DATA PROTECTION ADDENDUM

This Data Protection Addendum ("**Addendum**") is incorporated by reference into the Service Agreement ("**Principal Agreement**") between ONSOLVE, LLC and its Affiliates ("**OnSolve**") and the company that executed the Principal Agreement (**"Company"**) acting on its own behalf and as agent for any Company Affiliate. This Addendum is effective as of the last date signed below. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

1. Definitions

1.1 Capitalized terms not otherwise defined below shall have the meaning given to them in the Principal Agreement.

1.2 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.2.1 "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership of a party to this Addendum, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

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

1.2.3 "**Company Personal Data Breach**" means a Personal Data Breach affecting Company Personal Data;

1.2.4 "**Contracted Processor**" means OnSolve or a Subprocessor;

1.2.5 "**Data Protection Laws**" means, to the extent applicable, UK and EU Data Protection Laws, the California Consumer Privacy Act (the "CCPA"), the California Privacy Rights Act (the "CPRA") (when it enters into force), the Colorado Privacy Act (the "CPA"), the Connecticut Data Privacy Act (the "CTDPA"), the Virginia Consumer Data Protection Act (the "VCDPA"), the Utah Consumer Privacy Act (the "UCPA"), and the data protection or privacy laws and regulations of any other country or jurisdiction;

1.2.6 "**Data Subject**" means any natural personal that to which any piece of "personal data" pertains, including a "consumer," "data subject," or similar term as defined under the Data Protection Laws.

1.2.7 "**UK and EU Data Protection Laws**" means all laws and regulations of the United Kingdom, the European Union, the European Economic Area (EEA), and their member states, applicable to the processing of Personal Data under the Principal Agreement, as amended or replaced from time to time, including without limitation in respect of the European Union the GDPR and in respect of the United Kingdom the UK GDPR;

1.2.8 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.2.9 "**Personal Data**" means any information that is considered "personally identifiable information," "personal information," "personal data," or like terms under applicable Data Protection Laws, including, but not limited to, information regarding or reasonably capable of being associated with an identifiable individual, device, or household. Personal Data may relate to any individual, including a current, prospective or former customer, employee, vendor or Data Subject of any Party and includes such information in any form, including paper and electronic forms. For avoidance of doubt, Personal Data shall not include anonymous, aggregated, or de-identified data to the extent such data is exempted or excluded from regulation under applicable Data Protection Laws.

1.2.10 "**Restricted Transfer**" means:

1.2.10.1 a transfer of Company Personal Data from Company to a Contracted Processor; or
1.2.10.2 an onward transfer of Company Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor.

In each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses;

1.2.11 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of OnSolve for Company pursuant to the Principal Agreement;

1.2.12 "**Standard Contractual Clauses**" means: in respect of transfers of personal data which are subject to the UK GDPR, the contractual clauses set out in Schedule 4, amended as indicated (in square brackets and italics) in that Schedule and under section12.4; and, in respect of transfers of personal data which are subject to the GDPR, the contractual clauses set out in Schedule 5 amended as indicated (in square brackets and italics) in that Schedule and under section 12.4;

1.2.13 "**Subprocessor**" means any entity appointed by or on behalf of OnSolve to Process Personal Data on behalf of Company in connection with the Principal Agreement;

1.2.14 "**UK GDPR**" means the GDPR, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018; and

1.3 The terms, "**Commission,**" "**Controller,**" "**Member State,**" "**Personal Data Breach,**" "**Processing,**" "**Service Provider,**" and "**Supervisory Authority**" shall have the same meaning as in the applicable Data Protections Laws, and their cognate terms shall be construed accordingly.

1.4 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 The Company warrants to OnSolve that:

2.1.1 it has all necessary rights to authorise OnSolve to process Company Personal Data in accordance with this Agreement and the Data Protection Laws; and

2.1.2 its instructions to OnSolve relating to processing of Company Personal Data will not put OnSolve in breach of Data Protection Laws.

2.2 Schedule 1 to this Addendum sets out the Processing instructions, as required by article 28(3) of the GDPR and the UK GDPR and equivalent requirements of other Data Protection Laws. Nothing in Schedule 1 (including as amended pursuant to this section 2.3) confers any right or imposes any obligation on any party to this Addendum.

2.3 OnSolve shall:

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

2.3.2 provide the same level of privacy protection to Personal Data as required of the Company under all applicable Data Protection Laws;

2.3.3 not further collect, sell, use, retain, disclose or otherwise Process Company Personal Data other than on the Company's documented instructions pursuant to the Company's specified business purpose, unless Processing is required by applicable laws to which the relevant Contracted Processor is subject, in which case OnSolve shall, to the extent permitted by applicable laws, inform the Company of that legal requirement before the relevant Processing of that Personal Data;

2.3.4 not sell Personal Data on behalf of the Company when a Data Subject has opted-out of the sale of their Personal Information with the Company under applicable Data Protection Laws, regardless of the instruction of the Company;

2.3.5 not sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, any Company Personal Data outside of the business relationship between OnSolve and the Company and in no event to another business or a third party for monetary or other valuable consideration unless expressly permitted by Data Protection Laws;

2.3.6 not Process any Personal Data for the purposes of cross-contextual behavioral advertising, as that term is defined and interpreted under Data Protection Laws;

2.3.7 not combine Company Personal Data with Personal Data it receives from or on behalf of another person or persons, or that it collects from its own interactions; and

2.3.8 notify the Company within five business days if it makes the determination that it can no longer meet its obligations under applicable Data Protection Laws or this Addendum.

2.4 OnSolve hereby certifies that it understands its contractual restrictions under Section 2.3 and shall comply with them.

2.5 Each Party shall be individually responsible for complying with the obligations imposed on it by Data Protection Laws. Neither Party shall be liable for the other Party's failure to comply with Data Protection Laws.

3. OnSolve

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

4. Security

4.1 As further detailed in Schedule 2, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, OnSolve shall in relation to the Company Personal Data implement appropriate technical and organizational measures designed to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR and the UK GDPR.

5. Sub-processing

5.1 OnSolve may continue to use those Sub-processors listed in Schedule 3.

5.2 OnSolve shall give Company prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within twenty (20) business days of receipt of that notice, Company notifies OnSolve in writing of any objections (on reasonable grounds) to the proposed appointment:

5.2.1 OnSolve shall work with Company in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; and

5.2.2 where such a change cannot be made within forty-five (45) days from OnSolve 's receipt of Company's notice, notwithstanding anything in the Principal Agreement, Company may by written notice to OnSolve with immediate effect terminate the Principal Agreement to the extent that it relates to the Services which require the use of the proposed Subprocessor.

5.3 With respect to each Subprocessor, OnSolve shall ensure that Subprocessor is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this Addendum and meet the requirements of Data Protection Laws, including article 28(3) of the GDPR.

5.4 Before the Sub-processor first processes Company Personal Data, OnSolve shall carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data as required by Data Protection Laws.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, OnSolve shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company's obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 OnSolve shall:

6.2.1 promptly notify Company if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that the Contracted Processor does not respond to that request, other than to confirm necessary details if required, except on the documented instructions of Company or as required by applicable laws to which the Contracted Processor is subject, in which case OnSolve shall, to the extent permitted by applicable law, inform Company of that legal requirement before the Contracted Processor responds to the request. For requests from California residents, OnSolve shall either act on behalf of Company in responding to the request in accordance with Company's instructions or inform the Data Subject that the request cannot be acted upon because the request has been sent to a Service Provider.

6.3 Without limiting the foregoing, for requests to delete, OnSolve shall, upon notification by Company, comply with the Data Subject request to delete by:

6.3.1 permanently and completely erasing the Data Subject's Personal Data from its existing systems except archived or back-up systems, deidentifying the personal information, or aggregating the Personal Data;

6.3.2 to the extent that an exception applies to the deletion of Personal Data, deleting the Data Subject's Personal Data that is not subject to the exception and refraining from using the Data Subject's Personal Data retained for any purpose other than the purpose provided for by that exception;

6.3.3 notifying any of its Subprocessors to delete from their records in the same manner the Data Subject's Personal Data obtained in the course of providing services; and

6.3.4 notifying any other Contracted Processor that may have accessed Personal Data from or through OnSolve, unless the information was accessed at the direction of Company, to delete the Data

Subject’s Personal Data unless this proves impossible or involves disproportionate effort. If any Contracted Processor determines that such a notification is impossible or would involve disproportionate effort, the Contracted Processor shall provide Company a detailed explanation that shall be relayed to the Data Subject that includes enough facts to give a Data Subject a meaningful understanding as to why the notification was not possible or involved disproportionate effort.

7. Company Personal Data Breach

7.1 OnSolve shall notify Company without undue delay upon OnSolve becoming aware of a Company Personal Data Breach.

7.2 OnSolve shall co-operate with Company and take such reasonable commercial steps to assist in the investigation, mitigation and remediation of each such Company Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

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

9. Deletion of Company Personal Data

9.1 At the option of the Company, OnSolve will delete or return to the Company all Company Personal Data after the end of the provision of Services relating to processing and delete any remaining copies. OnSolve will be entitled to retain any Company Personal Data required to comply with any applicable law or which it is required to retain for insurance, accounting, taxation or record keeping purposes.

10. Audit rights

10.1 OnSolve shall make available to the Company on request all information necessary to demonstrate compliance with this Addendum and will allow for and contribute to audits, including inspections, conducted by the Company or another auditor mandated by the Company, provided that the Company gives OnSolve reasonable prior written notice of each such audit and that each audit is carried out upon execution of a specific nondisclosure agreement, and at the Company’s cost, during regular business hours, so as to cause the minimum disruption to OnSolve’s business and without the Company or its auditor having any access to any data belonging to a customer other than the Company. For the avoidance of doubt, any materials disclosed during such audits and the results of and/or outputs from such audits will be kept confidential by the Company.

10.2 OnSolve will only be required to submit to one audit or inspection in any calendar year, except for any additional audits or inspections which:

10.2.1 Company reasonably considers necessary because a Company Personal Data Breach, or

10.2.2 Company is required to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory

10.3 Company has the right, upon notice to OnSolve, to take reasonable and appropriate steps to stop and remediate any Contracted Processor’s unauthorized use of Personal Data.

10.4 Information and audit rights of the Company only arise under section 10.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of applicable Data Protection Lawa (including, where applicable, article 28(3)(h) of the GDPR and the UK GDPR).

11. Restricted Transfers

11.1 Subject to section 11.3, the Company (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into:

11.1.1 in respect of a Restricted Transfer of Customer Personal Data which is subject to the UK GDPR, the Standard Contractual Clauses set out in Schedule 4 in respect of any Restricted Transfer from the Company to that Contracted Processor; and

11.1.2 in respect of a Restricted Transfer of Customer Personal Data which is subject to the GDPR, the Standard Contractual Clauses set out in Schedule 5 in respect of any Restricted Transfer from the Company to that Contracted Processor.

11.2 The relevant Standard Contractual Clauses shall come into effect under section 11.1 on the later of:

11.2.1 the data exporter becoming a party to them;

11.2.2 the data importer becoming a party to them; and

11.2.3 commencement of the relevant Restricted Transfer.

11.3 Section 11.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

12. General Terms

Governing law and jurisdiction

12.1 Without prejudice to clauses 17 (Governing law) and 18 (Choice of forum and jurisdiction) of the Standard Contractual Clauses contained in Schedule 5, and clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses contained in Schedule 4:

12.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

12.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

Order of precedence

12.2 Nothing in this Addendum reduces OnSolve's obligations under the Principal Agreement in relation to the protection of Personal Data or permits OnSolve to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

12.3 Subject to section 12.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

12.4 Company may:

12.4.1 by at least 30 (thirty) calendar days’ written notice to OnSolve from time to time make any variations to the Standard Contractual Clauses (including any relevant Standard Contractual Clauses entered into under section 12.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

12.4.2 propose any other variations to this Addendum which Company reasonably considers to be necessary to address the requirements of any Data Protection Law.

12.5 If Company gives notice under section 12.4.1:

12.5.1 Company shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by OnSolve to protect the Contracted Processors against additional risks associated with the variations made under section 12.4.1.

12.6 If Company gives notice under section 12.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Company's notice as soon as is reasonably practicable.

12.7 Neither Company nor OnSolve shall require the consent or approval of any Company Affiliate or OnSolve Affiliate to amend this Addendum pursuant to this section 12.5 or otherwise.

Severance

12.8 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

Company	**OnSolve, LLC:**
Signature:________________________________	**Signature:**_Bruce Duner________________________
Name:___________________________________	**Name: Bruce Duner**_______________________
Title: ___________________________________	**Title:** __**Chief Financial Officer**_______________
Date Signed: ______________________________	**Date Signed:** _____________________________

SCHEDULE 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Schedule 1 includes certain details of the Processing of Company Personal Data as required by Data Protection Laws (including Article 28(3) GDPR or UK GDPR (as applicable) and the CCPA).

Subject matter and duration of the Processing of Company Personal Data

The subject matter and duration of the Processing of the Company Personal Data are set out in the Principal Agreement and this Addendum.

The nature and purpose of the Processing of Company Personal Data

The processing of Company Personal Data as requested by Company in order to utilize those critical communication services set out in the Principal Agreement.

The types of Company Personal Data to be Processed

Name, business contact details (work telephone number, cell phone number, e-mail address and office address and location), personal contact details (home telephone number, cell phone number, other telephone, e-mail address and physical address), geolocation, and employee ID.

The categories of Data Subject to whom the Company Personal Data relates

Categories of Data Subjects, as determined by the Company, may include company representatives and (end) users, such as employees, job applicants, contractors, collaborators, partners, suppliers and customers of the Company. Data Subjects also may include consumers and individuals attempting to communicate or transfer personal data to users of the services to be provided under the Principal Agreement

The obligations and rights of Company and Company Affiliates

The obligations and rights of Company and Company Affiliates are set out in the Principal Agreement and this Addendum.

Instructions for Processing Company Personal Data

The instructions for Processing Company Personal Data are set out in the Principal Agreement.

SCHEDULE 2: TECHNICAL AND ORGANIZATIONAL MEASURES

Described in OnSolve’s Security Standards, which shall be provided to Company upon written request. OnSolve’s Security Standards may be updated from time to time; however, with respect to the level of security protocols and resulting level of protection of data, OnSolve’s Security Standards shall not be materially degraded.

SCHEDULE 3: APPROVED SUB-PROCESSORS

OnSolve’s Sub-processor list is available at https://www.onsolve.com/company/security/subprocessors/

SCHEDULE 4: UK ADDENDUM TO THE EU MODEL CLAUSES

INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

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

Part 1 Tables

Table 1: Parties

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: [insert] Trading name (if different): [insert] Main address (if a company registered address): [insert] Official registration number (if any) (company number or similar identifier): [insert]	Full legal name: OnSolve, LLC Trading name (if different): [insert] Main address (if a company registered address): 6240 Avalon Boulevard, Alpharetta, GA 30009 Official registration number (if any) (company number or similar identifier): [insert]
Key Contact	Full Name (optional): [insert] Job Title: [insert] Contact details including email: [insert]	Full Name (optional): [insert] Job Title: VP, Information Security Contact details including email: [insert]
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: [insert] Reference (if any): [insert] Other identifier (if any): [insert] Or ☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
	2 (Controller to Processor)	Shall apply	Shall not apply	General authorisation	Twenty (20) business days	No

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: . . . .

Address: . . . .

Contact person's name, position and contact details: . . . .

Activities relevant to the data transferred under these clauses: . . . .

Signature and date: . . . .

Role (controller/processor): . . . .

[REPLICATE SECTION 1 ABOVE IF THERE ARE MULTIPLE EXPORTERS]

Data importer(s): [Identity and contact details of the Data Importer(s), including any contact person with responsibility for data protection]

Name: . OnSolve, LLC . . . .

Address: .. 6240 Avalon Boulevard, Alpharetta, GA 30009 . . . .

Contact person's name, position and contact details: . VP, Information Security . . .

Activities relevant to the data transferred under these clauses: . As set forth in the Principal Agreement

Signature and date: . . . .

Role (controller/processor): Processor . . . .

Annex 1B: Description of Transfer:

Categories of data subjects whose personal data is transferred

Categories of Data Subjects, as determined by the Data Exporter, may include company representatives and (end) users, such as employees, job applicants, contractors, collaborators, partners, suppliers and customers of the Company. Data Subjects also may include consumers and individuals attempting to communicate or transfer personal data to users of the services to be provided under the Principal Agreement.

Categories of personal data transferred

Categories of personal Data, as determined by the Data Exporter, may only include personal contact information such as name, home address, home telephone or mobile number, fax number, email address, employment details including employer name, job title and function.

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.

None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The transfer will occur on a continuous basis throughout the duration of the Agreement

Nature of the processing

The Company Personal Data transferred will be subject to the processing activities described in the Principal Agreement.

Purpose(s) of the data transfer and further processing

The objective of processing of personal data by Data Importer is the performance of the services pursuant to the Principal Agreement.

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

For the duration of the performance of the services pursuant to the Principal Agreement

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

The processing of personal data by sub-processors is for the performance of the Data Importer Services pursuant to the Principal Agreement and continues for the duration of the Services.

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

Described in OnSolve's Security Standards, which shall be provided to Company upon written request. OnSolve's Security Standards may be updated from time to time; however, with respect to the level of security protocols and resulting level of protection of data, OnSolve's Security Standards shall not be materially degraded

Annex III: List of Sub processors (Modules 2 and 3 only): [insert]

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in **paragraph 5.4**: ☐ Importer

	☐ Exporter ☐ neither Party

Part 2 Mandatory Clauses

1. **Entering into this Addendum**

1.1 Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

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

2. **Interpretation of this Addendum**

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

"Addendum" This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs

"Addendum EU SCCs" The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information

"Appendix Information" As set out in Table 3

"Appropriate Safeguards" The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under article 46(2)(d) UK GDPR

"Approved Addendum" The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under **paragraph 5.3**

"Approved EU SCCs" The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021

"ICO" The Information Commissioner

"Restricted Transfer" A transfer which is covered by Chapter V of the UK GDPR

"UK" The United Kingdom of Great Britain and Northern Ireland

"UK Data Protection Laws" All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018; and

"UK GDPR" As defined in section 3 of the Data Protection Act 2018.

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

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

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

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

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

3. **Hierarchy**

3.1 Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in **paragraph 3.2** will prevail.

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

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

4. **Incorporation of and changes to the EU SCCs**

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

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

4.1.2 **paragraphs 3.1** to **3.3** override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

4.1.3 this Addendum (including the Addendum EU SCCs incorporated into it) is:

4.1.3.1 governed by the laws of England and Wales; and

4.1.3.2 any dispute arising from it is resolved by the courts of England and Wales

in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

4.2 Unless the Parties have agreed alternative amendments which meet the requirements of **paragraph 4.1**, the provisions of **paragraph 4.4** will apply.

4.3 No amendments to the Approved EU SCCs other than to meet the requirements of **paragraph 4.1** may be made.

4.4 The following amendments to the Addendum EU SCCs (for the purpose of **paragraph 4.1**) are made:

4.4.1 References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

4.4.2 In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

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

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

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

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

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

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

4.4.6 References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent article or section of UK Data Protection Laws;

4.4.7 References to Regulation (EU) 2018/1725 are removed;

4.4.8 References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

4.4.9 The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

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

4.4.11 The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

4.4.12 In Clause 16(e), subsection (i) is replaced with:

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

4.4.13 Clause 17 is replaced with:

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

4.4.14 Clause 18 is replaced with:

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

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

5. **Amendments to this Addendum**

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

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

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

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

5.3.2 reflects changes to UK Data Protection Laws;

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

5.4 If the ICO issues a revised Approved Addendum under **paragraph 5.3**, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

5.4.1 its direct costs of performing its obligations under the Addendum; and/or

5.4.2 its risk under the Addendum,

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

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

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under **paragraph 5.3** of those Mandatory Clauses.

SCHEDULE 5: STANDARD CONTRACTUAL CLAUSES (where GDPR applies)

SECTION 1

1. PURPOSE AND SCOPE

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

1.2 The Parties:

1.2.1 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 1.A** (hereinafter each ‘Data Exporter’); and

1.2.2 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 1.A** (hereinafter each ‘Data Importer’)

have agreed to these standard contractual clauses (hereinafter: ‘clauses’).

1.3 These clauses apply with respect to the transfer of personal data as specified in **Annex 1.B**.

1.4 The Appendix to these clauses containing the Annexes referred to therein forms an integral part of these clauses.

2. EFFECT AND INVARIABILITY OF THE CLAUSES

2.1 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.

2.2 These clauses are without prejudice to obligations to which the Data Exporter is subject by virtue of Regulation (EU) 2016/679.

3. THIRD-PARTY BENEFICIARIES

3.1 Data subjects may invoke and enforce these clauses, as third-party beneficiaries, against the Data Exporter and/or Data Importer, with the following exceptions:

3.1.1 **clause 1**, **clause 2**, **clause 3**, **clause 6**, **clause 7**;

3.1.2 **clause 8.1.2**, **8.9.1**, **8.9.3**, **8.9.4** and **8.9.5**;

3.1.3 **clause 9.1**, **9.3**, **9.4** and **9.5**;

3.1.4 **clause 12.1**, **12.4** and **12.5**;

3.1.5 **clause 13**;

3.1.6 **clause 15.1.3**, **15.1.4** and **15.1.5**;

3.1.7 **clause 16.5**;

3.1.8 **clause 18.1** and **18.2**.

3.2 **Clause 3.1** is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

4. INTERPRETATION

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

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

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

5. HIERARCHY

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

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 1.B**.

7. DOCKING CLAUSE

7.1 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 1.A**.

7.2 Once it has completed the Appendix and signed **Annex 1.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 1.A**.

7.3 The acceding entity shall have no rights or obligations arising under these clauses from the period prior to becoming a Party.

SECTION 2 OBLIGATIONS OF THE PARTIES

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

8.1.1 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.

8.1.2 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 1.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 2** 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 1.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 14.5** 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** 14.1.

8.6 **Security of processing**

8.6.1 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 2**. The Data Importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

8.6.2 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.

8.6.3 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.

8.6.4 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 1.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[1] (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:

8.8.1 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;

8.8.2 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;

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

8.8.4 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**

8.9.1 The Data Importer shall promptly and adequately deal with enquiries from the Data Exporter that relate to the processing under these clauses.

8.9.2 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.

8.9.3 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.

8.9.4 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.

8.9.5 The Parties shall make the information referred to in **paragraphs 8.9.2** and **8.9.3**, including the results of any audits, available to the competent supervisory authority on request.

[1] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these clauses.

9. **USE OF SUB-PROCESSORS**

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 twenty (20) business 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.

9.1 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[2]. 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.

9.2 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.

9.3 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.

9.4 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.

10. **DATA SUBJECT RIGHTS**

10.1 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.

10.2 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 2** 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.

10.3 In fulfilling its obligations under **clauses 10.1** and **10.2**, the Data Importer shall comply with the instructions from the Data Exporter.

11. **REDRESS**

11.1 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.

11.2 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.

11.3 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:

[2] This requirement may be satisfied by the sub-processor acceding to these clauses under the appropriate Module, in accordance with Clause 7

11.3.1 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**;

11.3.2 refer the dispute to the competent courts within the meaning of **clause 18**.

11.4 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.

11.5 The Data Importer shall abide by a decision that is binding under the applicable EU or Member State law.

11.6 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.

12. LIABILITY

12.1 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.

12.2 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.

12.3 Notwithstanding **paragraph 12.2**, 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.

12.4 The Parties agree that if the Data Exporter is held liable under **paragraph 12.3 f**or 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.

12.5 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.

12.6 The Parties agree that if one Party is held liable under **paragraph 12.5**, 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.

12.7 The Data Importer may not invoke the conduct of a sub-processor to avoid its own liability.

13. SUPERVISION

13.1 [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 1.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 1.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 1.C**, shall act as competent supervisory authority.

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

SECTION 3 LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

14. LOCAL LAWS AND PRACTICES AFFECTING COMPLIANCE WITH THE CLAUSES

14.1 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.

14.2 The Parties declare that in providing the warranty in **paragraph 14.1**, they have taken due account in particular of the following elements:

14.2.1 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;

14.2.2 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[3];

14.2.3 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.

14.3 The Data Importer warrants that, in carrying out the assessment under **paragraph 14.2**, 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.

14.4 The Parties agree to document the assessment under **paragraph 14.2** and make it available to the competent supervisory authority on request.

14.5 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 14.1**, 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 14.1**.

14.6 Following a notification pursuant to **paragraph 14.5**, or if the Data Exporter otherwise has reason to believe that the Data Importer can no longer fulfil its obligations under these clauses, the Data Exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure

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

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 16.1.4** and **16.1.5** shall apply.

15. OBLIGATIONS OF THE DATA IMPORTER IN CASE OF ACCESS BY PUBLIC AUTHORITIES

15.1 Notification

15.1.1 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:

15.1.1.1 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

15.1.1.2 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.

15.1.2 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.

15.1.3 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.).

15.1.4 The Data Importer agrees to preserve the information pursuant to **clauses 15.1.1** to **15.1.3** for the duration of the contract and make it available to the competent supervisory authority on request.

15.1.5 **Clauses 15.1.1** to **15.1.3** are without prejudice to the obligation of the Data Importer pursuant to **clause 14.5** 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

15.2.1 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 14.5**.

15.2.2 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.

15.2.3 The Data Importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION 4 FINAL PROVISIONS

16. NON-COMPLIANCE WITH THE CLAUSES AND TERMINATION

16.1 The Data Importer shall promptly inform the Data Exporter if it is unable to comply with these clauses, for whatever reason.

16.2 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 14.6**.

16.3 The Data Exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these clauses, where:

16.3.1 the Data Exporter has suspended the transfer of personal data to the Data Importer pursuant to **paragraph 16.2** and compliance with these clauses is not restored within a reasonable time and in any event within one month of suspension;

16.3.2 the Data Importer is in substantial or persistent breach of these clauses; or

16.3.3 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.

16.4 Personal data that has been transferred prior to the termination of the contract pursuant to **paragraph 16.3** 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.

16.5 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.

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 Ireland.

18. CHOICE OF FORUM AND JURISDICTION

18.1 Any dispute arising from these clauses shall be resolved by the courts of an EU Member State.

18.2 The Parties agree that those shall be the courts of Ireland.

18.3 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.

18.4 The Parties agree to submit themselves to the jurisdiction of such courts.

Annex 1

A. LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Name: . . . .

   Address: . . . .

   Contact person's name, position and contact details: . . . .

   Activities relevant to the data transferred under these clauses: . . . .

   Signature and date: . . . .

   Role (controller/processor): . . . .

2. [REPLICATE SECTION 1 ABOVE IF THERE ARE MULTIPLE EXPORTERS]

Data importer(s): [Identity and contact details of the Data Importer(s), including any contact person with responsibility for data protection]

1. Name: . OnSolve, LLC . . . .

   Address: .. 6240 Avalon Boulevard, Alpharetta, GA 30009 . . . .

   Contact person's name, position and contact details: . VP, Information Security . . .

   Activities relevant to the data transferred under these clauses: . As set forth in the Principal Agreement

   Signature and date: . . . .

   Role (controller/processor): Processor . . . .

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Categories of Data Subjects, as determined by the Data Exporter, may include company representatives and (end) users, such as employees, job applicants, contractors, collaborators, partners, suppliers and customers of the Company. Data Subjects also may include consumers and individuals attempting to communicate or transfer personal data to users of the services to be provided under the Principal Agreement.

Categories of personal data transferred

Categories of personal Data, as determined by the Data Exporter, may only include personal contact information such as name, home address, home telephone or mobile number, fax number, email address, employment details including employer name, job title and function.

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.

None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The transfer will occur on a continuous basis throughout the duration of the Agreement

Nature of the processing

The Company Personal Data transferred will be subject to the processing activities described in the Principal Agreement.

Purpose(s) of the data transfer and further processing

The objective of processing of personal data by Data Importer is the performance of the services pursuant to the Principal Agreement.

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

For the duration of the performance of the services pursuant to the Principal Agreement

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

The processing of personal data by sub-processors is for the performance of the Data Importer Services pursuant to the Principal Agreement and continues for the duration of the Services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with **clause** 13

Data Protection Commission, Irish supervisory authority

Annex 2

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

Described in OnSolve’s Security Standards, which shall be provided to Company upon written request. OnSolve’s Security Standards may be updated from time to time; however, with respect to the level of security protocols and resulting level of protection of data, OnSolve’s Security Standards shall not be materially degraded.