Introduction

These terms and conditions (together with any documents incorporated by reference below, the “Agreement”) govern the supply of services by Paystratus Group Limited, (as the context requires, “Weavr”, “we”, “us”, “our”) to the entity approved by us to access the Weavr.io Platform (“you”, “your”) as indicated below.

Contact information: our contact details are available at https://weavr.io/contact.

We operate and maintain the Weavr.io Platform which enables you to access the Payment Services provided by regulated financial institutions (“the Payment Services Providers”), and to securely exchange your personal and financial data with the Payment Services Providers in relation to the provision of these services.

Our services to you are referred to as “the Weavr Services” throughout this Agreement. Your access to the Weavr Services is facilitated by the Application Provider by means of the Solution.

We provide the Weavr Services without charge to you but subject always to the terms and conditions of this Agreement.

The Payment Services are provided by authorised and regulated entities the details of which are provided on our website.

In certain circumstances you will also be bound by the terms and conditions of the Payment Services Provider(s) (which we identify on our website) and we and they shall be entitled to treat your use of the Weavr Services as confirmation of your acceptance of this Agreement and the terms and conditions applicable to the Payment Services.

Data

For the purposes of these clauses relating to data the following terms shall have the following meanings:

Data Protection Legislation: the UK Data Protection Legislation and (for so long as and to the extent that the law of the European Union has legal effect in the UK) the General Data Protection Regulation ((EU) 2016/679) and any other directly applicable European Union regulation relating to privacy.

Our Data: the data, not including any personal data, supplied by us or our licensor for the Business Purpose (as defined below).

Processed Data: any data that derives from us having Processed Your Data under this agreement, whether or not in combination with Our Data.

Processed Non Personal Data : all data, other than personal data, comprised in the Processed Data from time to time.

Relevant Data: Your Data and the Processed Data.

Security Breach: any security breach relating to:

(a) Your Personal Data reasonably determined by us to be sufficiently serious or substantial to justify notification to the Information Commissioner or other relevant supervisory authority in accordance with the Privacy and Data Protection Requirements; or

(b) Your Non-Personal Data reasonably determined by us to be sufficiently serious or substantial to give rise to a material risk of litigation by the individuals whose data is the subject of the breach.

Security Feature: any security feature, including any key, PIN, password, token or smartcard.

Standard Contractual Clauses: the standard contractual clauses for the transfer of personal data from the European Union to processors established in third countries as set out in the Annex to Commission Decision 2010/87/EU.

UK Data Protection Legislation: any data protection legislation from time to time in force in the UK including the Data Protection Act 1998 or 2018 or any successor legislation.

Your Data: the data supplied by you to us under the terms of this Agreement, including Your Personal Data and Your Non-Personal Data.

Your Non-Personal Data: all data comprised in Your Data from time to time other than Your Personal Data.

Your Personal Data: the personal data comprised in Your Data from time to time.

Collection, Storage and Use of Your Data

In order that you can use the Solution it is necessary that we collect information from you including information regarding your identity and (where you are a corporate body) the identities of your officers and employees.

Some of the information collected is Personal Data (as defined in the Data Protection Legislation).

Your Data is collected for the following purposes (“**Business Purpose**”):

to meet the anti-money laundering and similar obligations placed on us, the Application Provider or the Payment Services Provider(s);

to enable us to provide the Weavr Services;

to enable us to provide the necessary services to the Application Provider;

to share Your Data with the Payment Services Provider(s) and/or Application Provider so that they can meet any requirements they have in providing the relevant services.

We shall process Your Data for the Business Purpose only and in compliance with Your instructions from time to time.

You acknowledge that we are under no duty to investigate the completeness, accuracy or sufficiency of Your Data.

We may use Processed Non Personal Data to derive usage trends of the use of the Weavr Platform and for other commercial purposes. Any personal data shall always be made anonymous for such purposes.

Data retention

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

Security and Passwords

We shall ensure that the Relevant Data is kept secure and in an encrypted form, and shall use all reasonable security practices and systems applicable to the use of the Relevant Data to prevent, and take prompt and proper remedial action against, unauthorised access, copying, modification, storage, reproduction, display or distribution of the Relevant Data.

Where we use Security Features in relation to the Weavr Services (wholly or in part), the Security Features must be kept confidential and not lent, shared, transferred or otherwise misused by you.

If you or we:

(i) becomes aware of any unauthorised or unlawful processing of any Relevant Data or that any Relevant Data is lost or destroyed or has become damaged, corrupted or unusable;

(ii) becomes aware of any Security Breach; or

(iii) learns or suspects that any Security Feature has been revealed to or obtained by any unauthorised person,

that party shall, at its own expense, promptly notify the other party and fully co-operate with the other party to remedy the issue as soon as reasonably practicable.

We may change Security Features on notice to you for security reasons.

We shall take reasonable precautions to preserve the integrity of any Relevant Data processed by us and to prevent any corruption or loss of such Relevant Data.

We shall regularly make a back-up copy of the Relevant Data and record the copy on media from which the Relevant Data can be reloaded in the event of any corruption or loss of the Relevant Data.

If any of Your Data is lost or corrupted, our obligations under this clause shall be your exclusive right and remedy against us in respect of such loss or corruption.

Our Obligations

We shall:

(i) only make copies of Your Data to the extent reasonably necessary for the Business Purpose (which includes, for clarity, back-up, mirroring (and similar availability enhancement techniques), security, disaster recovery and testing of the Customer Data);

(ii) not extract, re-utilise, use, exploit, redistribute, re-disseminate, copy or store Your Data other than for the Business Purpose; and

(iii) not do anything that may materially damage your reputation.

We shall take reasonable steps to ensure the reliability of all our employees who have access to Your Personal Data.

Where we need to transfer any of Your Personal Data outside the EEA we shall do so only in accordance with the terms of the Standard Contractual Clauses.

Your Obligations

In your use of the Weavr Service you shall not:

access, store, distribute or transmit any viruses, or any material that:

(i) is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;

(ii) facilitates illegal activity;

(iii) depicts sexually explicit images;

(iv) promotes unlawful violence;

(v) is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or

(vi) is in any manner otherwise illegal or causes damage or injury to any person or property; and

shall not use or change your use of the Weavr Service in such a way as may (or may reasonably be expected to) overload or otherwise compromise the Weavr Platform or use it in any way which may reasonably be expected to be outside the parameters of normal use (for example by making excessive API calls through the system) and shall indemnify us against any costs we incur as a result of any such misuse;

and we reserve the right, without liability or prejudice to our other rights, to disable your access to the Weavr Services should you breach the provisions of this clause.

You shall not:

- attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Weavr Platform in any form or media or by any means; or
- attempt to reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Weavr Platform; or
- access all or any part of the Weavr Platform in order to build a product or service which competes with the Weavr Platform; or
- attempt to obtain, or assist third parties in obtaining, access to the Weavr Platform.

You shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Weavr Platform and, in the event of any such unauthorised access or use, promptly notify us.

In order for you to be able to use the Solution, the Weavr Services and Payment Services you may need your employees, officers, operatives and agents to access the Weavr Platform. Where we grant such access these individuals will be deemed to be authorised for the purposes of this Agreement and your agreements with the Application Provider and Payment Services Provider(s) and will be “Authorised Users”. You undertake that your Authorised Users shall only access the Weavr Platform for these purposes and shall keep secure any password or other security device provided for such access. You shall be liable for the acts and omissions of your Authorised Users as if they were your own and we may bloke their access at any time if we believe that any of the terms of this Agreement or the Payment Services Agreement(s) has been or may be breached.

Our Rights

We may suspend or terminate your access to the Weavr Platform at any time and for any reason, including but not limited to:

- you failing to use the Weavr Platform for the stated purpose;
- you failing to comply with any of these terms or any reasonable instruction we may issue;
- you withholding information which can reasonable be considered to be relevant in our granting you access to the Weavr Platform;
- your usage generating system loads that result in material negative impact on the performance of the Weavr Platform.

Your Rights

You have the right to:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we or our partners (if relevant) hold about you and to check that we are lawfully processing it. Where your personal data is held by any of our partners in relation to your use of the Weavr Services, the Payment Services or otherwise, we shall act as that partner’s agent in responding to your data subject access request.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as

you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

If you want us to establish the data's accuracy.

Where our use of the data is unlawful but you do not want us to erase it.

Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims.

You have objected to our use of Your Data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

Contact details

If you have any questions about this our use of your personal data please contact us in the following ways:

Email address: privacy@weavr.io

Postal address: Paystratus Group Ltd, Kemp House 160 City Road, London EC1V 2NX UK

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

No Warranty

Access to the Weavr Services is provided “as is” and we give no warranty that the access will be continuous and uninterrupted. We use our reasonable commercial endeavours to provide the Weavr Services 24/7 but shall not be liable to you or any third party if we are unable to achieve this.

We shall not be liable to you in relation to any loss you suffer from your use of the Weavr Services, the Payment Services or the Solution including but not limited to any loss of profits, loss of sales or business, loss of agreements or contracts, loss of anticipated savings, loss of use or corruption of software, data or information, loss of or damage to goodwill or indirect or consequential loss.

Intellectual Property Rights

You and we acknowledge that:

(i) all Intellectual Property Rights in Your Non-Personal Data are and will remain your property or the property of your licensors, as the case may be; and

(ii) all Intellectual Property Rights in Our Data are and will remain our property or the property of our licensors, as the case may be;

(iii) we shall have no rights in or to Your Non-Personal Data other than the right to use it for the Business Purpose in accordance with this agreement; and

(iv) you shall have no rights in or to Our Data other than a non-exclusive, royalty-free, personal, non-assignable, non-sub-licensable licence (co-terminous with this agreement) to process Processed Data for the Business Purpose in accordance with this Agreement.

You assign to us, and shall assign to us, all your Intellectual Property Rights in any Processed Non-Personal Data we may create under this Agreement, by way of future assignment.