, in particular wireframes, functionalities, software architectures and interfaces and designs of the SaaS Applications you use or have access to under this User Agreement.

20.3 Business and Trade Secrets are in particular but not limited to information related to prices, target figures, turnover / profit / income figures, economical figures, current and planned projects, technological and conceptual structures, analytical work, software architectures and interfaces, datasets and their usage, passwords, authorities, duties, suppliers and customers data, data of Business Partners as well as particularly all confidential information related to customers and suppliers of the Provider, Subscriber or any Third Party, to which you got access by using the Hosted Services when preparing or executing activities regarding to customers and suppliers of the Provider, Subscriber or any Third Party, as for example information on relevant customers or suppliers of the Provider, Subscriber or any Third Party, business processes, infrastructure, business plans and products, software, programming or any information, that you processed during usage of confidential information or by using the Hosted Services.

20.4 You shall comply with any bank secrecy, professional secrecy, telecommunications secrecy, postal secrecy, correspondence secrecy, social data secrecy and any other secrecy, copyright or privacy regulation that is applicable to you, the Provider, Subscriber or any Third Party.

21. Arbitration Clause

All disputes arising out of or in connection with this User Agreement, or any other agreement between you, your employer, contractors, partners, us and other parties, are subject to the Arbitration Clause 21 from the "SaaS Subscription and Data Processing Agreement". You hereby confirm that you have read the SaaS Subscription and Data Processing Agreement in full.

22. Effects of Termination

Upon termination of this User Agreement, all of the provisions of this User Agreement shall cease to have effect, save that the following provisions of this User Agreement shall survive and continue to have effect, in accordance with their express terms or otherwise indefinitely: Clauses 8.3, 11, 14, 19, 20 and 21.

23. Consequences of Violation

Violation of the terms set forth in this User Agreement may lead to suspension or termination of the user's account and/or legal action.

APPENDIX 3 (Data Processing Information)

1. Nature and Purpose of the Processing, Type of Personal Data as well as Categories of Data Subjects:

a) Purpose of the Processing:

Provision of SaaS Solutions and Hosted Services. General Business purposes, Subscriber & Client administration, Staff and HR administration, Marketing, Sales & Providing of Products and Services.

b) Nature of the Processing (as defined in Art. 4 No. 2 GDPR):

Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data.

c) Type of Personal Data (as defined in Art. 4 No. 1, 13, 14 and 15 GDPR):

Personal Data acc. to Art. 4 No. 1 GDPR, in particular, data of employees, Subscribers and other Business Partners of Subscribers.

2. Categories of Data Subjects

Subscribers, Potential Subscribers, Employees, Employees of Third Parties, Business Partners, Suppliers, Communication Participants, Contractual Partners, Service Providers, Consultants, Freelancers, Authorized Agents, Data Protection Officers.

3. Categories of Personal Data

Subscribers, Potential Subscribers, Employees, Employees of Third Parties, Business Partners, Suppliers, Communication Participants, Contractual Partners, Service Providers, Consultants, Freelancers, Authorized Agents, Data Protection Officers, HR Contact Persons, Names, Address Data, Contact Information, Location data, Identification numbers, Online identifiers, Security identifiers, Other Identifiers, Factors specific to the economic identity.

4. Technical and Organizational Measures (TOMs)

1. Measures of pseudonymization and encryption of personal data

Pseudonymisation of personal data that are no longer needed in plain text

Encryption of websites (SSL)

Encryption of e-mail (TLS 1.2 or 1.3)

2. **Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services**

Confidentiality and data protection agreements with employees

NDAs with third parties

Hardware- or software-firewall

Anti-Virus software

Regular backups

3. **Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident**

Regular backups of the whole system

Regular test of backup and recovery

Regular training of IT staff

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

Regular review of processes by IT

Regular audits (e.g. by the DPO)

5. **Measures for user identification and authorisation**

Authentication with username / password

Regular checks of authorisations

Password guideline

Limitation of the number of administrators

Management of rights by system administrator

Differentiation between authorisations

6. **Measures for the protection of data during transmission**

Use of encryption technologies

Logging of activities and events

Encryption of email (TLS 1.2 or 1.3)

Use of company internal / restricted drives

7. Measures for the protection of data during storage

Logging of actions and events
Limitation of the number of administrator's
Firewall

8. Measures for ensuring physical security of locations at which personal data are processed

Manual locking system
Security locks
Key control

9. Measures for ensuring events logging

Logging activated on application level
Regular manual checks of logs

10. Measures for ensuring system configuration, including default configuration

Configuration change control process
Data protection by default and design is observed
Configuration only by system administrator
Regular training of IT staff

11. Measures for internal IT and IT security governance and management

IT security policy
Training of employees on data security
IT team with clear roles and responsibilities

12. Measures for certification/assurance of processes and products

Clear overview of the provisions applicable to the provided products/services/processes
Regular internal and/or external audits
Assignment of audit responsibilities to certified experts

13. Measures for ensuring data minimization

Identification of the purpose of processing
Assessment of a link between processing and purpose
Identification of the applicable retention periods for each data category
Secure erasure of the data after expiration of the retention period

14. Measures for ensuring data quality

Logging of entry and modification of data
Assignment of rights for data entry
Traceability of entry, modification of data by individual user names (not user groups)

15. Measures for ensuring limited data retention

Regular training on retention periods
Regular audit and assessment of retained data

16. Measures for ensuring accountability

Provision of training / awareness rising
Regular controls and checks
Appropriate policies on data protection
Conclusion of SCCs
Use of secure data erasure
Legal basis for processing exists for all activities
Documented privacy policy

17. Measures for allowing data portability and ensuring erasure

Personal data is stored in a structured format
Monitoring of legal deadline ensured
Observation of retention periods
Establishment of data portability process
Proper handling of data subject requests
Secure data erasure and data carrier destruction ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com (certified data erasure and destruction).

18. For transfers to (sub-) processors, also 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

Secure data erasure and data carrier destruction ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com (certified data erasure and destruction).
Contractually agreed on effective control rights

Contractually agreed on provision of assistance to the controller

5. Sub-Processors of Personal Data

This are the current sub-processors of Willing & Able Licensing LLC. The respective contact addresses are published on their websites.

Company Name	Website	Services	Country	Location of Service
Hetzner	hetzner.de	Hosting & Cloud	Germany	Gunzenhausen
1&1	1und1.de	Hosting & Cloud	Germany	Montabaur
Strato	Strato.de	Hosting & Cloud	Germany	Berlin
Contabo GmbH	contabo.com	Hosting & Cloud	Germany	München
Amazon Web Services	aws.amazon.com	Hosting & Cloud	Germany	Frankfurt
Microsoft Azure	azure.microsoft.com	Hosting & Cloud	Netherlands	Amsterdam
Microsoft Office 365	office.com	Office 365	Netherlands	Amsterdam
Google Cloud	cloud.google.com	Hosting & Cloud	Ireland	Dublin
Google G-Suite	gsuite.google.com	G-Suite	Ireland	Dublin
DGD	dg-datenschutz.de	Audits, Trainings, Consulting	Germany	Petershausen
Notebook12	Notebook12.com	Deletion Data Carrier Destruction	Germany	Petershausen
Willing & Able Operations	willing-able.com	Development, Sales and Support	Armenia	Yerevan
Willing & Able Georgia	willing-able.com	Development, Sales and Support	Georgia	Tbilissi

APPENDIX 4 (Standard Contractual Clauses)

Section A
STANDARD CONTRACTUAL CLAUSES 2021/915 BETWEEN CONTROLLERS AND PROCESSORS

Clause 1
Purpose and scope

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2
Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3
Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, 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 or Regulation (EU) 2018/1725 respectively.
(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4
Hierarchy

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

Clause 5
Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.
(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.
(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

Clause 6
Description of the processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7
Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (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 purposes of processing and the risks involved for the data subjects.
(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing 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 ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit 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 an audit, the controller may take into account relevant certifications held by the processor.

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

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a)

GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor

shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

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

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub- processor to fulfill its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfill a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8
Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9
Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1. Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679 shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679 with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2. Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

Clause 10
Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.
(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.
(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I
List of parties

Controller(s): [Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]

Controller Number 1:

Name: Subscriber (see in application)

Address: Legal address of Subscriber (based in the EU/EEA) (see in application)

Contact person's name, position and contact details: Legal representative of Subscriber (see in application)

Where applicable, the controller's data protection officer: Name available upon request

Accession date: Date of system registration of the respective processor (see in application)

Concluded by acceptance of Willing & Able SaaS Subscription and Data Processing Agreement

Controller Number 2:

Name: Subscribers Subsidiary that is using the application as a Controller (see in application)

Address: Legal address of Subscribers Subsidiary (based in the EU/EEA) (see in application)

Contact person's name, position and contact details: Legal representative of Subscribers Subsidiary (see in application)

Where applicable, the controller's data protection officer: Name available upon request, if any

Accession date: Date of system registration of the respective processor (see in application)

Concluded by acceptance of Willing & Able SaaS Subscription and Data Processing Agreement

Controller Number 3:

Name: Subscription Partner that is using the application as a Controller (see in application)

Address: Legal address of Subscription Partner (based in the EU/EEA) (see in application)

Contact person's name, position and contact details: Legal representative of Subscription Partner (see in application)

Where applicable, the controller's data protection officer: Name available upon request, if any

Accession date: Date of system registration of the respective processor (see in application)

Concluded by acceptance of Willing & Able SaaS Subscription and Data Processing Agreement

Controller Number 4:

Name: Franchise Partner that is using the application as a Controller (see in application)

Address: Legal address of Franchise Partner (based in the EU/EEA) (see in application)

Contact person's name, position and contact details: Legal representative of Franchise Partner (see in application)

Where applicable, the controller's data protection officer: Name available upon request, if any

Accession date: Date of system registration of the respective processor (see in application)

Concluded by acceptance of Willing & Able SaaS Subscription and Data Processing Agreement

Processor(s): [Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer]

Processor Number 1:

Name: Subscribers Subsidiary that is using the application as a Processor (see in application)

Address: Legal address of Subscribers Subsidiary (based in the EU/EEA) (see in application)

Contact person's name, position and contact details: Legal representative of Subscribers Subsidiary (see in application)

Where applicable, the controller's data protection officer: Name available upon request, if any

Accession date: Date of system registration (see in application)

Concluded by acceptance of Willing & Able SaaS Subscription and Data Processing Agreement

Processor Number 2:

Name: Subscribers Contractor that is using the application as a Processor (see in application)

Address: Legal address of Subscribers Contractor (based in the EU/EEA) (see in application)

Contact person's name, position and contact details: Legal representative of Subscribers Contractor (see in application)

Where applicable, the controller's data protection officer: Name available upon request, if any

Accession date: Date of system registration (see in application)

Concluded by acceptance of Willing & Able SaaS Subscription and Data Processing Agreement

Processor Number 3:

Name: Subscription Partner that is using the application as a Processor (see in application)

Address: Legal address of Subscription Partner (based in the EU/EEA) (see in application)

Contact person's name, position and contact details: Legal representative of Subscription Partner (see in application)

Where applicable, the controller's data protection officer: Name available upon request, if any

Accession date: Date of system registration (see in application)

Concluded by acceptance of Willing & Able SaaS Subscription and Data Processing Agreement

Processor Number 4:

Name: Franchise Partner that is using the application as a Processor (see in application)

Address: Legal address of Franchise Partner (based in the EU/EEA) (see in application)

Contact person's name, position and contact details: Legal representative of Franchise Partner (see in application)

Where applicable, the controller's data protection officer: Name available upon request, if any

Accession date: Date of system registration (see in application)

Concluded by acceptance of Willing & Able SaaS Subscription and Data Processing Agreement

ANNEX II
Description of the processing

Categories of data subjects whose personal data is processed

Customers	Potential customers
Employees	Business partners
Apprentices	Suppliers
Communication participants	Trainees
Service providers	Consultants
Students	Authorized Agents
Shareholders	Contact Persons
Subscribers	

Categories of personal data processed

Names	Identification number
Location data	Online identifier
Customer data	Data of potential customers
Data of employees	Data of Business Partners
Data of apprentices	Data of suppliers
Data of communic. participants	Data of trainees
Data of service providers	Data of consultants
Data of students	Data of authorized agents
Data of shareholders	Data of contact persons
Data of subscribers	

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

Sensitive data processed

None

Applied restrictions or safeguards

Access restrictions
Keeping a record of access to the data
Restrictions for onward transfers
Additional security measures, see TOMs of Willing & Able.

Nature of the processing

Collection	Adaptation	Disclosure by transmission
Restriction	Recording	Alteration
Dissemination	Erasure	Organisation
Retrieval	Otherwise making available	Destruction
Structuring	Consultation	Alignment
Storage	Use	Combination

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

Usage of Online-Application of Willing & Able.

Duration of the processing

The data is processed on a continuous basis.

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

Subject matter of (sub-) processing: Granting access to usage of Online-Application of Willing & Able.

Nature of (sub-) processing: Usage of Online-Application of Willing & Able.

Duration of (sub-) processing: The data is processed on a continuous basis.

ANNEX III

Technical and organisational measures including technical and organisational measures to ensure the security of the data

EXPLANATORY NOTE:

The technical and organisational measures need to be described concretely and not in a generic manner.

Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:

1. **Measures of pseudonymization and encryption of personal data**

Pseudonymisation of personal data that are no longer needed in plain text

Encryption of websites (SSL)

Encryption of e-mail (TLS 1.2 or 1.3)

2. **Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services**

Confidentiality and data protection agreements with employees

NDAs with third parties

Hardware- or software-firewall

Anti-Virus software

Regular backups

3. **Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident**

Regular backups of the whole system

Regular test of backup and recovery

Regular training of IT staff

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

Regular review of processes by IT

Regular audits (e.g. by the DPO)

5. Measures for user identification and authorisation

Authentication with username / password
Regular checks of authorisations
Password guideline
Limitation of the number of administrators
Management of rights by system administrator
Differentiation between authorisations

6. Measures for the protection of data during transmission

Use of encryption technologies
Logging of activities and events
Encryption of email (TLS 1.2 or 1.3)
Use of company internal / restricted drives

7. Measures for the protection of data during storage

Logging of actions and events
Limitation of the number of administrator's
Firewall

8. Measures for ensuring physical security of locations at which personal data are processed

Manual locking system
Security locks
Key control

9. Measures for ensuring events logging

Logging activated on application level
Regular manual checks of logs

10. Measures for ensuring system configuration, including default configuration

Configuration change control process
Data protection by default and design is observed
Configuration only by system administrator

Regular training of IT staff

11. Measures for internal IT and IT security governance and management

IT security policy
Training of employees on data security
IT team with clear roles and responsibilities

12. Measures for certification/assurance of processes and products

Clear overview of the provisions applicable to the provided products/services/processes
Regular internal and/or external audits
Assignment of audit responsibilities to certified experts

13. Measures for ensuring data minimization

Identification of the purpose of processing
Assessment of a link between processing and purpose
Identification of the applicable retention periods for each data category
Secure erasure of the data after expiration of the retention period

14. Measures for ensuring data quality

Logging of entry and modification of data
Assignment of rights for data entry
Traceability of entry, modification of data by individual user names (not user groups)

15. Measures for ensuring limited data retention

Regular training on retention periods
Regular audit and assessment of retained data

16. Measures for ensuring accountability

Provision of training / awareness rising
Regular controls and checks
Appropriate policies on data protection
Conclusion of SCCs
Use of secure data erasure

Legal basis for processing exists for all activities
Documented privacy policy

17. Measures for allowing data portability and ensuring erasure

Personal data is stored in a structured format
Monitoring of legal deadline ensured
Observation of retention periods
Establishment of data portability process
Proper handling of data subject requests
Secure data erasure and data carrier destruction ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com (certified data erasure and destruction).

18. For transfers to (sub-) processors, also 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

Secure data erasure and data carrier destruction ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com (certified data erasure and destruction).
Contractually agreed on effective control rights
Contractually agreed on provision of assistance to the controller

ANNEX IV
List of sub-processors

EXPLANATORY NOTE:

This Annex needs to be completed in case of specific authorisation of sub-processors (Clause 7.7(a), Option 1).

The controller has authorised the use of the following sub-processors:

See section “Sub-Processors of Personal Data” in Willing & Able SaaS Subscription and Data Processing Agreement, and/or separate document.

Section B
STANDARD CONTRACTUAL CLAUSES 2021/914
MODULE ONE: Transfer Controller to Controller

Clause 1
Purpose and scope

(a) The purpose of these 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 contractual clauses ('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) The data subjects can enforce against the data exporter and/or data importer these Clauses, with the following exceptions:

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

(ii) Clause 8.5 (e) and Clause 8.9 (b)

(iv) Clause 12 (a) and (d);

(v) Clause 13;

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

(vii) Clause 16 (e);

(viii) Clause 18 (a) and (b);

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

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of other 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 hereunder.

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.

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:

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

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

(iii)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

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 anonymisation 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 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) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

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

(b) 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 established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has

appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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 fulfill 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.

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 Germany.

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 Germany.

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

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

ANNEX I

A. LIST OF PARTIES

Data exporter Number 1:

Name: Subscriber (see in application)

Address: Legal address of Subscriber (see in application)

Contact person's name, position and contact details: Legal representative of Subscriber (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration of the data importer (see in application)

Role: Controller

Data exporter Number 2:

Name: Subscribers Subsidiary (see in application)

Address: Legal address of Subscribers Subsidiary (see in application)

Contact person's name, position and contact details: Legal representative of Subscribers Subsidiary (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration of the data importer (see in application)

Role: Controller

Data importer Number 1:

Name: Subscribers Subsidiary (see in application)

Address: Legal address of Subscribers Subsidiary (see in application)

Contact person's name, position and contact details: Legal representative of Subscribers Subsidiary (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration (see in application)

Role: Controller

Data importer Number 2:

Name: Business Partner (see in application)

Address: Legal address of Business Partner (see in application)

Contact person's name, position and contact details: Legal representative of Business Partner (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration (see in application)

Role: Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transfered

Customers	Potential customers
Employees	Business partners
Apprentices	Suppliers
Communication participants	Trainees
Service providers	Consultants
Students	Authorized Agents
Shareholders	Contact Persons
Subscribers	

Categories of personal data transfered

Names	Identification number
Location data	Online identifier
Customer data	Data of potential customers
Data of employees	Data of Business Partners
Data of apprentices	Data of suppliers
Data of communic. participants	Data of trainees
Data of service providers	Data of consultants
Data of students	Data of authorized agents
Data of shareholders	Data of contact persons
Data of subscribers	

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.

Sensitive data transferred

None

Applied restrictions or safeguards

Access restrictions

Keeping a record of access to the data

Restrictions for onward transfers

Additional security measures, see TOMs of Willing & Able.

Frequency of transfer:

The data is transferred on a continuous basis.

Nature of processing

Collection	Adaptation	Disclosure by transmission
Restriction	Recording	Alteration
Dissemination	Erasure	Organisation
Retrieval	Otherwise making available	Destruction
Structuring	Consultation	Alignment
Storage	Use	Combination

Purpose(s) of the data transfer and further processing

Usage of Online-Application of Willing & Able.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The data is retained for a longer period. The statutory retention period is used to determine the retention period.

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

Subject matter of (sub-) processing: Granting access to usage of Online-Application of Willing & Able.

Nature of (sub-) processing: Usage of Online-Application of Willing & Able.

Duration of (sub-) processing: The data is processed on a continuous basis.

C. COMPETENT SUPERVISORY AUTHORITY

Greece - Hellenic Data Protection Authority

ANNEX II

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. Measures of pseudonymization and encryption of personal data

Pseudonymisation of personal data that are no longer needed in plain text

Encryption of websites (SSL)

Encryption of e-mail (TLS 1.2 or 1.3)

2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Confidentiality and data protection agreements with employees

NDAs with third parties

Hardware- or software-firewall

Anti-Virus software

Regular backups

3. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Regular backups of the whole system

Regular test of backup and recovery

Regular training of IT staff

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

Regular review of processes by IT

Regular audits (e.g. by the DPO)

5. Measures for user identification and authorisation

Authentication with username / password

Regular checks of authorisations
Password guideline
Limitation of the number of administrators
Management of rights by system administrator
Differentiation between authorisations

6. Measures for the protection of data during transmission

Use of encryption technologies
Logging of activities and events
Encryption of email (TLS 1.2 or 1.3)
Use of company internal / restricted drives

7. Measures for the protection of data during storage

Logging of actions and events
Limitation of the number of administrator's
Firewall

8. Measures for ensuring physical security of locations at which personal data are processed

Manual locking system
Security locks
Key control

9. Measures for ensuring events logging

Logging activated on application level
Regular manual checks of logs

10. Measures for ensuring system configuration, including default configuration

Configuration change control process
Data protection by default and design is observed
Configuration only by system administrator
Regular training of IT staff

11. Measures for internal IT and IT security governance and management

IT security policy
Training of employees on data security
IT team with clear roles and responsibilities

12. Measures for certification/assurance of processes and products

Clear overview of the provisions applicable to the provided products/services/processes
Regular internal and/or external audits
Assignment of audit responsibilities to certified experts

13. Measures for ensuring data minimization

Identification of the purpose of processing
Assessment of a link between processing and purpose
Identification of the applicable retention periods for each data category
Secure erasure of the data after expiration of the retention period

14. Measures for ensuring data quality

Logging of entry and modification of data
Assignment of rights for data entry
Traceability of entry, modification of data by individual user names (not user groups)

15. Measures for ensuring limited data retention

Regular training on retention periods
Regular audit and assessment of retained data

16. Measures for ensuring accountability

Provision of training / awareness rising
Regular controls and checks
Appropriate policies on data protection
Conclusion of SCCs
Use of secure data erasure
Legal basis for processing exists for all activities
Documented privacy policy

17. Measures for allowing data portability and ensuring erasure

Personal data is stored in a structured format
Monitoring of legal deadline ensured
Observation of retention periods
Establishment of data portability process
Proper handling of data subject requests
Secure data erasure and data carrier destruction ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com (certified data erasure and destruction).

18. **For transfers to (sub-) processors, also 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**

Secure data erasure and data carrier destruction ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com (certified data erasure and destruction).
Contractually agreed on effective control rights
Contractually agreed on provision of assistance to the controller

Section C
STANDARD CONTRACTUAL CLAUSES 2021/914
MODULE TWO: Transfer Controller to Processor

Clause 1
Purpose and scope

(a) The purpose of these 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 contractual clauses ('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) The data subjects can enforce against the data exporter and/or data importer these Clauses, with the following exceptions:

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

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16 (e);

(viii) Clause 18 (a) and (b);

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

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of other 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 hereunder.

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.

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 defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

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

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

8.9. Documentation and compliance

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

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

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of 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)
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 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

(c) The data importer shall provide, at the data exporter's request, a copy of such a 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.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

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

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.
(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has

appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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 fulfill 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.

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part

of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

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 Germany.

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

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

ANNEX I

A. LIST OF PARTIES

Data exporter Number 1:

Name: Subscriber (see in application)

Address: Legal address of Subscriber (see in application)

Contact person's name, position and contact details: Legal representative of Subscriber (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration of the data importer (see in application)

Role: Controller

Data exporter Number 2:

Name: Subscribers Subsidiary (see in application)

Address: Legal address of Subscribers Subsidiary (see in application)

Contact person's name, position and contact details: Legal representative of Subscribers Subsidiary (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration of the data importer (see in application)

Role: Controller

Data importer Number 1:

Name: Subscribers Subsidiary (see in application)

Address: Legal address of Subscribers Subsidiary (see in application)

Contact person's name, position and contact details: Legal representative of Subscribers Subsidiary (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration (see in application)

Role: Processor

Data importer Number 2:

Name: Business Partner (see in application)

Address: Legal address of Business Partner (see in application)

Contact person's name, position and contact details: Legal representative of Business Partner (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration (see in application)

Role: Processor

Data importer Number 3:

Name: Willing & Able Licensing LLC

Address: Geronti Kikodze Street 11, 1st Floor, 0105 Tbilisi, Republic of Georgia

Contact person's name, position and contact details: see imprint of Willing & Able website

Activities relevant to the data transferred under these Clauses: Usage and provision of the application, and/or related services.

Where applicable, of its/their data protection officer and/or representative in the European Union: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., DGD Deutsche Gesellschaft für Datenschutz GmbH, Fraunhoferring 3, 85238 Petershausen, Germany

Date: Date of system registration of Subscriber (see in application)

Role: Processor

Data importer Number 4:

Name: Willing & Able Operations LLC

Address: Shop 141, Building 25, 1st Floor, Norashen, Ajapnyak, Yerevan, 0036, Republic of Armenia

Contact person's name, position and contact details: see imprint of Willing & Able website

Activities relevant to the data transferred under these Clauses: Usage and provision of the application, and/or related services.

Where applicable, of its/their data protection officer and/or representative in the European Union: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., DGD Deutsche Gesellschaft für Datenschutz GmbH, Fraunhoferring 3, 85238 Petershausen, Germany

Date: Date of system registration of Subscriber (see in application)

Role: Processor

Data importer Number 5:

Name: Willing & Able Georgia LLC

Address: Geronti Kikodze Street 11, 1st Floor, 0105 Tbilisi, Republic of Georgia

Contact person's name, position and contact details: see imprint of Willing & Able website

Activities relevant to the data transferred under these Clauses: Usage and provision of the application, and/or related services.

Where applicable, of its/their data protection officer and/or representative in the European Union: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., DGD Deutsche Gesellschaft für Datenschutz GmbH, Fraunhoferring 3, 85238 Petershausen, Germany

Date: Date of system registration of Subscriber (see in application)

Role: Processor

Data importer Number 6:

Name: Subscription Partner (see in application)

Address: Legal address of Subscription Partner (see in application)

Contact person's name, position and contact details: Legal representative of Subscription Partner (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration (see in application)

Role: Processor

Data importer Number 7:

Name: Franchise Partner (see in application)

Address: Legal address of Franchise Partner (see in application)

Contact person's name, position and contact details: Legal representative of Franchise Partner (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration (see in application)

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transfered

Customers	Potential customers
Employees	Business partners
Apprentices	Suppliers
Communication participants	Trainees
Service providers	Consultants
Students	Authorized Agents
Shareholders	Contact Persons
Subscribers	

Categories of personal data transfered

Names	Identification number
Location data	Online identifier
Customer data	Data of potential customers
Data of employees	Data of Business Partners
Data of apprentices	Data of suppliers
Data of communic. participants	Data of trainees
Data of service providers	Data of consultants
Data of students	Data of authorized agents
Data of shareholders	Data of contact persons
Data of subscribers	

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.

Sensitive data transferred

None

Applied restrictions or safeguards

Access restrictions

Keeping a record of access to the data

Restrictions for onward transfers

Additional security measures, see TOMs of Willing & Able.

Frequency of transfer:

The data is transferred on a continuous basis.

Nature of processing

Collection	Adaptation	Disclosure by transmission
Restriction	Recording	Alteration
Dissemination	Erasure	Organisation
Retrieval	Otherwise making available	Destruction
Structuring	Consultation	Alignment
Storage	Use	Combination

Purpose(s) of the data transfer and further processing

Usage of Online-Application of Willing & Able.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The data is retained for a longer period. The statutory retention period is used to determine the retention period.

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

Subject matter of (sub-) processing: Granting access to usage of Online-Application of Willing & Able.

Nature of (sub-) processing: Usage of Online-Application of Willing & Able.

Duration of (sub-) processing: The data is processed on a continuous basis.

C. COMPETENT SUPERVISORY AUTHORITY

Greece - Hellenic Data Protection Authority

ANNEX II

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. Measures of pseudonymization and encryption of personal data

Pseudonymisation of personal data that are no longer needed in plain text

Encryption of websites (SSL)

Encryption of e-mail (TLS 1.2 or 1.3)

2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Confidentiality and data protection agreements with employees

NDAs with third parties

Hardware- or software-firewall

Anti-Virus software

Regular backups

3. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Regular backups of the whole system

Regular test of backup and recovery

Regular training of IT staff

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

Regular review of processes by IT

Regular audits (e.g. by the DPO)

5. Measures for user identification and authorisation

Authentication with username / password

Regular checks of authorisations
Password guideline
Limitation of the number of administrators
Management of rights by system administrator
Differentiation between authorisations

6. Measures for the protection of data during transmission

Use of encryption technologies
Logging of activities and events
Encryption of email (TLS 1.2 or 1.3)
Use of company internal / restricted drives

7. Measures for the protection of data during storage

Logging of actions and events
Limitation of the number of administrator's
Firewall

8. Measures for ensuring physical security of locations at which personal data are processed

Manual locking system
Security locks
Key control

9. Measures for ensuring events logging

Logging activated on application level
Regular manual checks of logs

10. Measures for ensuring system configuration, including default configuration

Configuration change control process
Data protection by default and design is observed
Configuration only by system administrator
Regular training of IT staff

11. Measures for internal IT and IT security governance and management

IT security policy
Training of employees on data security
IT team with clear roles and responsibilities

12. Measures for certification/assurance of processes and products

Clear overview of the provisions applicable to the provided products/services/processes
Regular internal and/or external audits
Assignment of audit responsibilities to certified experts

13. Measures for ensuring data minimization

Identification of the purpose of processing
Assessment of a link between processing and purpose
Identification of the applicable retention periods for each data category
Secure erasure of the data after expiration of the retention period

14. Measures for ensuring data quality

Logging of entry and modification of data
Assignment of rights for data entry
Traceability of entry, modification of data by individual user names (not user groups)

15. Measures for ensuring limited data retention

Regular training on retention periods
Regular audit and assessment of retained data

16. Measures for ensuring accountability

Provision of training / awareness rising
Regular controls and checks
Appropriate policies on data protection
Conclusion of SCCs
Use of secure data erasure
Legal basis for processing exists for all activities
Documented privacy policy

17. Measures for allowing data portability and ensuring erasure

Personal data is stored in a structured format
Monitoring of legal deadline ensured
Observation of retention periods
Establishment of data portability process
Proper handling of data subject requests
Secure data erasure and data carrier destruction ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com (certified data erasure and destruction).

18. **For transfers to (sub-) processors, also 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**

Secure data erasure and data carrier destruction ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com (certified data erasure and destruction).
Contractually agreed on effective control rights
Contractually agreed on provision of assistance to the controller

ANNEX III
LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

See section “Sub-Processors of Personal Data” in Willing & Able SaaS Subscription and Data Processing Agreement, and/or separate document.

Section D
STANDARD CONTRACTUAL CLAUSES 2021/914
MODULE THREE: Transfer Processor to Processor

Clause 1
Purpose and scope

(a) The purpose of these 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 between the Parties 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) The data subjects can enforce against the data exporter and/or data importer these Clauses, with the following exceptions:

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

(ii) Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16 (e);

(viii) Clause 18 (a) and (b);

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

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of other 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.

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 exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3. Transparency

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

8.4. Accuracy

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

8.5. Duration of processing and erasure or return of data

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

8.6. Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7. Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European 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;

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

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

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

8.9. Documentation and compliance

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

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

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

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

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

Clause 9
Use of sub-processors

(a)
GENERAL WRITTEN AUTHORISATION: The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11
Redress

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

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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). The data exporter shall forward the notification to the controller.

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

Clause 15

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

15.1. Notification

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

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

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

The data exporter shall forward the notification to the controller.

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

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

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

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

15.2. Review of legality and data minimisation

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

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

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

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17
Governing law

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 Germany.

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 Germany.

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

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

ANNEX I

A. LIST OF PARTIES

Data exporter Number 1:

Name: Subscriber (see in application)

Address: Legal address of Subscriber (see in application)

Contact person's name, position and contact details: Legal representative of Subscriber (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration of the data importer (see in application)

Role: Processor

Data exporter Number 2:

Name: Subscribers Subsidiary (see in application)

Address: Legal address of Subscribers Subsidiary (see in application)

Contact person's name, position and contact details: Legal representative of Subscribers Subsidiary (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration of the data importer (see in application)

Role: Processor

Data exporter Number 3:

Name: Willing & Able Licensing LLC

Address: Geronti Kikodze Street 11, 1st Floor, 0105 Tbilisi, Republic of Georgia

Contact person's name, position and contact details: see imprint of Willing & Able website

Activities relevant to the data transferred under these Clauses: Usage and provision of the application, and/or related services.

Where applicable, of its/their data protection officer and/or representative in the European Union: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., DGD Deutsche Gesellschaft für Datenschutz GmbH, Fraunhoferring 3, 85238 Petershausen, Germany

Date: Date of system registration of Subscriber (see in application)

Role: Processor

Data exporter Number 4:

Name: Willing & Able Operations LLC

Address: Shop 141, Building 25, 1st Floor, Norashen, Ajapnyak, Yerevan, 0036, Republic of Armenia

Contact person's name, position and contact details: see imprint of Willing & Able website

Activities relevant to the data transferred under these Clauses: Usage and provision of the application, and/or related services.

Where applicable, of its/their data protection officer and/or representative in the European Union: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., DGD Deutsche Gesellschaft für Datenschutz GmbH, Fraunhoferring 3, 85238 Petershausen, Germany

Date: Date of system registration of Subscriber (see in application)

Role: Processor

Data exporter Number 4:

Name: Willing & Able Georgia LLC

Address: Geronti Kikodze Street 11, 1st Floor, 0105 Tbilisi, Republic of Georgia

Contact person's name, position and contact details: see imprint of Willing & Able website

Activities relevant to the data transferred under these Clauses: Usage and provision of the application, and/or related services.

Where applicable, of its/their data protection officer and/or representative in the European Union: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., DGD Deutsche Gesellschaft für Datenschutz GmbH, Fraunhoferring 3, 85238 Petershausen, Germany

Date: Date of system registration of Subscriber (see in application)

Role: Processor

Data exporter Number 6:

Name: Subscription Partner (see in application)

Address: Legal address of Subscription Partner (see in application)

Contact person's name, position and contact details: Legal representative of Subscription Partner (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration of the data importer (see in application)

Role: Processor

Data exporter Number 7:

Name: Franchise Partner (see in application)

Address: Legal address of Franchise Partner (see in application)

Contact person's name, position and contact details: Legal representative of Franchise Partner (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration of the data importer (see in application)

Role: Processor

Data importer Number 1:

Name: Subscribers Subsidiary (see in application)

Address: Legal address of Subscribers Subsidiary (see in application)

Contact person's name, position and contact details: Legal representative of Subscribers Subsidiary (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration (see in application)

Role: Processor

Data importer Number 2:

Name: Business Partner (see in application)

Address: Legal address of Business Partner (see in application)

Contact person's name, position and contact details: Legal representative of Business Partner (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration (see in application)

Role: Processor

Data importer Number 3:

Name: Willing & Able Licensing LLC

Address: Geronti Kikodze Street 11, 1st Floor, 0105 Tbilisi, Republic of Georgia

Contact person's name, position and contact details: see imprint of Willing & Able website

Activities relevant to the data transferred under these Clauses: Usage and provision of the application, and/or related services.

Where applicable, of its/their data protection officer and/or representative in the European Union: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., DGD Deutsche Gesellschaft für Datenschutz GmbH, Fraunhoferring 3, 85238 Petershausen, Germany

Date: Date of system registration (see in application)

Role: Processor

Data importer Number 4:

Name: Willing & Able Operations LLC

Address: Shop 141, Building 25, 1st Floor, Norashen, Ajapnyak, Yerevan, 0036, Republic of Armenia

Contact person's name, position and contact details: see imprint of Willing & Able website

Activities relevant to the data transferred under these Clauses: Usage and provision of the application, and/or related services.

Where applicable, of its/their data protection officer and/or representative in the European Union: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., DGD Deutsche Gesellschaft für Datenschutz GmbH, Fraunhoferring 3, 85238 Petershausen, Germany

Date: Date of system registration (see in application)

Role: Processor

Data importer Number 5:

Name: Willing & Able Georgia LLC

Address: Geronti Kikodze Street 11, 1st Floor, 0105 Tbilisi, Republic of Georgia

Contact person's name, position and contact details: see imprint of Willing & Able website

Activities relevant to the data transferred under these Clauses: Usage and provision of the application, and/or related services.

Where applicable, of its/their data protection officer and/or representative in the European Union: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., DGD Deutsche Gesellschaft für Datenschutz GmbH, Fraunhoferring 3, 85238 Petershausen, Germany

Date: Date of system registration (see in application)

Role: Processor

Data importer Number 6:

Name: Subscription Partner (see in application)

Address: Legal address of Subscription Partner (see in application)

Contact person's name, position and contact details: Legal representative of Subscription Partner (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration (see in application)

Role: Processor

Data importer Number 7:

Name: Franchise Partner (see in application)

Address: Legal address of Franchise Partner (see in application)

Contact person's name, position and contact details: Legal representative of Franchise Partner (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration (see in application)

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transfered

Customers	Potential customers
Employees	Business partners
Apprentices	Suppliers
Communication participants	Trainees
Service providers	Consultants
Students	Authorized Agents
Shareholders	Contact Persons
Subscribers	

Categories of personal data transfered

Names	Identification number
Location data	Online identifier
Customer data	Data of potential customers
Data of employees	Data of Business Partners
Data of apprentices	Data of suppliers
Data of communic. participants	Data of trainees
Data of service providers	Data of consultants
Data of students	Data of authorized agents
Data of shareholders	Data of contact persons
Data of subscribers	

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.

Sensitive data transferred

None

Applied restrictions or safeguards

Access restrictions

Keeping a record of access to the data

Restrictions for onward transfers

Additional security measures, see TOMs of Willing & Able.

Frequency of transfer:

The data is transferred on a continuous basis.

Nature of processing

Collection	Adaptation	Disclosure by transmission
Restriction	Recording	Alteration
Dissemination	Erasure	Organisation
Retrieval	Otherwise making available	Destruction
Structuring	Consultation	Alignment
Storage	Use	Combination

Purpose(s) of the data transfer and further processing

Usage of Online-Application of Willing & Able.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The data is retained for a longer period. The statutory retention period is used to determine the retention period.

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

Subject matter of (sub-) processing: Granting access to usage of Online-Application of Willing & Able.

Nature of (sub-) processing: Usage of Online-Application of Willing & Able.

Duration of (sub-) processing: The data is processed on a continuous basis.

C. COMPETENT SUPERVISORY AUTHORITY

Greece - Hellenic Data Protection Authority

ANNEX II

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. Measures of pseudonymization and encryption of personal data

Pseudonymisation of personal data that are no longer needed in plain text

Encryption of websites (SSL)

Encryption of e-mail (TLS 1.2 or 1.3)

2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Confidentiality and data protection agreements with employees

NDAs with third parties

Hardware- or software-firewall

Anti-Virus software

Regular backups

3. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Regular backups of the whole system

Regular test of backup and recovery

Regular training of IT staff

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

Regular review of processes by IT

Regular audits (e.g. by the DPO)

5. Measures for user identification and authorisation

Authentication with username / password

Regular checks of authorisations
Password guideline
Limitation of the number of administrators
Management of rights by system administrator
Differentiation between authorisations

6. Measures for the protection of data during transmission

Use of encryption technologies
Logging of activities and events
Encryption of email (TLS 1.2 or 1.3)
Use of company internal / restricted drives

7. Measures for the protection of data during storage

Logging of actions and events
Limitation of the number of administrator's
Firewall

8. Measures for ensuring physical security of locations at which personal data are processed

Manual locking system
Security locks
Key control

9. Measures for ensuring events logging

Logging activated on application level
Regular manual checks of logs

10. Measures for ensuring system configuration, including default configuration

Configuration change control process
Data protection by default and design is observed
Configuration only by system administrator
Regular training of IT staff

11. Measures for internal IT and IT security governance and management

IT security policy
Training of employees on data security
IT team with clear roles and responsibilities

12. Measures for certification/assurance of processes and products

Clear overview of the provisions applicable to the provided products/services/processes
Regular internal and/or external audits
Assignment of audit responsibilities to certified experts

13. Measures for ensuring data minimization

Identification of the purpose of processing
Assessment of a link between processing and purpose
Identification of the applicable retention periods for each data category
Secure erasure of the data after expiration of the retention period

14. Measures for ensuring data quality

Logging of entry and modification of data
Assignment of rights for data entry
Traceability of entry, modification of data by individual user names (not user groups)

15. Measures for ensuring limited data retention

Regular training on retention periods
Regular audit and assessment of retained data

16. Measures for ensuring accountability

Provision of training / awareness rising
Regular controls and checks
Appropriate policies on data protection
Conclusion of SCCs
Use of secure data erasure
Legal basis for processing exists for all activities
Documented privacy policy

17. Measures for allowing data portability and ensuring erasure

Personal data is stored in a structured format
Monitoring of legal deadline ensured
Observation of retention periods
Establishment of data portability process
Proper handling of data subject requests
Secure data erasure and data carrier destruction ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com (certified data erasure and destruction).

18. **For transfers to (sub-) processors, also 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**

Secure data erasure and data carrier destruction ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com (certified data erasure and destruction).
Contractually agreed on effective control rights
Contractually agreed on provision of assistance to the controller

ANNEX III
LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

See section “Sub-Processors of Personal Data” in Willing & Able SaaS Subscription and Data Processing Agreement, and/or separate document.

Section E
STANDARD CONTRACTUAL CLAUSES 2021/914
MODULE FOUR: Transfer Processor to Controller

Clause 1
Purpose and scope

(a) The purpose of these 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 between the Parties 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) The data subjects can enforce against the data exporter and/or data importer these Clauses, with the following exceptions:

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

(ii) Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 13;

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

(v) Clause 16 (e);

(vi) 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 other 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 hereunder.

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.

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 exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2. Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and 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 of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and 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 data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 10
Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11
Redress

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.

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 14
Local laws and practices affecting compliance with the Clauses

Where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU):

(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 fulfill 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

Where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU:

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.

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 collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. 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 a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18
Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Germany.

ANNEX I

A. LIST OF PARTIES

Data exporter Number 1:

Name: Subscriber (see in application)

Address: Legal address of Subscriber (see in application)

Contact person's name, position and contact details: Legal representative of Subscriber (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration of the data importer (see in application)

Role: Processor

Data exporter Number 2:

Name: Subscribers Subsidiary (see in application)

Address: Legal address of Subscribers Subsidiary (see in application)

Contact person's name, position and contact details: Legal representative of Subscribers Subsidiary (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration of the data importer (see in application)

Role: Processor

Data exporter Number 3:

Name: Willing & Able Licensing LLC

Address: Geronti Kikodze Street 11, 1st Floor, 0105 Tbilisi, Republic of Georgia

Contact person's name, position and contact details: see imprint of Willing & Able website

Activities relevant to the data transferred under these Clauses: Usage and provision of the application, and/or related services.

Where applicable, of its/their data protection officer and/or representative in the European Union: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., DGD Deutsche Gesellschaft für Datenschutz GmbH, Fraunhoferring 3, 85238 Petershausen, Germany

Date: Date of system registration of Subscriber (see in application)

Role: Processor

Data exporter Number 4:

Name: Willing & Able Operations LLC

Address: Shop 141, Building 25, 1st Floor, Norashen, Ajapnyak, Yerevan, 0036, Republic of Armenia

Contact person's name, position and contact details: see imprint of Willing & Able website

Activities relevant to the data transferred under these Clauses: Usage and provision of the application, and/or related services.

Where applicable, of its/their data protection officer and/or representative in the European Union: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., DGD Deutsche Gesellschaft für Datenschutz GmbH, Fraunhoferring 3, 85238 Petershausen, Germany

Date: Date of system registration of Subscriber (see in application)

Role: Processor

Data exporter Number 5:

Name: Willing & Able Georgia LLC

Address: Geronti Kikodze Street 11, 1st Floor, 0105 Tbilisi, Republic of Georgia

Contact person's name, position and contact details: see imprint of Willing & Able website

Activities relevant to the data transferred under these Clauses: Usage and provision of the application, and/or related services.

Where applicable, of its/their data protection officer and/or representative in the European Union: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E., DGD Deutsche Gesellschaft für Datenschutz GmbH, Fraunhoferring 3, 85238 Petershausen, Germany

Date: Date of system registration of Subscriber (see in application)

Role: Processor

Data exporter Number 6:

Name: Subscription Partner (see in application)

Address: Legal address of Subscription Partner (see in application)

Contact person's name, position and contact details: Legal representative of Subscription Partner (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration of the data importer (see in application)

Role: Processor

Data exporter Number 7:

Name: Franchise Partner (see in application)

Address: Legal address of Franchise Partner (see in application)

Contact person's name, position and contact details: Legal representative of Franchise Partner (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration of the data importer (see in application)

Role: Processor

Data importer Number 1:

Name: Business Partner (see in application)

Address: Legal address of Business Partner (see in application)

Contact person's name, position and contact details: Legal representative of Business Partner (see in application)

Activities relevant to the data transferred under these Clauses: Usage and provision of the application.

Where applicable, of its/their data protection officer and/or representative in the European Union: Name available upon request.

Date: Date of system registration (see in application)

Role: Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transfered

Customers	Potential customers
Employees	Business partners
Apprentices	Suppliers
Communication participants	Trainees
Service providers	Consultants
Students	Authorized Agents
Shareholders	Contact Persons
Subscribers	

Categories of personal data transfered

Names	Identification number
Location data	Online identifier
Customer data	Data of potential customers
Data of employees	Data of Business Partners
Data of apprentices	Data of suppliers
Data of communic. participants	Data of trainees
Data of service providers	Data of consultants
Data of students	Data of authorized agents
Data of shareholders	Data of contact persons
Data of subscribers	

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.

Sensitive data transferred

None

Applied restrictions or safeguards

Access restrictions

Keeping a record of access to the data

Restrictions for onward transfers

Additional security measures, see TOMs of Willing & Able.

Frequency of transfer:

The data is transferred on a continuous basis.

Nature of processing

Collection	Adaptation	Disclosure by transmission
Restriction	Recording	Alteration
Dissemination	Erasure	Organisation
Retrieval	Otherwise making available	Destruction
Structuring	Consultation	Alignment
Storage	Use	Combination

Purpose(s) of the data transfer and further processing

Usage of Online-Application of Willing & Able.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The data is retained for a longer period. The statutory retention period is used to determine the retention period.

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

Subject matter of (sub-) processing: Granting access to usage of Online-Application of Willing & Able.

Nature of (sub-) processing: Usage of Online-Application of Willing & Able.

Duration of (sub-) processing: The data is processed on a continuous basis.

APPENDIX 5 (Swiss Transborder Data Flow Agreement)

Swiss Transborder Data Flow Agreement

by and between the

PARTY 1

(hereinafter Data Exporter)

and the

PARTY 2

(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.

ANNEX1 TO THE SWISS TRNSBOARDER DATA FLOW AGREEMENT

Description of the Transfer and Processing

1. Catalogue of Personal Data to be transferred and processed:

Data Subjects: Subscribers, Potential Subscribers, Employees, Employees of Third Parties, Business Partners, Suppliers, Communication Participants, Contractual Partners, Service Providers, Consultants, Freelancers, Authorized Agents, Data Protection Officers.

2. Purpose(s) of the transfer and processing:

Provision and use of SaaS Application(s).

3. Categories of the Persons Affected:

Subscribers, Potential Subscribers, Employees, Employees of Third Parties, Business Partners, Suppliers, Communication Participants, Contractual Partners, Service Providers, Consultants, Freelancers, Authorized Agents, Data Protection Officers, HR Contact Persons, Names, Address Data, Contact Information, Location data, Identification numbers, Online identifiers, Security identifiers, Other Identifiers, Factors specific to the economic identity.

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:

Willing & Able Operations LLC
Shop 141, Building 25, 1st Floor
Norashen, Ajapnyak
Yerevan, 0036
Republic of Armenia
Managing Director: Davit Mnatsakanyan

Registration No.: 271.110.1077503
Code of legal entity: 51649254
TPAN: 01 292739
Insurer's code: 49117503
E-Mail: dpo@willing-able.com

APPENDIX 6 (Joint Controllership Agreement between the Provider and FranchisePartner or Subscription Partner)

Joint Controllership Agreement between the Provider and FranchisePartner or Subscription Partner in accordance with Art. 26 GDPR

between

the Provider

(hereinafter referred to as "**Controller 1**")

and

the FranchisePartner

or the SubscriptionPartner

(hereinafter referred to as "**Controller 2**")

Preamble

The controllers have jointly defined the purposes and means of processing described in this agreement. In this respect, they qualify as joint controllers within the meaning of Art. 26(1), 4 No. 7 GDPR. This Agreement governs the rights and obligations of the two controllers with respect to joint controllership.

The following Agreement shall apply only to activities and services that are jointly managed, provided or otherwise incorporated by both controllers.

§ 1 Definitions

The legal definitions from Art. 4 GDPR shall apply. In addition, the following definitions are applicable to this agreement:

Main Contract is any Agreement between the two controllers, in which other contractual obligations of the controllers are specified.

Contractor is any processor or other service provider within the meaning of Art. 28 or Chapter V GDPR whose services are required and/or used by the respective controller for the provision or performance of tasks that are specified in this Agreement or in the Main Contract.

Third Country is any country outside the European Union (EU) or the European Economic Area (EEA).

Secure Data Deletion means repeated overwriting of a data carrier, partitions, or individual files with random characters or characters that match a particular pattern that ensures that previously stored data is unrecoverable.
Data Carrier Destruction is the physical destruction of a data carrier.

§ 2 Subject Matter of Processing

2.1 The subject matter of processing is specified in the Main Contract. All mutually deliverables are governed exclusively by the Main Contract.

2.2 The purpose of joint Personal Data processing is: Providing of SaaS Applications to achieve a mutual benefit.

2.3 Processed categories of Personal Data are: Subscribers, Potential Subscribers, Employees, Employees of Third Parties, Business Partners, Suppliers, Communication Participants, Contractual Partners, Service Providers, Consultants, Freelancers, Authorized Agents, Data Protection Officers, HR Contact Persons, Names, Address Data, Contact Information, Location data, Identification numbers, Online identifiers, Security identifiers, Other Identifiers, Factors specific to the economic identity.

§ 3 Duration of the Agreement

3.1 The duration of this Agreement is based on the duration of the Main Contract. This Agreement ends simultaneously with the Main Contract.

3.2 The right to termination without notice due to material breach of this Agreement remains unaffected.

3.3 Termination requires prior written notice to be effective.

§ 4 Extraordinary Termination

4.1 Both controllers may terminate this Agreement at any time without notice in the event that the other controller seriously breaches any laws or regulations on Data Protection which are valid in the European Union or Member States, or other provisions of this Agreement. A serious breach is, inter alia, if a controller has not fulfilled all obligations set out in this Agreement.

4.2 In case of any breach by one of the controllers, the other controller shall set a reasonable deadline for remedy. If the remedy does not occur in time, the latter is entitled to extraordinary termination.

§ 5 Allocation of Responsibilities

5.1 Each controller ensures compliance with all laws and legal provisions applicable, in particular, the legality of the operations performed when processing Personal Data. However, both controllers shall be equally responsible for the lawfulness of joint processing.

5.2 The location of Controller 1 shall be deemed to be the Principal place of business and reference for determination of the competent supervisory authority.

§ 6 Ensuring Transparency Information & Data Subject Rights

6.1 Controller 1 provides the Data Subject with the transparency information required under Art. 13 and 14 GDPR.

6.2 Both controllers shall implement Technical and Organizational Measures to fulfil, within the statutory time limits, the rights of the Data Subjects resulting from Chapter III GDPR.

6.3 Controller 1 undertakes to provide the Data Subject with the information to which they are entitled according to Art. 15 GDPR and shall ensure that the Data Subject's rights can be exercised in full.

6.4 Controller 1 acts as a contact point for Data Subjects.

§ 7 Provision According to Art. 26 (2) Sentence 2 GDPR

Controller 1 provides the Data Subjects with the substance of this Agreement in a transparent manner. This means, that the complete language of this Agreement is made available to the public as an Appendix to the SaaS Subscription and Data Processing Agreement.

§ 8 Processing Activities and Functionality of the SaaS Applications

8.1 Controller 1 is responsible for all processing activities and all functionality implemented or provided by the SaaS Applications.

§ 9 General Responsibilities of the Controllers

9.1 Controller 2 shall inform Controller 1 immediately, if any bugs, errors or irregularities are discovered by him or Third Parties during the use or examination of the SaaS Applications.

9.2 Each controller shall inform the other controller if Data Protection inquiries are made in connection with the other controller or joint controllership.

9.3 Controller 1 maintains the directory of processing activities (Art. 30 GDPR).

9.4 Controller 1 is responsible for the obligations resulting from Art. 33 and Art. 34 GDPR.

9.5 If a Data Protection Impact Assessment (hereinafter referred to as "DPIA") (Art. 35 GDPR) is required, the DPIA will be carried out by Controller 1.

9.6 If a Legitimate Interest Assessment (hereinafter referred to as "LIA") (Art. 6 (1) (f) GDPR) is required, the LIA will be carried out by Controller 1.

9.7 Each controller agrees to keep Technical and Organizational Measures of the other controller confidential as long as they are not published or otherwise made public by the other controller.

9.8 Insofar as required by law, the controllers shall designate a Data Protection Officer. In the absence of a legal obligation, they shall designate a contact person with the rights and duties to make decisions in regards to Data Protection. A change of the Data Protection Officer or a contact person shall be communicated to the other controller.

§ 10 Ensuring Confidentiality

10.1 Each controller declares that all persons entrusted by him with data processing have signed confidentiality/Data Protection agreements with the controller before commencing processing activities or are subject to statutory duty of confidentiality, and that such agreements or statutory duties continue to apply after termination of their employment, freelancer status or other contractual relationship.

10.2 Each controller declares that all persons engaged by him for any activities have signed agreements and are obligated to protect trade secrets, business secrets and professional secrets of the controller and Third Parties or are subject to statutory duty of confidentiality in this regard, and that such agreements or statutory duties continue to apply after termination of their employment, freelancer status or other contractual relationship.

§ 11 Ensuring Safety of Processing

11.1 Both controllers shall organize their activities in such way that they meet the requirements of applicable IT security laws, including Data Protection laws and regulations. Each controller shall adopt appropriate Technical and Organizational Measures to safeguard Personal Data from misuse and loss and comply with the requirements of law and modern standards of Data Protection. The Technical and

Organizational Measures of both controllers have been exchanged, and are checked and controlled.

11.2 The Technical and Organizational Measures are subject to technical progress and further development. In this regard, each controller is allowed to and shall implement from time to time alternative, but demonstrably adequate or better measures. Each controller shall ensure that the contractually agreed level of protection is not undercut.

§ 12 Data Carrier Destruction and Secure Data Deletion

12.1 The controllers agree that Data Carrier Destruction and Secure Data Deletion shall be carried out in accordance with GDPR.

12.2 When required, Controller 1 shall carry out Data Carrier Destruction and Secure Data Deletion.

§ 13 Processor

13.1 Each controller shall conclude an Agreement in accordance with Art. 28 GDPR or fulfil the conditions laid down in Chapter V of GDPR with each of its processors, if the processor should act within the scope of joint controllership.

13.2 The other controller has the right to prohibit the commissioning of a processor for important reasons. The alleged unreliability of a processor should be understood as an important reason.

13.3 Each processor should provide, if possible, its services in the European Union (EU) or in the European Economic Area (EEA). Where a service is provided, in whole or in part, by a processor in a Third Country, both controllers shall give their consent to the transfer of Personal Data to the Third Country.

13.4 Each controller shall ensure that all processors used by him have designated a Data Protection Officer, if the processor is legally obliged to do so. If there is no legal obligation to designate a Data Protection Officer, the processor shall provide the respective controller with a contact person that has the right and obligation to make decisions on Data Protection.

§ 14 Liability

14.1 For damages caused to a Data Subject, both controllers are jointly liable towards the Data Subject.

14.2 Each controller is liable to the other controller for such damages that are attributable to him.

14.3 Further liability claims under applicable laws and regulations remain unaffected.

§ 15 Supplement by the European Union and Member State Law

15.1 In addition to the provisions of this agreement, the European Union law, in particular the General Data Protection Regulation and the Data Protection law of the Member States, apply internally between the controllers.

15.2 If the controllers are subject to obligations under EU or Member State law not included in this Agreement, such provisions shall automatically be deemed to have been agreed between the parties in accordance with the spirit and purpose of this Agreement as they would have been agreed upon by two controllers who are in compliance with Data Protection law.

§ 16 Arbitration Clause

16.1 All disputes arising out of or in connection with this Agreement or its validity shall be finally settled in accordance with the Arbitration Rules of the German Arbitration Institute (DIS) without recourse to the ordinary courts of law.

16.2 The arbitral tribunal shall be comprised of a sole arbitrator.

16.3 The seat of the arbitration is Munich, Germany. For economic reasons, both parties agree to online arbitration and will use any online meeting system provided by the arbitrator.

16.4 The language of the arbitration shall be German.

16.5 The rules of law applicable to the merits shall be German Law.

16.6 The parties jointly nominate the following Attorney at Law to act as the arbitrator:

Ulrich Baumann

c/o CORPLEGAL

Prinzregentenstr. 22

80538 Munich (Germany)

Telephone: +49 (0)89 / 23 23 73 6-0

Telefax: +49 (0)89 / 23 23 73 6-91

E-Mail: mail@corplegal.global

16.7 The arbitrator can assign the case to another arbitrator without obtaining consent of the parties.

16.8 The arbitrator and contact details set out may be updated from time to time. Controller 2 hereby agrees that Controller 1 may change the arbitrator on its own discretion.

§ 17 Severability Clause

17.1 If any provision of this Agreement is determined by any court or other competent authority to be unlawful and/or unenforceable, the other provisions of this Agreement will continue in effect. If any unlawful and/or unenforceable provision would be lawful or enforceable if part of it were deleted, that part will be deemed to be deleted, and the rest of the provision will continue in effect, unless that would contradict the clear intention of the parties, in which case the entirety of the relevant provision will be deemed to be deleted.

17.2 If the Controllers disagree on a provision that is to be supplemented and necessary, they shall appeal to the Arbitral Tribunal.

APPENDIX 7 (Joint Controllership Agreement between the Subscribers and a Subsidiary)

Joint Controllership Agreement between the Subscriber and a Subsidiary in accordance with Art. 26 GDPR

between

the Subscriber

(hereinafter referred to as "**Controller 1**")

and

the Subsidiary of the Subscriber

(hereinafter referred to as "**Controller 2**")

Preamble

The controllers have jointly defined the purposes and means of processing described in this agreement. In this respect, they qualify as joint controllers within the meaning of Art. 26(1), 4 No. 7 GDPR. This Agreement governs the rights and obligations of the two controllers with respect to joint controllership.

The following Agreement shall apply only to activities and services that are jointly managed, provided or otherwise incorporated by both controllers.

§ 1 Definitions

The legal definitions from Art. 4 GDPR shall apply. In addition, the following definitions are applicable to this agreement:

Main Contract is any Agreement between the two controllers, in which other contractual obligations of the controllers are specified.
Contractor is any processor or other service provider within the meaning of Art. 28 or Chapter V GDPR whose services are required and/or used by the respective controller for the provision or performance of tasks that are specified in this Agreement or in the Main Contract.
Third Country is any country outside the European Union (EU) or the European Economic Area (EEA).

Secure Data Deletion means repeated overwriting of a data carrier, partitions, or individual files with random characters or characters that match a particular pattern that ensures that previously stored data is unrecoverable.
Data Carrier Destruction is the physical destruction of a data carrier.

§ 2 Subject Matter of Processing

2.1 The subject matter of processing is specified in the Main Contract. All mutually deliverables are governed exclusively by the Main Contract.

2.2 The purpose of joint Personal Data processing is: Joint usage of SaaS Applications.

2.3 Processed categories of Personal Data are: Subscribers, Potential Subscribers, Employees, Employees of Third Parties, Business Partners, Suppliers, Communication Participants, Contractual Partners, Service Providers, Consultants, Freelancers, Authorized Agents, Data Protection Officers, HR Contact Persons, Names, Address Data, Contact Information, Location data, Identification numbers, Online identifiers, Security identifiers, Other Identifiers, Factors specific to the economic identity.

§ 3 Duration of the Agreement

3.1 The duration of this Agreement is based on the duration of the Main Contract. This Agreement ends simultaneously with the Main Contract.

3.2 The right to termination without notice due to material breach of this Agreement remains unaffected.

3.3 Termination requires prior written notice to be effective.

§ 4 Extraordinary Termination

4.1 Both controllers may terminate this Agreement at any time without notice in the event that the other controller seriously breaches any laws or regulations on Data Protection which are valid in the European Union or Member States, or other provisions of this Agreement. A serious breach is, inter alia, if a controller has not fulfilled all obligations set out in this Agreement.

4.2 In case of any breach by one of the controllers, the other controller shall set a reasonable deadline for remedy. If the remedy does not occur in time, the latter is entitled to extraordinary termination.

§ 5 Allocation of Responsibilities

5.1 Each controller ensures compliance with all laws and legal provisions applicable, in particular, the legality of the operations performed when processing Personal Data. However, both controllers shall be equally responsible for the lawfulness of joint processing.

5.2 The location of Controller 1 shall be deemed to be the Principal place of business and reference for determination of the competent supervisory authority.

§ 6 Ensuring Transparency Information & Data Subject Rights

6.1 The transparency information required under Art. 13 and 14 GDPR is published by the Provider of the SaaS Application.

6.2 Both controllers shall implement Technical and Organizational Measures to fulfil, within the statutory time limits, the rights of the Data Subjects resulting from Chapter III GDPR.

6.3 Controller 1 undertakes to provide the Data Subject with the information to which they are entitled according to Art. 15 GDPR and shall ensure that the Data Subject's rights can be exercised in full.

6.4 Controller 1 acts as a contact point for Data Subjects.

§ 7 Provision According to Art. 26 (2) Sentence 2 GDPR

Controller 1 provides the Data Subjects with the substance of this Agreement in a transparent manner. This means, that the complete language of this Agreement is made available to the public as an Appendix to the SaaS Subscription and Data Processing Agreement.

§ 8 Processing Activities and Functionality of the SaaS Applications

8.1 Controller 1 is responsible for all processing activities and all functionality implemented or provided by the SaaS Applications.

§ 9 General Responsibilities of the Controllers

9.1 Controller 2 shall inform Controller 1 immediately, if any bugs, errors or irregularities are discovered by him or Third Parties during the use or examination of the SaaS Applications.Each controller shall inform the other controller if Data Protection inquiries are made in connection with the other controller or joint controllership.

9.3 Controller 1 maintains the directory of processing activities (Art. 30 GDPR).

9.4 Controller 1 is responsible for the obligations resulting from Art. 33 and Art. 34 GDPR.

9.5 If a Data Protection Impact Assessment (hereinafter referred to as "DPIA") (Art. 35 GDPR) is required, the DPIA will be carried out by Controller 1.

9.6 If a Legitimate Interest Assessment (hereinafter referred to as "LIA") (Art. 6 (1) (f) GDPR) is required, the LIA will be carried out by Controller 1.

9.7 Each controller agrees to keep Technical and Organizational Measures of the other controller confidential as long as they are not published or otherwise made public by the other controller.

9.8 Insofar as required by law, the controllers shall designate a Data Protection Officer. In the absence of a legal obligation, they shall designate a contact person with the rights and duties to make decisions in regards to Data Protection. A change of the Data Protection Officer or a contact person shall be communicated to the other controller.

§ 10 Ensuring Confidentiality

10.1 Each controller declares that all persons entrusted by him with data processing have signed confidentiality/Data Protection agreements with the controller before commencing processing activities or are subject to statutory duty of confidentiality, and that such agreements or statutory duties continue to apply after termination of their employment, freelancer status or other contractual relationship.

10.2 Each controller declares that all persons engaged by him for any activities have signed agreements and are obligated to protect trade secrets, business secrets and professional secrets of the controller and Third Parties or are subject to statutory duty of confidentiality in this regard, and that such agreements or statutory duties continue to apply after termination of their employment, freelancer status or other contractual relationship.

§ 11 Ensuring Safety of Processing

11.1 Both controllers shall organize their activities in such way that they meet the requirements of applicable IT security laws, including Data Protection laws and regulations. Each controller shall adopt appropriate Technical and Organizational Measures to safeguard Personal Data from misuse and loss and comply with the requirements of law and modern standards of Data Protection. The Technical and Organizational Measures of both controllers have been exchanged, and are checked and controlled.

11.2 The Technical and Organizational Measures are subject to technical progress and further development. In this regard, each controller is allowed to and shall implement from time to time alternative, but demonstrably adequate or better measures. Each controller shall ensure that the contractually agreed level of protection is not undercut.

§ 12 Data Carrier Destruction and Secure Data Deletion

12.1 The controllers agree that Data Carrier Destruction and Secure Data Deletion shall be carried out in accordance with GDPR.

12.2 When required, Controller 1 shall carry out Data Carrier Destruction and Secure Data Deletion.

§ 13 Processor

13.1 Each controller shall conclude an Agreement in accordance with Art. 28 GDPR or fulfil the conditions laid down in Chapter V of GDPR with each of its processors, if the processor should act within the scope of joint controllership.

13.2 The other controller has the right to prohibit the commissioning of a processor for important reasons. The alleged unreliability of a processor should be understood as an important reason.

13.3 Each processor should provide, if possible, its services in the European Union (EU) or in the European Economic Area (EEA). Where a service is provided, in whole or in part, by a processor in a Third Country, both controllers shall give their consent to the transfer of Personal Data to the Third Country.

13.4 Each controller shall ensure that all processors used by him have designated a Data Protection Officer, if the processor is legally obliged to do so. If there is no legal obligation to designate a Data Protection Officer, the processor shall provide the respective controller with a contact person that has the right and obligation to make decisions on Data Protection.

§ 14 Liability

14.1 For damage caused to a Data Subject, both controllers are jointly liable towards the Data Subject.

14.2 Each controller is liable to the other controller for such damages that are attributable to him.

14.3 Further liability claims under applicable laws and regulations remain unaffected.

§ 15 Supplement by the European Union and Member State Law

15.1 In addition to the provisions of this agreement, the European Union law, in particular the General Data Protection Regulation and the Data Protection law of the Member States, apply internally between the controllers.

15.2 If the controllers are subject to obligations under EU or Member State law not included in this Agreement, such provisions shall automatically be deemed to have been agreed between the parties in accordance with the spirit and purpose of this Agreement as they would have been agreed upon by two controllers who are in compliance with Data Protection law.

§ 16 Arbitration Clause

16.1 All disputes arising out of or in connection with this Agreement or its validity shall be finally settled in accordance with the Arbitration Rules of the German Arbitration Institute (DIS) without recourse to the ordinary courts of law.

16.2 The arbitral tribunal shall be comprised of a sole arbitrator.

16.3 The seat of the arbitration is Munich, Germany. For economic reasons, both parties agree to online arbitration and will use any online meeting system provided by the arbitrator.

16.4 The language of the arbitration shall be German.

16.5 The rules of law applicable to the merits shall be German Law.

16.6 The parties jointly nominate the following Attorney at Law to act as the arbitrator:

Ulrich Baumann

c/o CORPLEGAL

Prinzregentenstr. 22

80538 Munich (Germany)

Telephone: +49 (0)89 / 23 23 73 6-0

Telefax: +49 (0)89 / 23 23 73 6-91

E-Mail: mail@corplegal.global

16.7 The arbitrator can assign the case to another arbitrator without obtaining consent of the parties.

16.8 The arbitrator and contact details set out may be updated from time to time. Controller 2 hereby agrees that Controller 1 may change the arbitrator on its own discretion.

§ 17 Severability Clause

17.1 If any provision of this Agreement is determined by any court or other competent authority to be unlawful and/or unenforceable, the other provisions of this Agreement will continue in effect. If any unlawful and/or unenforceable provision would be lawful or enforceable if part of it were deleted, that part will be deemed to be deleted, and the rest of the provision will continue in effect, unless that would contradict the clear intention of the parties, in which case the entirety of the relevant provision will be deemed to be deleted.

17.2 If the Controllers disagree on a provision that is to be supplemented and necessary, they shall appeal to the Arbitral Tribunal.

APPENDIX 8 (Standard Contractual Clauses for International Transfers from Controllers to Processors for the United Kingdom)

Parties Name of the data exporting organisation:	PARTY 1 (the data **exporter**")
Name of the data importing organisation:	PARTY 2 (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 importer[1]	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

[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.

	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, by the 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.
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 Clauses[2]. 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

[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.

	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.

Appendix 1

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

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Please select one option:

The data exporter is (please specify briefly your activities relevant to the transfer):

User of the SaaS Applications.

The data exporter's business or organisation type is:

General Business or Body

The data exporter is using the personal data which is being transferred for the following purposes or activities:

The data exporter is using the personal data which is being transferred for the following purposes or activities:

Staff administration, including permanent and temporary staff, including appointment or removals, pay, discipline; superannuation, work management, and other personnel matters in relation to the data exporter's staff.

Administration of justice, including internal administration and management of courts of law, or tribunals and discharge of court business.

Consultancy and advisory services, including giving advice or rendering professional services, and the provision of services of an advisory, consultancy or intermediary nature.

Education, including the provision of education or training as a primary function or as a business activity.

Health administration and services, including the provision and administration of patient care.

Information and databank administration, including the maintenance of information or databanks as a reference tool or general resource. This includes catalogues, lists, directories and bibliographic databases.

IT, digital, technology or telecom services, including use of technology products or services, telecoms and network services, digital services, hosting, cloud and support services or software

Legal services, including advising and acting on behalf of clients.

Licensing and registration, including the administration of licensing or maintenance of official registers.

Procurement, including deciding whether to accept any person or organisation as a supplier, and the administration of contracts, performance measures and other records.

Data importer

The data importer is (please specify briefly your activities relevant to the transfer):

Provider or User of the SaaS Applications.

The data importer's business or organisation type is:

General Business or Body

The data importer's activities for the data exporter, which are relevant to the transfer are:

Consultancy and general advisory services.

Education or training services.

Information and databank administration, including the maintenance of information or databanks as a reference tool or general resource. This includes catalogues, lists, directories and bibliographic databases.

IT, digital, technology or telecom services, including provision of technology products or services, telecoms and network services, digital services, hosting, cloud and support services or software licensing

Legal administration and legal support services.

Staff administration services, including appointment or removals, pay, discipline; superannuation, training, employee benefits, work management, and other personnel matters in relation to the data exporter's staff.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Each category includes current, past and prospective data subjects. Where any of the following is itself a business or organisation, it includes their staff.

staff including volunteers, agents, temporary and casual workers

customers and clients (including their staff)

suppliers (including their staff)

members or supporters

shareholders

relatives, guardians and associates of the data subject

complainants, correspondents and enquirers;

experts and witnesses

advisers, consultants and other professional experts

Categories of data

The personal data transferred concern the following categories of data (please specify):

The following is a list of standard descriptions of categories of data:

Personal details, including any information that identifies the data subject and their personal characteristics, including: name, address, contact details, age, date of birth, sex, and physical description.

Education and training details, including information which relates to the education and any professional training of the data subject, including academic records, qualifications, skills, training records, professional expertise, student and pupil records.

Employment details, including information relating to the employment of the data subject, including employment and career history, recruitment and termination details, attendance records, health and safety records, performance appraisals, training records, and security records.

Goods or services provided and related information, including details of the goods or services supplied, licences

issued, and contracts.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Personal data which is on, which reveals, or which concerns:

none

Processing operations

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

Receiving data, including collection, accessing, retrieval, recording, and data entry

Holding data, including storage, organisation and structuring

Using data, including analysing, consultation, testing, automated decision making and profiling

Updating data, including correcting, adaptation, alteration, alignment and combination

Protecting data, including restricting, encrypting, and security testing

Sharing data, including disclosure, dissemination, allowing access or otherwise making available

Returning data to the data exporter or data subject

Erasing data, including destruction and deletion

Appendix 2

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

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

See description of the importer's security measures set out in the Agreement above or separate document.