SUPPLIER SERVICE DESCRIPTION

Contents:

This set of terms covers the following services:

Service Descriptions

Open Banking – Payment Initiation Service (PIS)

The Supplier will provide facilities to enable a Customer, upon visiting the Buyer's webpage, to choose an "Open Banking" payment option or to scan a QR Code. Once the option is selected or the QR Code scanned, the Customer is routed to an open banking payment initiator (provided by a PISP, such term is defined in the Supplier Specific Terms which enables such Customer to select a bank account to make the payment.

Where the Buyer has agreed to use the Open Banking (PIS) Aggregator service, the Supplier Group is authorised by the Buyer to receive such payments from the Customers in respect of payments due to the Buyer and initiated by the Customer when the Customer uses the Open Banking Service, aggregates them and then onward settle such payments to the Buyer.

Account Information Service (Basic)

This service enables the Customer of a Buyer, via a link or QR Code sent to them, that enables such Customer to access their bank or payment accounts using an AIS enquiry. It therefore gives the Buyer's Customer control over their financial circumstances by managing their payment options.

Variable Recurring Payments (VRP)

Variable recurring payments is a service offered via Open Banking to enable a Customer of the Buyer to instruct their bank or account service provider ("the Bank") to set up a payment to the Client. The payment is made using payment initiation services (PISP)

Account Information Service (Enhanced)

A service to enable a Buyer to access financial information relating to the financial standing of individuals and/or organisations either via the Supplier's Portal, or the Aperidata Portal.

SUPPLIER SERVICE SPECIFIC TERMS

PART ONE : Open Banking – Payment Initiation Service (PIS)

1. Definitions

AIS	Account Information Service
AISP	Account Information Service Provider
Buyer OB Service	The Transaction whereby the Customer uses a QR Code or the the Supplier's Payment App to access the PISP's service for the purpose of making a payment to the Buyer.
Customer's Payment Account Service Provider	The bank or payment institution holding the account to be used by the Customer to make the payment to the Buyer.
Financial Data	the Buyer's bank account and sort code to be used to receive the payment initiated by the Customer from the Customers bank account using Open Banking Initiative standards.
Payment Initiation	The instruction given by the Customer to generation of the Payment Order.
Payment Initiation Request	The request sent by the Customer via the open banking infrastructure to initiate the payment to the Buyer.
Payment Order	The payment made by the Customer to the Buyer.
PayPoint Payment Channel	Means the QR Code and/or such other method as may be agreed in writing with the Buyer from time to time.
PISP	Payment Initiation Service Provider
PIS Aggregator Service	A service where the Buyer has authorised the Supplier's subcontractor and Group Company, PayPoint Collections Limited to receive payments from Customers in respect of payments due to the Buyer and initiated by the Customer when the Customer uses the Open Banking Service;
OB Product Overview	The description of the "Buyer Journey" when using the service.
Open Banking Initiative	The organisation being the Open Banking Implementation Entity (OBIE) creating the software standards and industry guidelines required to offer open banking services.
OBF	The functionality included in the PayPoint Payment Channel to provide a service to enable a Customer to access Open Banking to initiate a payment to the Buyer for either goods and/or services provided by the Buyer, or for the purposes of donating money.
QR Code	Means the code to be scanned by a Customer to access the PISP to initiate a Payment Initiation Request.
TPP	Third Party Provider being an organisation approved by the Open Banking Initiative to support open banking services.

2. Open Banking

2.1. The Supplier will provide the Buyer with:

2.1.1.If relevant, the QR Code to be displayed visually by the Buyer;

2.1.2. the OBF.

2.2. The OBF enables a Buyer to provide Financial Data to a Customer for the Customer to use to populate the payment initiation instruction provided by the Customer's TPP to the PISP to initiate a payment to the Buyer.

2.3. This Buyer OB Service is only available to a Buyer that is using the PayPoint Payment Channel as specified in OB Product Overview.

2.4. The Buyer will ensure that the Financial Data;

a) Provided to the Supplier is accurate and up to date;

b) Relates wholly and exclusively to payment accounts in the name of the Buyer;

c) The amount of the Payment Initiation:

(i) requested by the Buyer from the Customer, for funds owed to and/or due to the Buyer for goods and/or services and/or a payment arising from a legally binding contract;

(ii) that the Customer has agreed to make to the Buyer, being the value of the donation.

d) Provide the Supplier with the Financial Data as specified in the Order Form to be disclosed to the TPP;

e) Comply to the extent applicable with the Open Banking Customer Experience Guidelines as published at https://www.openbanking.org.uk/

f) Once Payment Initiation Request has been submitted by the Customer, the Buyer will confirm the successful initiation of a Payment Order.

g) No further payments will be initiated by PISP unless the Customer repeat the steps to make a payment for a further purchase unless in accordance with Open Banking Customer Experience Guidelines.

2.5. If specified in the Order Form, the Buyer will complete the integration to the Supplier in respect of the OBF and the Buyer will maintain the integration for the period of this Agreement.

2.6. The Supplier will provide the Buyer with;

a) Functionality in the PayPoint Payment Channel to provide the Open Banking capability as specified in the OB Product Description;

b) Hold the Financial Data as specified in the Order Form;

c) Report to the Buyer if the Buyer OB Service is not performing within the specification as specified in OB Product Description.

d) Report of the completion of a Payment Initiation Request by the Customer to the Buyer as a direct consequence of the submission of the Financial Data by the Buyer to the Customer via the OBF.

e) Comply to the extent applicable with the Open Banking Customer Experience Guidelines as published at https://www.openbanking.org.uk/.

2.7. The Supplier is not responsible for the actions of the Customer's Payment Account Service Provider.

2.8. The Buyer acknowledges that the Supplier is not the TPP for the purposes of Open Banking and is not responsible for and/or liable for the actions or omissions of the TPP and/or the Customer in relation to initiating the payment to the Buyer.

2.9. To make the payment, the Customer will use a regulated PISP to make the payment directly to the Buyer. The Supplier is not responsible for the Customer making the payment to the Buyer or the actions of the regulated PISP. The PISP acts on behalf of the Customer and upon the instruction of the Customer.

2.10. The Charges payable for the OBF are as specified in the G-Cloud 15 Call Off Contract.

2.11. The provision of the OB Service is subject to the terms and conditions imposed by the Open Banking Initiative and may be varied or amended at any time as required for compliance with the relevant rules and/or guidance as issued.

3. Open Banking (PIS) Aggregator Service

3.1. Buyer Authorisations and Confirmation

In order to use the PIS Aggregator Service, the Buyer agrees the following:

3.1.1. The Supplier is authorised by the Buyer to instruct the Customer when using the Open Banking Service to make payment of funds due to the Buyer to an account held by the Supplier in the name of the Buyer.

3.1.2. The receipt of payment by the Supplier from the Customer, settles the Customer's debt to the Buyer to the value of the payment received.

3.1.3. Other than payments incurred by PPCL for transfers by the Settlement Bank (pursuant to clause 3.4.6 below), there will be no charge for the PIS Aggregator Service.

3.2. Obligations of the Supplier

3.2.1. The Supplier shall provide the Buyer's Customer with details of the the Supplier account used to receive the payments from the Buyer's Customer as part of the Customer's use of the Open Banking Service, such payments shall hereinafter be referred to as "**Open Banking PIS Transactions"**.

3.2.2. The Supplier shall report to the Buyer the value of the funds received from the Open Banking PIS Transactions.

3.2.3. The Supplier shall hold the funds received from the Open Banking PIS Transactions in accounts identified as Buyer funds.

3.2.4. The Supplier shall make payment to the Buyer of such funds in accordance with the Banking Arrangements detailed in clause 3.4 below.

3.3. Data Protection

3.3.1. The Buyer acknowledges that in order to receive the payment from the Customer, the Supplier will process the Customer's personal data. Such processing by the Supplier shall be on the basis that the Supplier is acting as the Controller.

3.3.2. The Supplier and the Buyer agrees that the subsequent reporting to the Buyer of the payments received from the Customer and sharing of such data, shall be on the basis of data sharing and the provisions of Part 1 of the Data Protection Addendum shall apply.

3.4. Banking Arrangements

3.4.1. The Supplier shall, via its subcontractor and group company, PayPoint Collections Limited (PPCL):

a) provide financial operations management to effect reconciliation, investigate claims and answer queries from the Buyer in relation to the operation of Banking Arrangements and the transfer of funds relating to the Open Banking PIS Transactions to the Buyer's Designated Account ("**Settlement**"); and

b) effect Settlement.

3.4.2. PPCL and the Buyer have agreed that all payments collected with respect to Open Banking PIS Transactions shall be paid to the Buyer in accordance with the terms contained in this clause.

3.4.3. The Buyer confirms and accepts that the funds from the Open Banking PIS Transactions will be credited to accounts maintained by the Settlement Bank (the "**Collections Accounts**"), prior

to transfer to the destination account designated by the Buyer (the "**Designated Account**") in accordance with paragraph 3.4.7 of this clause.

3.4.4. PPCL undertakes and agrees that at no time will PPCL have any beneficial interest in monies in the Collections Accounts, and such monies will be held on trust by PPCL at all times for the Buyer, according to the Buyer's respective entitlements which shall be determined by reference to the amounts paid by the Customers for their respective accounts as notified to PPCL by PPNL. The perpetuity period applicable to the trusts established in relation to the Collections Accounts shall be 80 years from the date hereof.

3.4.5. PPCL, via the Supplier, shall be entitled to recover from the Buyer:

a) the cost of fees charged by the Settlement Bank in respect of transfers from the Collections Account to the Designated Account; and
b) any sums credited in error to the Designated Account by PPCL.

3.4.6. The transfer of the Open Banking PIS Transactions to the Buyer shall take place within three (3) Banking Days of the Transaction date.

3.4.7. The Buyer undertakes:

a) to provide to PPCL details of its Designated Account, together with specimen signatures of all required authorised signatories for the purpose of verifying such details; and
b) to repay, forthwith on demand by PPCL all sums credited in error to the Designated Account (to the extent these are not already set off by PPCL pursuant to paragraph 6 of this clause, above). Such repayments shall be made by the Buyer to a Collections Account notified to the Buyer.

For the purposes of this clause, the **"Settlement Bank"** means Barclays Bank plc or such other clearing bank in the United Kingdom as PPCL may substitute from time to time;

4. <u>Buyer's Obligations [FOR QR CODE USE ONLY]</u>

4.1. The Buyer shall:

a. Facilitate the QR Code being displayed and distributed.

b. Ensure the QR Codes are displayed at a location that has internet access and sufficient broadband capacity to enable a Customer to donate.

c. Maintain the quality of the QR Code to ensure that it remains undamaged, readable and can be effectively scanned to enable a Transaction to be initiated. PPNL accepts no liability and shall not be in breach of this Agreement where the quality of the QR Code is reduced due to non-compliance with this clause and a Payment Initiation Request cannot be made.

d. The Buyer shall be responsible for ensuring that the QR Codes displayed are securely preserved to ensure that they cannot be tampered with, altered or fraudulently replaced. The Buyer shall indemnify PPNL against any third party claims made against it as a result of a Transaction which has been made through a fraudulent QR Code.

e. Encourage Customers to use an approved secure QR scanner.

f. Report any issues in relation to the performance of the QR Code to PayPoint in a prompt and timely manner.

Open Banking Schedule Order Form

1. Integration Requirement
    - Website Integration by Buyer to PPNL.

2. Buyer's Financial Data
   The account details provided by the Buyer for receipt of the payment from the Customer.
    - Account Name (in full):
    - Account Number:
    - Account Sort Code:
    - Buyer ID (if applicable):

3. OB Product Overview

Open Banking Payments

1. The Open Banking Service allows a Buyer's Customer to make a payment direct from the Customer's own bank account to the Buyer's bank account using a credit transfer.
2. The service creates an automated process for the Customer to initiate the payment via Open Banking. This process is available by PayPoint's web and app payment channels. It allows the Customer to make a secure and fast payment as the Customer (the account holder) gives consent to the payment request.
3. To make a one-off Open Banking payment the Customer will need to add a service/product number which is then validated against the Buyer's own predefined validation rules.
4. The Customer will choose/add the payment amount and select they wish to Pay by Bank.
5. The Customer is presented a list of banks where they will need to select the bank holding the account they wish to debit.
6. The Customer provides consent to access their bank account and is required to authenticate themselves with their bank.
7. Once authenticated the Customer can authorise the Bank Transfer and funds will be transferred from the Customer's bank account to the Buyer's bank account.
8. When the payment is initiated, the payment response page is displayed to the Customer, detailing the confirmation of the Customer's payment consent and a valid Vend Code (UTRN), if applicable.
9. If the Customer provided an email address, the Customer will also receive an email transaction receipt.
10. The Buyer will receive notification that the payment has been initiated via the PayPoint service in the transaction reports.

PART TWO : Account Information Service (Basic)

1. Overview

The AIS (Basic) Service is where the Customer is sent a link or QR Code that enables the Customer to access their bank or payment accounts using an AIS enquiry. The AIS enquiry is supported by an AISP.

The purpose of the AIS (Basic) Service is to give the Buyer's Customer control over their financial circumstances by managing their payment options.

By providing this service to the Customer, the Buyer is able reduce the risk of a payments being made into a closed account or attempting to obtain payments from an account with insufficient funds.

2. Service Description

2.1 The Customer uses the AIS request to identify which bank or payment account the Customer wants the Buyer to use to make or receive a payment.

2.2 The Customer authorises the AISP to shares the details of the bank or payment account selected with the Supplier for release to the Buyer to enable the Buyer to either:

- 2.2.1 Make a payment to the Customer by using a credit transfer; or
- 2.2.2 Receive a payment from the Customer such as a request for a direct debit.

2.3 Save to the extent no Payment Initiation is activated by the Customer, the operation of the AIS (Basic) Service is in accordance with the Open Banking Services Schedule in that:

- 2.3.1 The Customer is sent a link or QR Code.
- 2.3.2 The Customer connects to the AISP and makes an AIS request.

2.4 The Customer can verify which account to use to make to or receive the payment from the Buyer.

2.5 The Customer consents to the AISP sharing details of the account selected with the Buyer.

2.6 The AIS (Basic) Service uses the OBF.

2.7 Once completed, the Customer does not initiate a payment. The Buyer can then either initiate a payment to the Customer or initiate a direct debit to the Customer's bank or payment account providing the Buyer holds the appropriate direct debit mandate.

PART THREE : Variable Recurring Payments (VRP)

These terms and conditions together with the VRP Order Form are supplemental to the Agreement as hereinafter defined.

It is now agreed.

1. Overview

1.1. Variable recurring payments is a service offered via Open Banking to enable a Customer of the Buyer to instruct their bank or account service provider ("the Bank") to set up a payment to the Buyer. The payment is made using payment initiation services (PISP)

1.2. Such payment is made within set parameters agreed by the Customer as to the value and the frequency and the Customer's Consent that is set out in the VRP Instruction.

1.3. The VRP Service is for either:

a) A Commercial, non sweeping, Variable Recurring Payment (cVRP) being a payment originating from a VRP Instruction from the Customer account to the Buyer's Destination Account.

b) A Sweeping VRP payment being a payment originating from the VRP Instruction from the Customer's Account to another account held in the same Customer Name.

1.4. The VRP Service is permitted when:

a) The source account is a personal current account (PCA) or business current account (BCA).

b) The Destination Account is any account into which a domestic payment can be made by the payer's bank's direct channel.

c) Both accounts are UK sterling accounts.

d) The payments can be an unattended payment, not requiring any interaction by or presence of the payment service user at the time of making the payment.

1.5. The VRP Service is only available in the United Kingdom, for payments made from a UK Bank account and for payments in Sterling.

1.6. The Supplier is acting as a technical service provider in relation to the VRP Service.

1.7. Any payment services such as payment initiation provided to the Customer and/or the Buyer are provided by a PISP authorised by the FCA.

2. Definitions

2.1. Save to the extent expressly varied herein, the definitions in the Agreement shall apply. The following definitions are added in relation to the VRP Service.

Agreement	The G-Cloud 15 Call Off Contract between the Supplier and the Buyer for technology and payment related services.
Account	The payment account held by a Bank for the Customer and used to make payments associated with the VRP consent provide by the Customer.
API	Application Programme Interface
Bank	Account Service Provider, being a credit institution or other such regulated entity holding the Customer's Account.

Banking Infrastructure	Open Banking or such other national systems or scheme used to support the VRP Service.
CDD Checks	Customer Due Diligence checks.
Buyer	The Buyer as specified on the Order Form.
Client Account	The account held by the Buyer on behalf of the Customer that receives the payment from the Customer's Account.
Consent (VRP Instruction)	The permission from the Customer for the Buyer to request the VRP is paid into the Destination Account as set out in the VRP Instruction.
Customer	The Customer of the Buyer.
Customer Dispute	A complaint or issue raised by the Customer in relation to the payment and/or VRP Mandate.
Destination Account	The account held by the Customer or the Buyer receiving the payment.
FCA	Financial Conduct Authority
Instruction Consent Management Interface	The facility to enable a Customer to provide Consent for the VRP.
OBP	The entity accredited and authorised to submit the VRP Request in the Banking Infrastructure on behalf of the Buyer.
PCA	Personal Current Account
PISP	Payment Initiation Service Provider
Open Banking	The entity providing operational rules and/or standards to be applied to a transaction submitted using the Open Banking infrastructure.
Relevant Standards	The standards applied to the VRP Service by Open Banking, together with any applicable laws.
TPP	Third Party Provider
VRP	Variable Recurring Payment
Commercial VRP (cVRP)	The use of the commercial VRP Service for the Customer to make a non-sweeping payment to a third party.
VRP Instruction	The instruction from the Customer to make the transfer of funds from their Account to the Destination Account
VRP Order Form	The document setting out the commencement date for the service, together with any charges and any special conditions applicable to the VRP Service.
VRP Request	The request from the Buyer for the PISP to initiate the payment from the Customer's Account to the Destination Account.
VRP Service	Variable Recurring Payment service supporting the provision of payments to a Buyer
VRP Sweeping	The automated transfer of funds from the Customer's account to another account held in the same Customer's name.

3. Service Description - Commercial VRP (cVRP) non-sweeping

3.1. ***Consent and Set Up Request***

The Buyer will provide the Customer with the ability for the Customer to give their consent to the PISP for the VRP Instruction to be set up on the Customer's Account. The VRP Instruction shall include:

a) as a minimum, details of the Client's Destination Account,

b) the maximum amount of each payment
c) the maximum amount of each payment per specified interval, and
d) where applicable, if the payment is for a fixed period.

3.2. ***Authorisation***

Subject to the Customer providing the consent to the PISP, the PISP will notify the Customer's Bank that the VRP is set up on the Customer's Account. The VRP can only be initiated if the Bank approves the VRP.

3.3. ***Payment Initiation***

Subject to the VRP Instruction and Authorisation being in place, the PISP will upon receipt of the VRP Request from the Buyer initiate the VRP from the Customer's Account to the Client's Destination Account.

3.4. ***Consent Withdrawal***

The parties acknowledge that the Customer can withdraw their Consent to the VRP Instruction at any time. The PISP shall not be required to initiate a VRP request associated with a VRP Instruction if the Consent has been withdrawn.

4. Service Description - VRP Sweeping

4.1. ***Consent and Set Up Request***

The Buyer will provide the Customer with the ability for the Customer to give their consent to the PISP for the VRP Instruction to be set up on the Customer's Account. The VRP Instruction shall include:

a) as a minimum, details of the Customer's Destination Account for sweeping of funds the maximum amount of each payment
b) the maximum amount of each payment per specified interval, and
c) where applicable, if the payment is for a fixed period.

4.2. ***Authorisation***

Subject to the Customer providing the consent to the PISP, the PISP will notify the Customer's Bank that the VRP is set up on the Customer's Account. The VRP can only be initiated if the Bank approves the VRP.

4.3. ***Payment Initiation***

Subject to the VRP Instruction and Authorisation being in place, the PISP will upon receipt of the VRP Request from the Buyer initiate the VRP Sweeping from the Customer's Account to the Customer's Destination Account.

4.4. ***Consent Withdrawal***

The parties acknowledge that the Customer can withdraw their Consent to the VRP Instruction at any time. The PISP shall not be required to initiate a VRP request associated with a VRP Instruction if the Consent has been withdrawn.

5. Buyer Obligations – Commercial VRP (CVRP) non-sweeping

5.1. The Buyer is responsible for obtaining the Customer's Consent to the VRP Instruction and initiating the VRP Request in accordance with the Authorised Consent.

5.2. The Buyer warrants that the Buyer has and will maintain the VRP Instruction required to initiate the VRP Request.

5.3. The Buyer shall have and maintain any integrations required to submit a VRP request to the OBP.

5.4. The Buyer shall notify the Supplier immediately in writing if the Buyer becomes aware of:
   a) Any unauthorised or fraudulent VRP Requests being made.
   b) Any degradation in the performance of the API.

5.5. The Buyer shall indemnify the Supplier against any claims or losses whatsoever or howsoever arising from an unauthorised or fraudulent VRP Requests being made in relation to the Customer's Account.

5.6. The Buyer must provide their Customers with an interface for them to view and cancel ongoing VRP Instruction Consents. The Instruction Consent Management Interface must comply with the principles set out by the Open Banking standards.

6. Buyer Obligations – VRP – Sweeping

6.1. The Buyer is responsible for obtaining the Customer's Consent to the VRP Instruction and initiating the VRP Request in accordance with the Authorised Consent.

6.2. The Buyer agreed that it
   a) holds accounts on behalf of the Customer that qualifies as the VRP Sweeping Account as determined by Open Banking.
   b) has and will maintain the VRP Instruction from the Customer required to initiate the VRP Request.

6.3. The Buyer is acting for the Customer as a TPP to facilitate the Customer transferring funds from the Customer Account to the VRP Sweeping Account.

6.4. The Buyer shall have and maintain any integrations required to submit a VRP request to the OBP.

6.5. The Buyer shall notify the Supplier immediately in writing if the Buyer becomes aware of:
   c) Any unauthorised or fraudulent VRP Requests being made.
   d) Any degradation in the performance of the API.

6.6. The Buyer shall indemnify the Supplier against any claims or losses whatsoever or howsoever arising from an unauthorised or fraudulent VRP Requests being made in relation to the Customer's Account.

6.7. The Buyer must provide their Customers with an interface for them to view and cancel ongoing VRP Instruction Consents. The Instruction Consent Management Interface must comply with the following principles set out by the Open Banking standards.

7. Supplier Obligations

7.1. The Supplier shall provide the APIs to enable the Buyer to transfer data to the OBP.

7.2. The performance of the APIs shall be in accordance with the APIs Relevant Standards as the same may be amended by Open Banking from time to time. Provided always that any updates or amendments shall not be in accordance with the clause 9 (API Change Management).

7.3. To the extent that IPR is provided under these Supplemental Terms, the provisions of the Agreement shall apply.

8. OBP Obligations

8.1. The OBP shall have and will maintain, the appropriate authorisation, consents and/or approvals to submit data into the Banking Infrastructure.

8.2. The OBP acting on behalf of the Buyer shall submit the VRP Request to the Customer's Bank in accordance with the VRP Consent.

9. API Change Management

9.1. The Supplier will make available to the Buyer the relevant API Materials as amended from time to time to enable the Buyer to submit VRP Requests.

9.2. The Supplier may change its VRP APIs or API Materials (API Change) in its sole discretion from time to time on giving notice to the Buyer of at least 90 days prior to the effective date of the API Change, except where a shorter period is required to comply with applicable law or regulation, the requirements of a regulator or the Relevant Standards (API Change Notice), and shall publish the revised API Materials (as appropriate) on its website.

9.3. The Supplier will ensure that the API Change Notice includes sufficient detail to enable the Buyer to understand and take any action required as a result of such API Change.

9.4. Following receipt of an API Change Notice by the Buyer will promptly take any reasonable action required by that API Change Notice.

9.5. The Supplier will use reasonable endeavours to ensure that any API Change which relates to a change to the API does not result in a material degradation of functionality or security of the API.

9.6. For a period of at least 90 days following the effective date of any API Change which relates to a change to the API, which is not backwards compatible, The Supplier will ensure that it supports the then previous version of the API, unless it is prohibited by law, the requirements of a regulator or the Relevant Standards from doing so.

9.7. The parties acknowledge the Relevant Standards may be amended from time to time.

10. Fund Settlement

10.1. The settlement of payments due under the VRP is directly between the Customer's Bank and the Destination Account.

10.2. Neither the Supplier nor the PISP are responsible for the settlement of the payment to the Buyer arising from the VRP providing the VRP request has been submitted to the Customer's Bank.

11. Record Keeping

11.1. In order to comply with the Relevant Standard, retention of data shall be the duration of the mandate plus six years after

a) the last payment transaction or
b) expiry or revocation of the mandate (and be exercised in accordance with data protection law).

11.2. The retained data shall include:

a) VRP Instruction Consents.
b) VRP Instruction Parameters.
c) Payments made under the VRP Instruction.
d) Details of cancellation requests and/or withdrawal of consents.
e) Confirmation of completion of record deletions in accordance with the Relevant Standards.

12. Charges

12.1. The Charges for the VRP Service and payment terms shall be as specified in the VRP Order Form.

13. Liability

13.1. Save to the extent expressly varied herein, the liability of the Buyer and the Supplier shall be as specified in the Agreement.

13.2. Neither the Supplier nor the OBP is liable to the Buyer if:

a) the Buyer fails to receive a payment associated with a VRP Request where such failure is due to an act or omission on the party of the Customer, the Buyer's Bank and/or the Customer's Bank; or

b) the Customer withdraws their consent to the VRP.

13.3. Neither party shall be liable for any failure to provide the VRP Service arising from a failure, suspension and/or reduction in the Banking Infrastructure used to initiate and/or receive the payments associated with the VRP Service. Such failure to include but not limited to cyber and/or operational incidents.

14. Information Requests

14.1. The Buyer shall retrain such data as required to resolve a Customer Dispute.

14.2. Where the Buyer shall promptly provide the PISP and/or OBP such information as may reasonable be requested to investigate a Consumer Dispute including but not limited to:

a) Details of the VRP Instruction.

b) The amount and date of a payment or payments.

c) Any cancellation provided by the Customer to their PISP or OBP.

15. Complaints and Disputes

15.1. If the Buyer receives a Customer Dispute which it reasonably believes the Customer's Bank is required by applicable law and regulation to resolve, the Buyer will promptly and no later than 2 working days from receipt forward the Customer Dispute to the Customer's Bank.

15.2. Inform the Customer that the Customer Dispute has been forwarded, together with an explanation of why it has been forwarded and the name of the Customer's Bank; and will

not provide the Customer with its view as to whether the Customer's Bank will or is likely to refund the Customer.

16. Onboarding and Monitoring

16.1. The Buyer acknowledges that if required for the provision of the VRP Service, the Supplier and/or the OBP may at their sole discretion conduct such CDD Checks in relation to the Buyer and/or the Buyer's business as the Supplier and/or the OBP think fit. Such CDD Checks may be conducted prior to signature of this Agreement and on an ongoing basis.

17. Termination Rights

17.1. In addition to the termination rights in the Agreement, the Supplier may terminate or suspend the VRP Service upon notice in writing to the Buyer if:

a) If the Supplier and/or the OBP receives an adverse report on the Buyer arising from CDD Checks.
b) The Buyer has submitted VRP Requests contrary to the terms of this Schedule (Variable Recurring Payments Service).
c) The Buyer has without due cause, failed to have and/or maintain a VRP Mandate associated with any VRP Request.
d) There are fraudulent VRP Requests made by or on behalf of the Buyer.
e) The Buyer provides access to the API to a third party without prior written consent of the Supplier.
f) The Buyer fails to maintain security associated with use of the API.

Supplier Data Processing Agreement/Data Processing terms

1. Personal Data – Commercial VRP (cVRP) non -sweeping

1.1. To the extent personal data is transferred during the VRP Service, the basis of the transfer is:
a) Independent Controller (Buyer) and Independent Controller (PISP).
b) Customer provides personal data in relation to the VRP Service, Customer has consented to the data being shared with the Buyer and the Bank.
c) PayPoint shall act as processor to the Buyer and the terms of Joint Schedule 10 of the Agreement shall apply.
d) The Buyer shall promptly and no later than 48 hours after the event, notify the Supplier if it experiences a data breach in relation to or impacting the VRP Service.
e) The Buyer shall be responsible for responding to and/or acting when for the Customer exercising their rights under the Data Protection Legislation.

2. Personal Data – VRP Sweeping

2.1. To the extent personal data is transferred during the VRP Service, the basis of the transfer is:
a) Independent Controller (Customer) and Independent Controller (Buyer).
b) Customer provides personal data in relation to the VRP Service, Customer has consented to the data being shared with the Buyer and the Bank.
c) The Supplier and/or OBP shall act as processor to the Buyer and the terms of Joint Schedule 10 of the Agreement shall apply.
d) The Buyer shall promptly and no later than 48 hours after the event, notify the Supplier if it experiences a data breach in relation to or impacting the VRP Service.
e) The Buyer shall be responsible for responding to and/or acting when for the Customer exercising their rights under the Data Protection Legislation.

PART FOUR : Account Information Service (Enhanced) via the Supplier's Portal

For the purposes of the G-Cloud 15 Call Off Contract, RSM 2000 Limited (PayPoint Digital) is a subcontractor to the Supplier.

1. Definitions

Access Identifier: the multiple factor authentication identifier, such as a username, security access token and unique personal identification number (as requested by the client), provided by PayPoint Digital to the Client's User to enable access and use of the Web Service.

Account Information Service (Enhanced) or AIS (E): the service provided to enable Customer to request financial information is provided to the Buyer including but not limited to credit references and credit information.

Account Information Service Provider: as defined in the Payment Services Regulations 2017.

Account Management Contact: the Buyer's nominated individual as set out on the Order Form who shall act as the main contact between the Parties for the purpose of confirming Users and receiving the security access tokens. The Account Management Contact may also be the Supervisor.

Agreement: means the G-Cloud 15 Call Off Contract between the Supplier and the Buyer, which these terms supplement;

AIS Enquiry: the obtaining of financial information in relation to the Customer's payment account by the Credit Reference Agency in their capacity as an Account Information Service Provider.

AIS Request: a consent provided by the Customer to Credit Reference Agency providing permission for the Credit Reference Agency to make an AIS Enquiry in relation to the Customer's payment account.

API: Application Programming Interface.

Banking Infrastructure: the system used to send and receive the Information Requests;

Buyer: the person, firm, local authority, public body, association or company as set out in the Agreement.

Client Portal: the functionality that allows the Buyer to submit Information Requests, view Reports associated with the Financial Information Service;

Client Profile: the Buyer's unique profile created as part of the Web Services and/or Bulk Submission (if applicable).

Credit Reference Agency: An organisation authorised by the Financial Conduct Authority to provide credit references and credit information and as an Account Information Service Provider.

Customer: the organisation and/or individual that is the subject of the Information Request.

Information Request: the request sent by the Buyer to the Customer in the form of a link to a website hosted by PayPoint Digital for the Customer to make an AIS Request to the Credit Reference Agency.

Integration Guide: the specifications and procedures, including but not limited to security requirements as referenced in Schedule 3 (Integration Guide).

OBIE: the Open Banking Implementation Entity and/or any successor thereto providing the access to the confirmation of payee directory and/or register] via the Banking Infrastructure.

Operating Service Hours: The period during which an Information Request can be submitted being 24/7 or such other period as the AIS (E) is available via the industry infrastructure if less.

Order Form: the order form attached to these Terms and Conditions setting out the particulars of the relationship between the Parties and forming part of this Agreement.

Pay.UK: Pay.UK limited company number 10872449 trading as wearepay providing the access to the confirmation of payee directory and/or register**.**

Report: The information provided to the Customer and the Buyer relating to the financial standing of the Customer produced by the Credit Reference Agency. The content of the Report will be as specified in Schedule 4 (Integration and Operations) as the same may be amended from time to time by notice in writing.

Terms and Conditions: the terms and conditions set out herein.

Transaction: means the submission of an Information Request.

Transaction Fees: the fees payable for using the AIS (E) as set out on the Order Form.

User: each of the Buyer's required users (nominated to PayPoint Digital by the Account Management Contact subject to payment of the required fee as set out in the Order Form, provided with Access Identifiers and granted the rights to use the Web Service as set out in this Agreement.

User Credentials: the instructions issued to permit a User to access the Financial Information Service.

Web Service: the website located at the URL provided and notified to the Client by PayPoint Digital for use by the Client pursuant to the terms of this Agreement, through which the Client can create and manage Information Requests.

2. Intentionally Blank

3. Service Overview

3.1. PayPoint Digital will provide the Buyer with the AIS (E) as the same is more fully described in Schedule 2 (Service Description).

3.2. The AIS (E) is only available where Information Requests are made in relation to UK based payments and accounts held with UK banks, building societies and other payment service providers.

3.3. The Credit Reference Agency will be responsible for determining the content of Credit Reference and/or Credit Information provided to the Buyer based on the information requested by the Buyer as specified in Schedule 4.

3.4. The Report will only be provided if the Customer consents via the Credit Reference Agency portal or website (as applicable).

3.5. For the purpose of the Agreement PayPoint Digital will facilitate the receipt of the information for the Buyer. PayPoint Digital is not responsible for the content and has not created the content.

4. Service Availability

4.1. PayPoint Digital will take all reasonable steps to maintain the integrations required to provide the Financial Information Service.

4.2. PayPoint Digital will not be responsible to the Buyer for any failure to provide the AIS (E) due to failure of the Open Banking system, third party systems or networks, a failure on the part of the Credit Reference Agency to respond to a request.

4.3. An Information Request can be made during the Operating Service Hours.

4.4. PayPoint Digital cannot guarantee that all Customer payment accounts will be available for interrogation via the AIS (E).

4.5. PayPoint Digital is entitled to issue a variation to this Agreement in the event the Financial Information Services is amended to include or remove the types of payments and/or accounts.

5. PayPoint Digital Obligations

5.1. PayPoint Digital shall exercise the care of a Reasonable and Prudent Operator in the performance of their respective Services and any additional services provided as may be agreed between the Parties in writing from time to time.

5.2. PayPoint Digital warrants that it and its sub-contractors have obtained and shall maintain all necessary consents and licences to carry out their respective Services.

6. Buyer Obligations

6.1. The Buyer shall ensure it has all necessary consents, permissions and/or authorisation required to make Information Requests.

6.2. The Buyer will not use the AIS (E) in contravention of Applicable Laws.

6.3. The Buyer is responsible for the action of its Users.

6.4. The Buyer is not entitled to use the AIS (E)for the submission of Information Requests on behalf of third parties without PayPoint Digital's prior written consent.

6.5. The Buyer will submit Information Requests via the Web Service and/or the Bulk Submission process (if applicable).

7. Service Access

7.1. During the Term, and subject to the Buyer performing its obligations under this Agreement, PayPoint Digital grants the Buyer a limited non-exclusive, non-transferable, non-sub-licensable right and licence to access and use the Web Services solely as necessary to request, create, manage Information Requests as contemplated by, and pursuant to, this Agreement.

7.2. The Buyer may make the Information Requests via;

7.2.1. the Buyer Portal (individually, via API or as a batch file as specified in the Order Form);

7.2.2. such other submission method as specified in the Order Form.

and must act in accordance with the Operating Instructions associated with the submission method used.

7.3. The Buyer must not:

7.3.1. Interfere or attempt to interfere in any manner with the functionality or proper working of the Web Service and/or Bulk Submission;

7.3.2. Modify, alter, tamper with, repair or otherwise create derivative works included in the Web Service and/or Bulk Submission; and

7.3.3. Reverse engineer, disassemble or decompile the Web Service and/or Bulk Submission.

7.4. PayPoint Digital shall create a Client Profile and shall provide the Buyer (via the Account Management Contact) the Supervisor Access Identifier and Access Identifiers for all initially required Users.

7.5. The Buyer remains responsible for maintaining the secrecy and the security of the Access Identifiers provided by PayPoint Digital. The Buyer is fully responsible, and PayPoint Digital shall bear no liability, for all activities that occur under its Access Identifiers, regardless whether such activities are authorised or unauthorised, or by third parties unless such activities are directly attributed to the fraudulent or negligent acts or omissions of PayPoint Digital.

8. Downtime and Suspensions

8.1. PayPoint Digital shall use reasonable endeavours to ensure any scheduled maintenance, upgrades or modifications to the AIS (E) are conducted outside of Operating Hours. In the event such scheduled work is required during Operating Hours then PayPoint Digital shall use reasonable endeavours to provide no less than 14 (fourteen) days' prior notice to the Buyer.

8.2. The Buyer acknowledges that its access to the AIS (E) may be immediately suspended if:

8.2.1. Emergency maintenance is required;

8.2.2. There is, or is suspected to be, a security breach or a denial of service attack or other attack on the Financial Information Service;

8.2.3. There is any other event, including fraud, which, at PayPoint Digital's sole discretion, may create a risk to the Financial Information Service, the Buyer or any other PayPoint Digital Client if the Web Service is not suspended; or

8.2.4. It is required due to regulatory and/or legal reasons.

9. Charges

9.1. The fees and charges payable are as specified in the Agreement. All charges shall be invoiced by and payable to the Supplier.

10. Unauthorised Requests

10.1. The Buyer is responsible for the prevention of the use of the AIS (E) to make unauthorised, malicious or excessive Information Requests ("Unauthorised Use") and for the submission and management of all Information Requests.

10.2. The Buyer will notify PayPoint Digital if the Buyer becomes aware of Unauthorised Use of the Financial Information Service.

10.3. The Buyer will, if so requested in writing by PayPoint Digital provide PayPoint Digital with details of the Buyer's Users to prevent Unauthorised Use of the Financial Information Services.

10.4. If PayPoint Digital reasonably suspects that an act or acts of Unauthorised Use of the AIS (E) or any other analogous illegal activity has taken place or may take place, the Buyer shall co-operate fully with any reasonable requests made by PayPoint Digital.

10.5. In the event that PayPoint Digital, in its sole discretion (acting reasonably at all times) believes that the Buyer is not fully co-operating with its requests, PayPoint Digital shall be entitled to require the Buyer to make all necessary changes to the Unauthorised Use measures and the Buyer shall bear all reasonable costs of making such changes.

10.6. Where the Buyer continues not to co-operate with PayPoint Digital pursuant to clause 10.5 (Unauthorised Requests), PayPoint Digital shall be entitled (acting reasonably at all times) to suspend the Financial Information Services indefinitely until such co-operation is forthcoming and where the Buyer continues to not co-operate, PayPoint Digital shall be entitled to terminate this Agreement immediately.

11. Regulatory Changes

11.1. If during the Term of this Agreement any matter shall arise as a result of any change in the law (including judicial interpretation) or in any statute, statutory instrument, order, directive or regulation or in any guidance notes or codes of practice which affects PayPoint Digital's ability to provide the AIS (E), then PayPoint Digital, on written notice to the Buyer, shall be entitled to either amend the AIS (E) so they comply with such change or immediately terminate the provision of the AIS (E) without any liability to the Buyer.

11.2. PayPoint Digital may amend, vary, suspend and/or terminate the Agreement if any permission, exemption, variation, consent and/or accreditation, the Rules, required to offer the AIS (E) is amended, terminated, suspended and/or expires.

12. Data

12.1. In relation to the AIS (E) the Buyer is the Controller and PayPoint Digital is the Processor.

12.2. For the purposes of this Agreement in relation to the processing and exchange of Personal Data under this Agreement the provisions of Schedule 3 (Data Protection Addendum) shall apply. The obligations of this clause 12 (Data) shall survive the termination of this Agreement.

12.3. All Parties shall comply with their requirements pursuant to all applicable data protection law, including the Data Protection Act 2018, all amendments and updates thereto and replacements thereof as such requirements arise in connection with this Agreement.

Schedule 1 – Order Form

Administration	
Account Management Contact (Buyer):	Name: E-mail: Address: Phone:
PayPoint Digital Contact:	Name: E-mail: Address: Phone:
PayPoint Digital Contact Billing	Name: E-mail: Address: Phone:
Commencement Date:	As stated in the Agreement
Initial Term:	As stated in the Agreement
Charges	
Set Up Fees (Single Payment - Payable on Signature)	As stated in the Agreement
Management Fee (Payable Monthly)	
Transaction Fee (Payable on each Information Request)	
User Licence Fee (For each User – Payable annually).	
Other Charges:	
Users	
Number of Level 1 Users	
Number of Finance Users	
SMS or Security Code Charges	
Special Conditions	
(if applicable)	
Invoicing	
Invoices will be provided by PayPoint Digital's Billing Service Provider. Payment to the Billing Service Provider in respect of an invoice issued will be deemed to be a payment to PayPoint Digital to the value of the funds received.	**The Supplier**

Schedule 2 – Service Description

1. Compliance

1.1. When submitting an Information Request, each party will comply with the Applicable Laws.

1.2. The Buyer will ensure the Customer is aware that a Credit Reference or AIS will be requested as part of the process for obtaining the Information Request.

2. Process

2.1. PayPoint Digital will provide the AIS (E) during Service Operating Hours.

2.2. To use the Financial Information Service;

2.2.1. The User will log on to the Client Portal.

2.2.2. The User will send an Information Request to the Customer that will, subject to the Consumer indicating their consent, enable the Customer to request the Credit Reference Agency make an AIS Request in relation to the Consumer's payment account.

2.2.3. The Buyer will ensure the Customer is aware that in making the AIS Request a Credit Reference will be obtained in relation to the Customer.

2.2.4. The Customer's consent to the AIS Request will be submitted by PayPoint Digital to the Credit Reference Agency.

2.2.5. The Credit Reference Agency will obtain the information in relation to the Customer's payment account via the AIS Request and provide a Credit Reference in the form of a Report.

2.2.6. The Credit Reference Agency will provide the Customer with access to the Report in a secure location.

2.2.7. The Credit Reference Agency will provide a visibility of the Report to PayPoint Digital, if personal data is disclosed PayPoint Digital will act as processor for the Buyer.

2.2.8. The User can access the Client Portal to view the Report and if required, download a copy.

2.2.9. [The Report will be held on the Client Portal for a period of twenty-eight (28) days. Once this period has expired PayPoint Digital will delete the Report from the Client Portal. Delete if no storage provided.]

2.3. PayPoint Digital will not amend the Report and is not responsible for the content of the Report.

3. Fraud and Crime

3.1. PayPoint Digital will permit the Buyer to submit an Information Request, except where PayPoint Digital has reasonable concerns on the validity of the Information Request.

3.2. PayPoint Digital may monitor where the Buyer is making multiple Information Requests to assess if the behaviour is an indication of fraud or wrongful activity.

3.3. PayPoint Digital is entitled to suspend, terminate and/or restrict the service if PayPoint Digital has concerns in relation to the Buyer's use of the AIS (E) and/or if the regulatory status of the Credit Reference Agency is changed.

Supplier Data Processing Agreement/Data Processing Term

Schedule 3 - DATA PROTECTION ADDENDUM

Controller to Controller

A. Overview

When providing the AIS (E) or using the AIS (E) a party shares Personal Data with the other or otherwise Processes such Personal Data under the Agreement(s).

PayPoint Digital shall act as Processor and the Buyer shall be the Controller.

1. Definitions

1.1. For the purpose of this Addendum the following additional definitions will apply;

Account Information Service	A request made by the Customer to enable account information to be accessed by Aperidata Limited for the purpose of providing the financial information to the Buyer.
Agreement(s)	The G-Cloud 15 Call Off Contract the Supplier and the Buyer for payment services and/or technology services.
Controller	shall have the meaning given in the Data Protection Legislation.
Customer	Means the Data Subject who is subject of the Information Request.
Customer Data	Means data identifying the individual provided by the Buyer.
Data Protection Legislation	the UK General Data Protection Regulation **("UK GDPR")** and any regulations and secondary legislation, as amended or updated from time to time, in the UK and (ii) any successor legislation to the UK GDPR or the Data Protection Act 2018. In each case interpreted in accordance with the DP Guidance.
Data Subject	shall have the meaning given in the Data Protection Legislation;
DP Guidance	means any and all guidelines, recommendations, best practice, opinions, directions, codes of practice and codes of conduct issued, adopted, recommended or approved the UK's Information Commissioner's Office and/or any other supervisory authority or data protection authority from time to time (whether or not legally binding) in relation to the processing of personal data, data privacy, electronic communications, marketing and/or data security.
Personal Data	shall have the meaning given in the Data Protection Legislation.
Personal Data Breach	shall have the meaning given in the UK GDPR.
Processor	shall have the meaning given in the Data Protection Legislation.
Processing	**Processing**" shall have the meaning given in the Data Protection Legislation, and "**Process**" and "**Processed**" shall be construed accordingly
Representative	means employees, staff, (excluding third parties providing industry services) sub-contractors and invitees of the Processor, engaged or due to be engaged in the provision of the Services or required to carry out obligations of the Processor under this Agreement.

Services	The services as the same are more fully described in the Agreement(s).
Service Data	The personal data exchanged between the parties to enable a Information Request to be made and the AIS (E) to be provided.
Technical Standards	The industry standards applied to the Service.

2. Processing Activities

2.1. PayPoint Digital will provide the processing services as described more fully in Data Protection clause 12(Processing Description) for the provision of the Service to the Buyer and the Service Data to the Buyer.

3. **Processor obligations**

3.1. Where PayPoint Digital acts as a Processor in respect of Personal Data (other than Shared Data) and the Buyer is the Controller, the Processor shall:

3.1.1. Process the Personal Data in accordance with the Agreement and such documented instructions as are given by the Controller from time to time. Any change in the instruction such as to vary the form of processing will be regarded as and subject to change control;

3.1.2. apply appropriate technical and organisational measures which are sufficient to comply with Article 32 of the GDPR (as appropriate) or any provisions to be applied to the transfer of Personal Data outside the United Kingdom applicable at the time of the transfer under the Data Protection Legislation;

3.1.3. ensure that its staff and any persons authorised to process the personal data have committed themselves to confidentiality through a written agreement with the PayPoint Digital and/or its Sub-Processor;

3.1.4. in relation to any persons authorised to Process (or who may otherwise have access to) Personal Data ensure that such persons adhere to the terms of this Agreement;

3.1.5. assist the Controller in ensuring compliance with Articles 32 to 36 of the GDPR (inclusive)) taking into account the nature of Processing and the information available to the Processor. The Processor may make a reasonable charge for this assistance.

3.1.6. upon the request of the Buyer, provide assistance to the Buyer relating to the Buyer's security; impact assessment; data breach reporting requirements and data protection or data privacy authority consultation obligations under the Data Protection Legislation. To the extent such assistance is not an obligation imposed upon the Processor under the Data Protection Legislation, the Processor may charge the Buyer its reasonable costs (or the rates otherwise agreed between the parties) for its time spent and expenses incurred in providing the Buyer with co-operation and assistance as required by this clause 3 (Processor Obligations) any such assistance being subject to agreement in writing;

3.1.7. taking into account the nature of the Processing Activities, assist the Buyer by undertaking the appropriate technical and organisational measures, insofar as this is possible, to respond to requests for exercising a Data Subject's rights in accordance with the Data Protection Legislation.

4. Data Transfer

4.1. The Processor may not transfer Personal Data to a third country that is outside the EEA without the appropriate or suitable safeguards to provide an adequate level of protection

such as are required under the Data Protection Legislation in order to ensure that the level of protection of natural persons guaranteed by the Data Protection Legislation is not undermined;

4.2. To the extent the transfer of Personal Data is required to enable the processing of the Personal Data in accordance with Scheme Rules, the Controller hereby gives consent to the processing subject to the Processor ensuring the appropriate controls, consents and protections are in place consistent with the requirements of the Data Protection Legislation.

4.3. The Processor will publish details of the transfers to any Sub-processors as specified in Clause 8 (Sub-processors).

5. Compliance

5.1. Each party shall at all times comply with the provisions of the Data Protection Legislation in connection with this Agreement and its performance of the Services (including the Processing Activities).

5.2. The Buyer warrants, represents and undertakes to PayPoint Digital that;

5.2.1. The Buyer has lawful grounds for processing the Personal Data.
5.2.2. Any instruction given by the Buyer, policy or procedure shall be lawful.

5.3. PayPoint Digital represents warrants and undertakes that;

5.3.1. The Personal Data will be processed in accordance with the Data Protection Legislation.
5.3.2. It and/or its Sub-contractors have and will for the duration of the Agreement maintain the appropriate authorisations, accreditations and/or permissions to process the Personal Data.

5.4. Each party shall promptly and without undue delay inform the other in writing:

5.4.1. if, in its opinion, an instruction or request by or on behalf of the Buyer, infringes the Data Protection Legislation;
5.4.2. in the event that it becomes aware of any breach of the Data Protection Legislation (including its Sub-Processors) in connection with this Agreement; and
5.4.3. of any provisions in any local law or of any changes in the laws of the country in which Personal Data is processed which does or could affect the Processor's ability to perform its obligations under this Schedule (Data Protection).

5.5. The parties confirm that the information relating to the subject matter and duration of the processing; the nature and purpose of the processing; the type of personal data; the categories of the data subjects; and the obligations and rights of the data controller have been set out in this Agreement.

5.6. A party shall notify the other party promptly and in any event within thirty-six (36) hours:

5.6.1. if it is required by Data Protection Legislation to act other than in accordance with any of the other party's instructions, provided that the Processor party is not prohibited by law from so notifying the other party; and/or
5.6.2. if it considers, in its opinion (acting reasonably), that any of the other party's instructions infringe any of the Data Protection Legislation; and/or
5.6.3. notify the other party promptly (and in any event within thirty-six (36) hours) following its receipt of any request, notice or complaint from a Data Subject exercising their

rights under the Data Protection Legislation (a "Data Subject Request") or any correspondence (whether written or verbal) from the ICO, and will provide the other party with all reasonable co-operation and assistance required by the other party in relation to any such Data Subject Request or ICO Correspondence.

6. Security

6.1. The Processor shall as appropriate;

6.1.1. taking into account the nature of the processing, state of art, the costs of implementation and the scope, context and purpose of the processing implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk;
6.1.2. apply the pseudonymisation and encryption of personal data;
6.1.3. have the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
6.1.4. have the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
6.1.5. process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
6.1.6. take steps to ensure that any natural person acting under the supervision of the Processor who has access to personal data does not process the Personal Data except on instructions from the Controller, unless they are is required to do so by law.

7. Data Breach Notification

7.1. PayPoint Digital shall without undue delay notify the Buyer immediately (and in any event no later than 36 hours) after having Personal Data Breach. Such notification shall:

7.1.1. describe the nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of the Personal Data records concerned; and
7.1.2. describe the measures taken or proposed to be taken by the Processor and/or its Sub-Processor to address the Personal Data Breach, including where appropriate measures to mitigate its possible adverse effects.
7.1.3. describe the implementation of any measures necessary to restore the security of compromised Personal Data, and
7.1.4. support the Buyer to make any notifications to the UK Information Commissioner's Office ("ICO") or affected Data Subjects

8. Use of Sub-processors

8.1. The Processor may only engage Sub-processors in accordance with the requirements set forth in this clause 8 (Use of Sub-processors).

8.2. The Controller acknowledges and agrees that the Processor's group companies may be retained as Sub-processors.

8.3. To the extent the Processor uses Sub-processors to Process the Controller's Personal Data, the Processor shall make available to the Controller a current list of Sub-processors for the respective Services with the identities of those Sub-processors (the **Sub-processor List**).

8.4. The Processor shall provide the Controller access updates on the Processor's website ("the Designated Web Page) to enable the Controller to have access to the relevant Sub-processor List and shall provide such updates via the Designated Web Page before authorising any new

Sub-processor(s) to Process Personal Data in connection with the provision of or use of the Services.

8.5. The Controller shall have the right to object the use of any particular Sub-processor by Processor. Such objection to be provided no later than seven (7) days after the publication of the Sub-processor's details on the Processor's Designated Web Page.

8.6. The Processor shall be liable for the acts and omissions of its Sub-processors to the same extent the Processor would be liable if performing the services of each Sub-processor directly under the terms of this Schedule, except as otherwise set forth in this Agreement.

8.7. To the extent the Controller uses a Service for which the use of a Sub-processor is included in a general authorisation, the terms of the general authorisation are set out on the Designated Web Page.

8.8. The Processor shall ensure that the Sub-processor contract (as it relates to the Processing of Personal Data) is on terms which are substantially the same as, and in any case no less onerous than, the terms set out in this Addendum.

9. Audits

9.1. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller and shall immediately inform the Controller if, in its opinion, an instruction infringes the Data Protection Legislation.

9.2. The Processor make available to the Buyer such information as the Buyer reasonably requests and the Processor is reasonably able to provide, and, permit and contribute to such audits, including inspections, conducted by the Buyer (or the Buyer's appointed auditors), as is necessary to demonstrate the Processor's compliance with the Data Protection Legislation subject to the applicable legal, regulatory and payment card accreditations. The Buyer will give reasonable notice of any audit and unless there are reasonable grounds to suspect a breach will limit audits to one annually.

9.3. Any audit is subject to the Processor's, legal, regulatory and/or payment industry accreditations including but not limited to PCI accreditation, its data processing facilities, procedures and documentation to be submitted for scrutiny, inspection or audit by the other party and/or provide the other party with written evidence of its compliance with the requirements of this clause 9 (Audits).

9.4. To the extent an audit is not permitted and/or restricted the Processor shall at all times be compliant with its obligations under this Agreement and shall demonstrate its compliance with the provision of the appropriate industry accreditation certification.

10. Retention and Transfer

10.1. If so requested by the Controller, the Processor will, during the term of this Agreement subject to legal and regulatory requirements and obligations, delete and/or transfer the Personal Data to the Controller.

10.2. The method and security of any such transfer to be agreed by the parties at the time and subject to the appropriate measures to ensure the security and integrity of the Personal Data, having account of cost and adequacy of any such measure as of the date of the transfer.

10.3. Any deletion of Personal Data undertaken by the Processor under this clause 10 (Retention and Transfer) shall be undertaken securely and in accordance with the relevant Data Protection Legislation.

10.4. Within thirty (30) days of Termination or Expiry of the Agreement, in a format acceptable to each party, to the extent permitted by law, payment card rules, payment service requirement and obligations, permanently delete, destroy or return all of the Personal Data the Buyer following termination or expiry of this Agreement and delete existing copies of such Personal Data unless (and only to the extent) the Processor is required to retain copies in order to comply with applicable law.

10.5. If following termination of the Agreement, the parties fail to agree a transfer date, format and process, the Processor may subject to legal and/or regulatory requirements, upon the provision of not less than thirty (30) days notice in writing delete the Personal Data.

10.6. The Processor may charge for any associated costs in relation to any cleansing, deletion or transfer of the Personal Data such costs and method of transfer to be agreed in writing by the parties at the time.

11. Processing Description

11.1. The legal basis for processing shall be:

11.1.1. Where necessary to carry out the Processor's obligations under this Agreement or to take steps to enter into an agreement with the Buyer; and/or

11.1.2. Where the law requires this processing.

12. Personnel and Training

12.1. The Processor will ensure that all appropriate Representatives are aware of and behave in accordance with the terms of the Processor obligations and confidentiality obligations contained in this Addendum.

12.2. The Processor shall and shall use reasonable endeavours to procure that all persons providing services under this Agreement are aware of and shall comply with the Data Protection Laws, and in particular the data protection principles set out therein, in connection with the subject matter of this Agreement.

13. Data Subject Requests

13.1. The Processor shall;

13.1.1. provide such co-operation and assistance to the Controller as the Controller may reasonably require to allow the Controller to comply with the rights of Data Subjects, including subject access rights and/or information notices served by any data protection authority;

13.1.2. refer to the Controller any communication from Data Subjects making a data subject access request and/or any other request in respect of the data, any Competent Authority or to either party's compliance with the Data Protection Laws and the Processor shall not, subject to any legal, statutory and/or regulatory obligation (when they shall to the extent permitted by law, advise the Controller of any such disclosure) disclose or release any Information to such a third party without obtaining the consent of the Controller.

13.1.3. provide such assistance as the Controller may reasonably require to enable the Controller to comply with its obligations pursuant to the Data Protection Laws to implement appropriate technical and organisational measures to ensure appropriate security of processing, to notify Personal Data Breaches to the Competent Authority and relevant Data Subjects, to carry out data protection impact assessments and/or to consult with the Competent Authority in relation to such assessments, as appropriate.

13.1.4. The Processor shall be entitled to charge the Controller a fee for such assistance as specified in this Addendum.

14. Retention, Correction and Deletion

14.1. The Processor shall if so instructed by the Controller will promptly;

14.1.1. comply with the Controller's instructions to return, delete, update and/or amend the Personal Data for the purpose of ensuring the accuracy and validity of the Personal Data; and

14.1.2. comply with the Controller's instruction to restrict, restrain from and/or suspend Processing of an individual Data Subject's Personal Data.

14.2. Any deletion of Personal Data undertaken by the Processor shall be as instructed by the Controller and undertaken securely and in accordance with the relevant Data Protection Laws.

15. Categories of Personal Data and Purpose.

15.1. For the purpose of this Addendum the categories of Data Subject may include:
PayPoint Digital employees, contractors, PayPoint Digital clients, customers of clients.

15.2. The Personal Data does not include Special Categories of Personal Data.

15.3. The purpose for which the Personal Data is provided is the Services as specified in the Agreement.

15.4. The duration of the processing will be the duration of the Agreement or such other period as the parties may agree in writing.

15.5. Either party may from time to time notify the other if this clause 15 (Categorise of Personal Data and Purpose) needs to be amended to reflect any changes made (or proposed to be made) to the processing of Personal Data under the Agreement, in which case both parties will act reasonably and in good faith in agreeing appropriate amendments so that description of the Personal Data remains accurate and complete.

General

16. Processing Description

Description	**Details**
Subject matter of the processing	Provision of the following to the extent specified in the product description for the Financial Information Services under the Agreement(s): • Credit Reference relating to the Customer. • Client User information (when using the Client Portal).
Duration of the processing	Term of the Agreement.

Nature and purpose of processing	• Storage • Processing • User log on, email and IP location in relation to Information Request generation or accessing reports via a portal.
Types of Personal Data	Personal Data. There are no Special Categories of Personal Data required for the processing.
Categories of Data Subject	• Customers of the Buyer • Employee and Contractors (Buyer and PayPoint Digital)
Plans for return or destruction of Personal Data	Controller to instruct. Please not data required for the Processor to comply with legal and/or regulatory obligations shall be retained for compliance purposes.
Permitted Transfers	To the extent required to perform the Financial Information Services as specified in the Agreement(s) or associated with the Agreement including but not limited to: • Financial Conduct Authority. • HMRC and other Tax Authorities. • Police and Investigatory Bodies. • Regulatory bodies and authorities including government and quasi government organisations. • Payment service providers and/or organisation acting as technical service provider under the Payment Service Regulations 2017. • Regulated telecommunication service providers. • OBIE • Pay.UK • Information Commissioner's Office. • Auditors • Sub-processor(s).
Non EEA Transfers (PayPoint Digital)	To the extent required to provide Services under the Agreement(s) and subject to clause 3 (Warranties) above (as applicable); • USA and other locations – Microsoft Inc. • USA and other locations – Salesforce Inc. Details of PayPoint Digital non EEA processing is available by e-mailing privacy@paypoint.com .
Processing Instructions and Technical Standards	The Processor will comply with the rules, standards and regulations applicable to the Information Request or similar including but not limited to those applied by the OBIE and/or Pay.UK. Any instruction from the Buyer shall comply with these Standards. Any change in instruction and or applicable Technical Standards shall be subject to change control and

	PayPoint Digital may charge for the implementation of such changes.
Personal Data Fields	May include any of the following: • Name: • E-mail Address; • Phone or contact details: • Bank account or payment account details. • Financial information relating to the Customer provided in relation to the Customer's Account Information Service requests. Please note, not all the above will include Personal Data being data that can identify a living individual when in the possession of the Processor. Personal Data will only be provided to the extent required to provide or receive Services under the Agreement.
Sub-processors	Aperidata Limited – Account information service provider and credit reference agency. PayPoint Network Limited – processor to PayPoint Digital

17. Data Protection Officer

17.1. The contact details for the PayPoint Digital Data Protection Officer are:

Data Protection Officer
PayPoint Digital Group
1 The Boulevard,
Shire Park,
Welwyn Garden City,
Hertfordshire,
AL7 1EL

E-mail: privacy@paypoint.com

17.2. The details of the Buyer Data Protection Officer (if any) will be notified by the Buyer to PayPoint Digital no later than 28 days after the date of this Agreement, by e-mailing privacy@paypoint.com.

18. Personal Data and processing activity

Subject matter of the processing	Information Requests
Duration of the processing	Transaction processing is transient at the point of time of the Information Request and thereafter for the duration of the Agreement or

	such other period as required to comply with payment industry standards.
Nature and purpose of the processing	The nature and purpose of the processing is to enable the verification of the data subject.
Type of personal data	Personal data to support the payment for goods and services, including name, account details, and payment details associated with the payment as defined by the Buyer, organisation, bank, payment system or scheme.
Categories of data subjects	Individuals being Customers of the Buyer. Employees and Representatives of PayPoint Digital and/or the Buyer.
Obligations and rights of the Buyer	As defined in the terms in this agreement.

Schedule 4 – Integration and Operation

1. Integration and Operations

1.1. The integration will be in accordance with the documentation provided as part of the developer integration.

1.2. The operation of the Service including the use of Bulk Submission, an API and/or any other submission methods will be as specified in the Operating Instructions.

1.3. For the propose of this Schedule 4, Operating Instructions shall available on the website as notified by PayPoint Digital to the Buyer from time to time.

1.4. The Reports will be viable to the Buyer via the on screen and/or portal access to which will be supported by PayPoint Digital.

2. Report Content

2.1. The Report will consist of the following information:

[insert] TO BE CONFIRMED

PART FIVE : Account Information Service (Enhanced) via the Aperidata Portal

For the purposes of the G-Cloud 15 Call Off Contract, RSM 2000 Limited (PayPoint Digital) is a subcontractor to the Supplier.

1. **Definitions**

Access Identifier: the multiple factor authentication identifier, such as a username, security access token and unique personal identification number (as requested by the client), provided by PayPoint Digital to the Client's User to enable access and use of the Web Service.

Account Information Service (Enhanced) or AIS (E): the service provided to enable Customer to request financial information is provided to the Buyer including but not limited to credit references and credit information.

Account Information Service Provider: as defined in the Payment Services Regulations 2017.

Account Management Contact: the Buyer's nominated individual as set out on the Order Form who shall act as the main contact between the Parties for the purpose of confirming Users and receiving the security access tokens. The Account Management Contact may also be the Supervisor.

Agreement: means the G-Cloud 15 Call Off Contract between the Supplier and the Buyer, which these terms supplement;

AIS Consent: a consent provided by the Customer to Service Provider providing permission for the Service Provider to make an AIS Request in relation to the Customer's payment account.

AIS Request: The request from the Customer following an AIS Consent for information in relation to their financial standing to be provided to the Account Information Service Provider.

API: Application Programming Interface.

Banking Infrastructure: the system used to send and receive the Information Requests;

Buyer: the person, firm, local authority, public body, association or company as set out in the Agreement.

Client Portal: the functionality that allows the Buyer to submit Information Requests, view Reports associated with the Financial Information Service;

Client Profile: the Buyer's unique profile created as part of the Web Services and/or Bulk Submission (if applicable).

Customer: the organisation and/or individual that is the subject of the Information Request.

Financial Information: any or all of the following

a) Name of account holder;
b) Bank Sort Code;
c) Bank Account number;
d) Available overdraft;
e) Bank account balance;

f) Transaction data (including card transactions, payments, standing orders and direct debits);

Information Request: the request sent by the Buyer to the Customer in the form of a link to a website hosted by PayPoint Digital for the Customer to make an AIS Request to the Service Provider.

Integration Guide: the specifications and procedures, including but not limited to security requirements as referenced in Schedule 3 (Integration Guide).

Open Banking Operator: the entity providing the access to Open Banking Infrastructure.

Open Banking: The banking infrastructure supporting AIS Requests.

Operating Service Hours: The period during which an Information Request can be submitted being 24/7 or such other period as the AIS (E) is available via the industry infrastructure if less.

Order Form: the order form attached to these Terms and Conditions setting out the particulars of the relationship between the Parties and forming part of this Agreement.

Pay.UK: Pay.UK limited company number 10872449 trading as wearepay providing the support to the Open Banking infrastructure**.**

Report: the information generated by the Service Provider that sets out the Financial Information allocated to a particular Customer following the collection, analysis and computation of their Financial Information to generate the Report and if requested by the Customer to be provided to the Buyer, the transaction data collated from the Financial Information.

Service Provider: An organisation authorised by the Financial Conduct Authority to provide credit references and financial information and is an Account Information Service Provider. The Service Provider is Aperidata Limited a company registered with the Financial Conduct Authority as an Account Information Service Provider with FRN 949181.

Terms and Conditions: the terms and conditions set out herein.

Transaction: means the submission of an Information Request.

Transaction Fees: the fees payable for using the AIS (E) as set out on the Order Form.

User: each of the Buyer's required users (nominated to PayPoint Digital by the Account Management Contact subject to payment of the required fee as set out in the Order Form, provided with Access Identifiers and granted the rights to use the Web Service as set out in this Agreement.

User Credentials: the instructions issued to permit a User to access the Financial Information Service.

Web Service: the Service Provider's website located at the URL provided and notified to the Buyer by PayPoint Digital for use by the Buyer pursuant to the terms of this Agreement, through which the Buyer can create and manage Information Requests.

2. **Intentionally Blank**

3. **Service Overview**

3.1. PayPoint Digital will instruct the Service Provider to provide the Buyer with the AIS (E) as the same is more fully described in Schedule 2 (Service Description).

3.2. The AIS (E) is only available where Information Requests are made in relation to UK based payments and accounts held with UK banks, building societies and other payment service providers.

3.3. The Service Provider will be responsible for determining the content of Financial Information provided to the Buyer based on the information requested by the Buyer as specified in Schedule 4.

3.4. The Report will only be provided if the Customer consents via the Service Provider portal or website (as applicable).

3.5. PayPoint Digital will manage the relationship with the Service Provider including payment of invoices on behalf of the Buyer's Transactions when using of the AIS (E) due to the Service Provider. PayPoint Digital shall be liable to the Buyer for any acts or omissions of the Service Provider in connection with the provision of the AIS (E) as if such acts or omissions were its own.

3.6. For the purpose of the Agreement PayPoint Digital will facilitate the receipt of the information for the Buyer. PayPoint Digital is not responsible for the content and has not created the content.

4. **Service Availability**

4.1. PayPoint Digital will use reasonable endeavours to ensure the Service Provider maintains the integrations required to provide the Buyer with details of the availability of the Financial Information Service.

4.2. PayPoint Digital will not be responsible to the Buyer for any failure to provide the AIS (E) due to failure of the Open Banking system, third party systems or networks

4.3. An Information Request can be made during the Operating Service Hours.

4.4. PayPoint Digital cannot guarantee that all Customer payment accounts will be available for interrogation via the Financial Information Service.

4.5. PayPoint Digital is entitled to issue a variation to this Agreement in the event the AIS (E) is amended to include or remove the types of payments and/or accounts as notified by Pay.UK to the participants. In the event such variation has a materially adverse impact on the Services in the Buyer's reasonable opinion, then the Buyer shall discuss with PayPoint Digital to agree a mutually acceptable way forward such the Services are not materially impacted. If this cannot be mutually agreed within a reasonable timescale, then the Buyer shall have the right to terminate this Agreement without incurring any costs (other than fees due to be paid).

4.6. The service levels applicable to the Service is as specified in Schedule 5 (Service Levels).

5. **PayPoint Digital Obligations**

5.1. PayPoint Digital shall exercise the care of a Reasonable and Prudent Operator in the performance of their respective Services and any additional services provided as may be agreed between the Parties in writing from time to time.

5.2. PayPoint Digital warrants that it and its sub-contractors have obtained and shall maintain all necessary consents and licences to carry out their respective Services.

6. **Buyer Obligations**

6.1. The Buyer shall ensure it has all necessary consents, permissions and/or authorisation required to make Information Requests.

6.2. The Buyer will not use the AIS (E) in contravention of Applicable Laws.

6.3. The Buyer is responsible for the action of its Users.

6.4. The Buyer is not entitled to use the AIS (E) for the submission of Information Requests on behalf of third parties without PayPoint Digital's prior written consent.

6.5. The Buyer will submit Information Requests via the Web Service and/or the Bulk Submission process (if applicable).

7. **Service Access**

7.1. During the Term, and subject to the Buyer performing its obligations under this Agreement, PayPoint Digital grants the Buyer a limited non-exclusive, non-transferable, non-sub-licensable right and licence to access and use the Web Services solely as necessary to request, create, manage Information Requests as contemplated by, and pursuant to, this Agreement.

7.2. The Buyer may make the Information Requests via;

7.2.1. the Client Portal (individually, via API or as a batch file as specified in the Order Form);

7.2.2. such other submission method as specified in the Order Form.

and must act in accordance with the Operating Instructions associated with the submission method used.

7.3. The Buyer must not:

7.3.1. Interfere or attempt to interfere in any manner with the functionality or proper working of the Web Service and/or Bulk Submission;

7.3.2. Modify, alter, tamper with, repair or otherwise create derivative works included in the Web Service and/or Bulk Submission; and

7.3.3. Reverse engineer, disassemble or decompile the Web Service and/or Bulk Submission.

7.4. PayPoint Digital shall create a Client Profile and shall provide the Buyer (via the Account Management Contact) the Supervisor Access Identifier and Access Identifiers for all initially required Users.

7.5. The Buyer remains responsible for maintaining the secrecy and the security of the Access Identifiers provided by PayPoint Digital. The Buyer is fully responsible, and PayPoint Digital shall bear no liability, for all activities that occur under its Access Identifiers, regardless whether such activities are authorised or unauthorised, or by third parties unless such activities are directly attributed to the fraudulent or negligent acts or omissions of PayPoint Digital.

8. **Downtime and Suspensions**

8.1. PayPoint Digital shall use reasonable endeavours to ensure any scheduled maintenance, upgrades or modifications to the AIS (E) by the Service Provider are conducted outside of Operating Hours. In the event such scheduled work is required during Operating Hours by the Service Provider then PayPoint Digital shall use reasonable endeavours to provide no less than 14 (fourteen) days' prior notice to the Buyer unless security concerns mean such length of notice cannot be provided, in which case PayPoint Digital shall provide as much notice as is reasonably possible given the circumstances.

8.2. The Buyer acknowledges that its access to the AIS (E) may be immediately suspended if:

8.2.1. Emergency maintenance is required;

8.2.2. There is, or is suspected to be, a security breach or a denial of service attack or other attack on the Financial Information Service;

8.2.3. There is any other event, including fraud, which, at PayPoint Digital's sole discretion, may create a risk to the Financial Information Service, the Buyer or any other PayPoint Digital Client if the Web Service is not suspended; or

8.2.4. It is required due to regulatory and/or legal reasons.

9. **Charges**

9.1. The fees and charges payable are as specified in the Agreement. All charges shall be invoiced by and payable to the Supplier.

10. **Unauthorised Requests**

10.1. The Buyer is responsible for the prevention of the Buyer's use of the AIS (E) to make unauthorised, malicious or excessive Information Requests ("Unauthorised Use") and for the submission and management of Information Requests.

10.2. The Buyer will notify PayPoint Digital if the Buyer becomes aware of Unauthorised Use of the Financial Information Service.

10.3. The Buyer will, if so requested in writing by PayPoint Digital provide PayPoint Digital with details of the Buyer's Users to prevent Unauthorised Use of the Financial Information Services.

10.4. If PayPoint Digital reasonably suspects that an act or acts of Unauthorised Use of the AIS (E) or any other analogous illegal activity has taken place or may take place, the Buyer shall co-operate fully with any reasonable requests made by PayPoint Digital.

10.5. In the event that PayPoint Digital, in its sole discretion (acting reasonably at all times) believes that the Buyer is not fully co-operating with its requests, PayPoint Digital shall be entitled to require the Buyer to make all necessary changes to the Unauthorised Use measures and the Buyer shall bear all reasonable costs of making such changes.

10.6. Where the Buyer continues not to co-operate with PayPoint Digital pursuant to clause 17.5 (Unauthorised Requests), PayPoint Digital shall be entitled (acting reasonably at all times) to suspend the Financial Information Services indefinitely until such co-operation is forthcoming and where the Buyer continues to not co-operate, PayPoint Digital shall be entitled to terminate this Agreement immediately.

11. **Regulatory Changes**

11.1. If during the Term of this Agreement any matter shall arise as a result of any change in the law (including judicial interpretation) or in any statute, statutory instrument, order, directive or regulation or in any guidance notes or codes of practice which affects PayPoint Digital's ability to provide the AIS (E), then PayPoint Digital, on written notice to the Buyer, shall be entitled to either amend the AIS (E) so they comply with such change or immediately terminate the provision of the Financial Information Services without any liability to the Buyer.

11.2. PayPoint Digital may amend, vary, suspend and/or terminate the Agreement if any permission, exemption, variation, consent and/or accreditation, the Rules, required to offer the AIS (E) is amended, terminated, suspended and/or expires.

12. **Data**

12.1. In relation to the AIS (E) the Buyer is a Controller and Service Provider is a Controller.

12.2. For the purposes of this Agreement in relation to the processing and exchange of Personal Data under this Agreement the provisions of Schedule 3 (Data Protection Addendum) shall apply. The obligations of this clause 12 (Data) shall survive the termination of this Agreement.

12.3. All Parties shall comply with their requirements pursuant to all applicable data protection law, including the Data Protection Act 2018, all amendments and updates thereto and replacements thereof as such requirements arise in connection with this Agreement.

Schedule 1 – Order Form

Administration	
Account Management Contact (Buyer):	Name: E-mail: Address: Phone:
PayPoint Digital Contact:	Name: E-mail: Address: Phone:
PayPoint Digital Contact Billing	Name: E-mail: Address: Phone:
Commencement Date:	As stated in the Agreement
Initial Term:	As stated in the Agreement
Charges	
Set Up Fees (Single Payment - Payable on Signature)	As stated in the Agreement
Service Management Fee (Payable Monthly)	
Transaction Fee (Payable on each Information Request)	
User Licence Fee (For each User – Payable annually).	
Other Charges:	
Users	
Number of Level 1 Users	
Number of Finance Users	
SMS or Security Code Charges	
Special Conditions	
(if applicable)	
Invoicing	
Invoices will be provided by PayPoint Digital's Billing Service Provider. Payment to the Billing Service Provider in respect of an invoice issued will be deemed to be a payment to PayPoint Digital to the value of the funds received.	**The Supplier**

Schedule 2 – Service Description

1. Compliance

1.1. When submitting an Information Request, each party will comply with the Applicable Laws.

1.2. The Buyer will ensure the Customer is aware that an AIS will be requested as part of the process for obtaining the Information Request.

2. Process

2.1. PayPoint Digital will ensure the Service Provider shall provide the AIS (E) during Service Operating Hours.

2.2. To use the Financial Information Service;

2.2.1. The User will log on to the Client Portal.

2.2.2. The User will send an Information Request to the Customer that will, subject to the Customer indicating their consent, enable the Customer to request the Service Provider make an AIS Request in relation to the Customer's payment account.

2.2.3. The Buyer will ensure the Customer is aware that in making the AIS Request a Credit Reference will be obtained in relation to the Customer.

2.2.4. The Customer's consent to the AIS Request will be managed by the Service Provider.

2.2.5. The Service Provider will obtain the information in relation to the Customer's payment account via the AIS Request and provide Financial Information in the form of a Report.

2.2.6. In the event of a Data Subject Access Request, the Service Provider will provide the Customer with access to the Report in a secure location.

2.2.7. The User can access the Client Portal to view the Report and if required, download a copy.

2.2.8. The image of the Report, obtained for each request, can be accessed for up to 3 months. This image will show all the information surfaced in terms of the AIS Enquiry at the time that it was made, and the information in the image will not be refreshed with contemporary data when it is viewed in the future.

2.3. PayPoint Digital will not have access to the Report and is not responsible for the content of the Report.

3. Fraud and Crime

3.1. PayPoint Digital will permit the Buyer to submit an Information Request, except when based on information provided by the Service Provider. PayPoint Digital has reasonable concerns on the validity of the Information Request.

3.2. PayPoint Digital may monitor where the Buyer is making multiple Information Requests to assess if the behaviour is an indication of fraud or wrongful activity.

3.3. PayPoint Digital is entitled to instruct the Service Provider to suspend, terminate and/or restrict the service if PayPoint Digital has concerns in relation to the Buyer's use of the AIS (E) and/or if the regulatory status of the Service Provider is changed.

Supplier Data Processing Agreement/Data Processing Term

Schedule 3 - DATA PROTECTION ADDENDUM

Controller to Controller Data Sharing

Overview

When providing the AIS (E) or using the AIS (E) a party shares Personal Data with the other or otherwise Processes such Personal Data under the Agreement(s).

Where the Customer of the Buyer requests the Service Provider to provide Financial Information derived from the Account Information Service to the Buyer, the exchange of any personal data is on the basis of Controller (Service Provider) to Controller (Buyer) and is with the consent of the Customer of the Buyer.

PayPoint Digital does not have access to the Financial Information or Account Information Service.

1. Definitions

1.1. For the purpose of this Addendum the following additional definitions will apply;

Account Information Service	A request made by the Customer to enable account information to be accessed by Aperidata Limited for the purpose of providing the Financial Information to the Buyer.
Agreement(s)	The G-Cloud 15 Call Off Contract between the Supplier and the Buyer for payment services and/or technology services.
Controller	shall have the meaning given in the Data Protection Legislation.
Customer	Means the Data Subject who is subject of the Information Request.
Customer Data	Means data identifying the individual provided by the Buyer.
Data Protection Legislation	Data Protection Legislation means: the Data Protection Act 2018 and UK General Data Protection Regulation **("UK GDPR")** and any regulations and secondary legislation, as amended or updated from time to time, in the UK and (ii) any successor legislation. In each case interpreted in accordance with the DP Guidance.
Data Subject	shall have the meaning given in the Data Protection Legislation;
DP Guidance	means any and all guidelines, recommendations, best practice, opinions, directions, codes of practice and codes of conduct issued, adopted, recommended or approved the UK's Information Commissioner's Office and/or any other supervisory authority or data protection authority from time to time (whether or not legally binding) in relation to the processing of personal data, data privacy, electronic communications, marketing and/or data security.
Personal Data	shall have the meaning given in the Data Protection Legislation.
Personal Data Breach	shall have the meaning given in the Data Protection Legislation.
Processor	shall have the meaning given in the Data Protection Legislation.
Processing	**Processing**" shall have the meaning given in the Data Protection Legislation, and "**Process**" and "**Processed**" shall be construed accordingly

Representative	means employees, staff, (excluding third parties providing industry services) sub-contractors and invitees of the Controller engaged or due to be engaged in the provision of the Services or required to carry out obligations of the Controller under this Agreement.
Services	The services as the same are more fully described in the Agreement(s).
Shared Data	The personal data exchanged between the parties to enable a Information Request to be made and the AIS (E) provided.
Technical Standards	The industry standards applied to the Service.

2. Data Sharing

2.1. The basis of the processing is independent Controller (Service Provider) to independent Controller (Buyer).

2.2. The Buyer based on consent will provide the Customer with the link to the Service Provider's Account Information Service generated from the Buyer Portal.

2.3. The Customer will respond to the Service Provider and the response shall be retained by the Service Provider.

2.4. The Service Provider with the consent of the Customer will make the AIS Service Request.

2.5. The Service Provider will process the information obtained from the AIS Service Request to create the Financial Information.

2.6. The Service Provider will provide the Financial Information to the Buyer with the consent of the Customer via the Buyer Portal.

2.7. The Shared Data to be shared between the parties shall be no more than is necessary in the particular circumstances.

2.8. The parties agree the Shared Data may only be used for the purpose specified in this clause 2 (Data Sharing).

3. Warranties

3.1. The party disclosing the Shared Data warrants that:

3.1.1. it has no reason to believe that it is prohibited from sharing, or that the other party is prohibited from receiving, the Shared Data in accordance with this Agreement.

3.1.2. at the time of sharing the Shared Data is accurate and up to date to the best of its knowledge; and

3.1.3. it will at all times ensure that it (and any sub-contractor) has obtained the Shared Data in accordance with Data Protection Legislation and has provided all necessary notices to Data Subjects and has procured all necessary consents, or satisfied another legal basis, to disclose the Shared Data to the party receiving it and for the party receiving the Shared Data to Process the Shared Data in compliance with Data Protection Legislation.

3.2. The party receiving the Shared Data warrants that:

3.2.1. it has no reason to believe that it is prohibited from receiving, or that the other party is prohibited from sharing, the Shared Data in accordance with this Agreement.

3.2.2. it shall not process the Shared Data for any purposes other than those set out in Clause 2 (Data Sharing).

4. Obligations

4.1. Each party is responsible for the accuracy of the Shared Data, providing always that:

4.1.1. The Customer has provided the correct details to the Buyer to give the consent; and

4.1.2. The Customer has provided the correct account details to the Service Provider to make the AIS Request; and

4.1.3. The responding bank or institution has provided the correct response to the AIS Request.

4.2. The parties shall apply appropriate security mechanisms and Technical Standards to the Shared Data to ensure its security in transit.

4.3. The parties agree to provide such reasonable assistance as is necessary to each other to enable them to comply with any Data Subject Request made.

4.4. Each party shall comply with the requirements of the Data Protection Legislation in respect of the activities involving Shared Data which are the subject of the Agreement and shall not knowingly do anything or permit anything to be done in respect of or in connection with the Data which might lead to or cause a breach by the other party of the Data Protection Legislation.

4.5. Each party shall ensure that.

4.5.1. any sub-contract it enters into in connection with the Agreement contains terms equivalent to those set out in this Addendum and contain obligations to comply with the data protection obligations contained herein. The sub-contracting party remains fully liable to the other party for any acts or omissions of any subcontractors.

4.5.2. access to the Shared Data is limited to:

(i) those Representatives who need access to the Data to meet the Controller's obligations under the Agreement; and

(ii) such part or parts of the Shared Data and to the extent and manner as is strictly necessary for performance of that Representative's duties.

4.6. Each party will ensure it has in place.

4.6.1. processes and procedures to ensure that the Representatives comply with appropriate procedures and guidelines in relation to the processing of Shared Data, and ensure that all the Representatives who have access to the Shared Data are aware of and have undertaken training in applicable Laws relating to handling such Shared Data (including the Data Protection Legislation); and are subject (by way of written agreement) to a duty of confidentiality;

4.6.2. technical and organisational security arrangements, for the processing of Personal Data and procedures for keeping the Personal Data safe from unauthorised disclosure or accidental deletion.

4.6.3. measures and procedure to respond to a Data Subject Access request.

4.6.4. measures and procedures to deal with a Data Breach including processes compliant with the requirements of the Data Protection Legislation.

4.6.5. data storage and retention policies and procedures consistent with and appropriate to the Data Protection Legislation.

4.6.6. If a party has its data compromised, the compromised party shall promptly inform the other party of any such breach such notification without undue delay and in any case within 36 hours from the event.

4.7. Save to the extent required for legal, regulatory or compliance purposes each party will cease to use the Shared Data upon termination of the Agreement.

5. Processing Activities

5.1. The processing activities are as described more fully in Data Protection clause 2 (Data Sharing) and clause 7 (Data Sharing Description) for the exchange of data between the Controller (Buyer) and the Controller (Service Provider).

6. Categories of Personal Data and Purpose.

6.1. The Personal Data may subject to the explicit consent of the Customer may include Special Categories of Personal Data.

6.2. The purpose for which the Personal Data is provided is the Services as specified in the Agreement.

6.3. The duration of the processing will be the duration of the Agreement or such other period as the parties may agree in writing.

6.4. Either party may from time to time notify the other if this clause 6 (Categorise of Personal Data and Purpose) needs to be amended to reflect any changes made (or proposed to be made) to the processing of Personal Data under the Agreement, in which case both parties will act reasonably and in good faith in agreeing appropriate amendments so that description of the Personal Data remains accurate and complete.

General

7. Data Sharing Description

Description	**Details**
Subject matter of the Data Sharing	Provision of the following to the extent specified in the product description for the Financial Information Services under the Agreement(s): • Customer Financial Information from Controller to Controller. • Client User information (when using the Client Portal). • Access to the Customer's bank account subject to the AIS consents for the purpose of collecting data used to produce the Report.
Duration of the Data Sharing	Term of the Agreement.
Nature and purpose of Data Sharing	• To enable the Buyer to verify income and outgoings of its customers consenting to the Service Provider to share their Financial Information for the purposes of [tariff review]. • Storage • Processing • User log on, email and IP location in relation to Information Request generation or accessing Reports via a portal.
Categories of Personal Data	Personal Data. Special Categories of Personal Data is not requested but may be disclosed by the Customer in relation to transactions appearing in the AIS Request.
Categories of Data Subject	• Customers of the Buyer (if provided by the Buyer to the Service Provider) • Employee and Contractors (Buyer, Service Provider and PayPoint Digital)
Frequency of Data Sharing	As and when a customer consents to participating in the Data Sharing to evidence their income and outgoings for their [tariff review]
Lawful basis for Data Sharing	• Customer – Explicit Consent

	• User – Legitimate Interests
Plans for return or destruction of Personal Data	Each Controller to apply their own standards. and as required to comply with legal and/or regulatory obligations shall be retained for compliance purposes.
Permitted Transfers	To the extent required to perform the Financial Information Services as specified in the Agreement(s) or associated with the Agreement including but not limited to: • Financial Conduct Authority. • HMRC and other Tax Authorities. • Police and Investigatory Bodies. • Regulatory bodies and authorities including government and quasi government organisations. • Payment service providers and/or organisation acting as technical service provider under the Payment Service Regulations 2017. • Regulated telecommunication service providers. • Open Banking Operator. • Pay.UK • Information Commissioner's Office. • Auditors • Sub-processor(s) (if applicable).
Non EEA Transfers (PayPoint Digital)	None Details of PayPoint Digital non EEA processing is available by e-mailing privacy@paypoint.com .
Processing Instructions and Technical Standards	The Service Provider shall comply with any standards applied by the OBIE and/or Pay.UK.
Personal Data Fields	May include any of the following: • Name: • E-mail Address; • Phone or contact details: • Bank account or payment account details. • Financial Information relating to the Customer provided in relation to the Customer's AIS requests. • Such other data as specified in Annex 1 Schedule 4. Please note, not all the above will include Personal Data being data that can identify a living individual when in the possession of the Controller. Personal Data will only be provided to the extent required to provide or receive Services under the Agreement.
Sub-processors	None the Service Provider is a data controller.

8. Data Protection Officer

8.1. The contact details for the PayPoint Digital Data Protection Officer are:

Data Protection Officer
PayPoint Digital Group
1 The Boulevard,
Shire Park,
Welwyn Garden City,
Hertfordshire,
AL7 1EL

E-mail: privacy@paypoint.com

Service Provider - Aperidata DPO.

Name: Andrew Bonsall

E-mail: Andrew.bonsall@aperidata.com

The details of the Buyer Data Protection Officer (if any) will be notified by the Buyer to PayPoint Digital no later than 28 days after the date of this Agreement, by e-mailing privacy@paypoint.com.

9. Compliance

9.1. The parties acknowledge that for compliance purposes the Service Provider must be a signatory to Schedule 3 (Data Protection) and agree to adhere to the requirements for data sharing as stated herein.

9.2. Each party agrees that all and/or any claims under this Schedule 3 (Data Protection) if arising shall be made:

a. By the Buyer against the Supplier for a breach by the Service Provider, or
b. By the Supplier against the Buyer for a breach by the Buyer.

And the limitation of liability provision as specified in clause 13.2 (Limitation of Liability) shall apply.

Schedule 4 – Integration and Operation

1. Integration and Operations

1.1. The integration will be in accordance with the documentation provided as part of the developer integration.

1.2. The operation of the Service including the use of Bulk Submission, an API and/or any other submission methods will be as specified in the Operating Instructions.

1.3. For the propose of this Schedule 4 (Integration and Operation), Operating Instructions shall available on the website as notified by PayPoint Digital to the Buyer from time to time.

1.4. The Reports will be viable to the Buyer via the on screen and/or portal access to which will be supported by PayPoint Digital.

2. Report Content

2.1. The Report will consist of the following information:

Data	**Comments**
Customer Account ID/PAN	Applicant consent request generation
Customer First Name & Surname	Applicant consent request generation
Customer Email Address	Applicant consent request generation - Optional
Customer Mobile Number	Applicant consent request generation
The following additional data is provided by Aperidata Applicant Account API:	
Bank Account Name(s)	AIS Account Data
Bank Account Number(s)	AIS Account Data
Bank Account Sort Code(s)	AIS Account Data
Bank Account Balance(s)	AIS Account Data
The following additional data is provided by Aperidata Applicant Credit Analysis Summary API:	
Approved Overdraft Limit	
Overdraft % Utilised	
Recipient of Benefits	Based on receiving any benefits including Universal Credit and Child benefit, as examples
Income	Average Income of 3 months
Committed Spend	
Necessary Expenditure	
Available Residual Balance	
Affordability	Trend analysis to state: Better/Same/Worsening

Annex 1 – Data Fields

[to be added]

Schedule 5 – Supplier Service Levels

1. Definitions

1.1. In this Schedule, unless the context otherwise requires, the following words shall have the following meanings:

AD System	Aperidata System
Agreement	Agreement for the provision of access to and use of the Services.
Authorised User	The individuals who are authorised or permitted to access and use the Console and Documentation by or on behalf of a Buyer.
Availability	The Service availability shall be [99.9%].
Buyer	As specified in the Agreement.
Client Environment	The environment which the Buyer or Authorised Users use with or to access and use the Product, including any and all information technology communication links required by the Buyer to facilitate the Buyer's and Authorised Users' access to and use of the Product and Service Provider Services.
Console	The Client Portal used by the Buyer to access the Services
Documentation	The electronic operating and instructions for the AD API as made available and updated by the Service Provider from time to time
Environment	The hosting environment procured by the Service Provider a from time to time to host the Product and AD System, being an environment within Amazon Web Services cloud facility
Incidents	A failure of the Product to operate substantially in accordance with the Documentation
Product	The method used to access the AD System being either the AD API or the Console, the details of which are set out in Agreement.
Services	The services provided by Service Provider via the Product and AD System which interrogates and analyses a specific Customer's Financial Information further to the consented account call for that Customer and where one is generated, transfers the AD Report in respect of that Customer either via the AD API or to the Console
Support	The support services provided by the Service Provider a as more particularly set out in this Schedule.
Working Day	Any day other than a Saturday, Sunday or public holiday in England when the clearing banks in the City of London are open for business.
Working Hours	The period from 09:00 to 17:00 GMT on any Working Day

2. Support Requests and Scope of Support

2.1. The Buyer must have used all reasonable endeavours to attempt to resolve problems and Incidents and if the issue cannot be resolved and the Buyer determines that the issue is one that relates to the Product or AD System and requires the attention of Service Provider's support team then log a support ticket with Service Provider by emailing support@aperidata.com (the Support Email Address).

2.2. Support will be made available during Working Hours and Service Provider shall all reasonable endeavours to provide second line technical support to Authorised Users in accordance with the service levels set out in the table below.

2.3. Service Provider use all reasonable endeavours to:

a) carry out planned maintenance during the maintenance window 22:00 to 2:00 GMT.

b) carry out unscheduled maintenance outside of Working Hours and give at least 6 Working Hours' notice in advance of such unscheduled maintenance; and

c) provide technical support for Incidents in accordance with paragraph 3 below; and

2.4. Support does not include Service Provider dealing with any failure of the Product or AD System to operate in accordance with the Documentation which arises from, as a result of or in connection with or maintenance of any equipment not belonging to Service Provider, including any Client Portal or the Client Environment.

2.5. Maintenance of the Environment, which will be provided at such times and intervals as are determined by the provider of these facilities and the Buyer acknowledges that Service Provider has no control over this.

a) any misuse, incorrect use of (i.e. use for a purpose for which it was not designed) the Product from whatever cause (other than any act or omission by Service Provider).

b) use of the Product in combination with any equipment, software or services not approved by Service Provider.

c) a breach of the Buyer's obligations under its the Agreement howsoever arising; or

d) the Buyer's failure to implement recommendations and/or requirements in respect of solutions to Incidents or upgrades to the Client Environment previously advised by Service Provider (as applicable).

(each a Service Exclusion)

3. Support Arrangements

3.1. Support outside of Working Hours or required in respect of any Service Exclusions is an additional service.

3.2. If the Buyer requires Service Provider to carry out such additional services, Service Provider shall not be obliged to provide the same until Service Provider's costs have been agreed and the Buyer has entered into such further documentation (as required by Service Provider) for the provision of such additional services.

4. Support Priorities for Incidents

4.1. Service Provider shall determine the priority of an Incident in accordance with the table set out in paragraph 4.2.

4.2. Service Provider shall provide the relevant response to the Incident in accordance and as required by the Service Availability, priority level, response and response times set out in the table below:

Priority level	Definition	Response and Response Time
P1	**Critical Incident:** A catastrophic error in, or failure of, the Product that causes a complete inability of the Product to operate.	**Initial Response** Acknowledge the Incident reported and confirm the Incident is a P1 priority level. **Initial Response Time** Within 2 Working Hours or if reported after Working Hours within 2 Working Hours the following Working Day following the report of the Incident to the Support Email Address. **Resolution Response** a. Restoration of the Product to a state that allows the Buyer to continue to use the Product in all material respects; or a. Resolution by way of a workaround reasonably acceptable to the Buyer further to which the priority level shall reduce to a priority level P2 or P3. **Resolution Response Time** 8 (eight) Working Hours following the report of the Incident to the Support Email Address. **Further Response** Continue to work on the Incident in accordance with the lower priority level the Incident has been downgraded to.

P2	**Significant Incident:** An error in, or failure of, the Product that has a significant business impact being the Product is usable, but severely restricted.	**Initial Response** Acknowledge the Incident reported and confirm the Incident is a P2 priority level. **Initial Response Time** 1 (one) Working Day following the report of the Incident to the Support Email Address. **Resolution Response** a. Restoration of the Product to a state that allows the Buyer to continue to use all functions of the Product in all material respects; or b. Resolution by way of a workaround reasonably acceptable to the Buyer further to which the priority level shall reduce to a priority level P3. **Resolution Response Time** 30 (thirty) Working Hours following the report of the Incident to the Support Email Address. **Further Response** Continue to work on the Incident in accordance with the lower priority level the Incident has been downgraded to.
P3	***Minor Incident:*** *An isolated or minor error in the Product that:* ***a.*** *does not significantly affect the Product functionality.* ***a.*** *may disable only certain non-essential functions; or* ***b.*** *does not materially impact the Buyer's business.*	**Initial Response** Acknowledge the Incident reported. **Initial Response Time** 1 (one) Working Day following the report of the Incident to the Support Email Address. **Resolution Response** Provide a patch or fix as a new release. **Resolution Response Time** At such time as Service Provider rolls out updates to the Product. The next update cycle to be within 30 days of the event..

5. Escalation

5.1. Out-of-hours support is provided based on incident severity, with critical (P1 and P2) issues triggering escalation via the Business-as-Usual (BAU) relationship management channel.

5.2. All issues raised will receive a timely initial response from our support team.

5.3. For high-severity issues, additional communication will be provided by the named relationship manager to ensure resolution is handled with the necessary urgency and visibility.

5.4. All operational and security incidents detected will be immediately escalated to Aperidata's CPO (Ally Dinsdale).

5.5. The CPO will then escalate the issue to the Aperidata senior management team.

5.6. Due to the nature of some of the monitoring controls in place (e.g. AWS CloudWatch security alerts are sent to the CEO (Steve Ashworth) and CPO, some incidents may be raised directly with some members of the senior management team, Commercial Director (Nicola Dunn).

5.7. The details of the individuals named in this paragraph 5 (Escalation) may be amended by e-mail to the Buyer's contacts.