EU Data Protection Addendum

This Data Protection Addendum ("**Addendum**") to the 365 Retail Markets Terms and Conditions (the "**Terms**") is entered between **365 Retail Markets, LLC** ("**365**") and the customer accepting the Terms ("**Customer**") together referred to as the "Parties" and each, individually, as a "Party", each of whom agrees to be bound by and comply with all terms and conditions contained in this Addendum, in addition to the terms of the Terms.

By accepting this Addendum the Parties hereby agree to enter into the Data Protection Agreement set forth in **Annex 1** to this Addendum (the "**DPA**").

This Addendum is issued subject to all terms and conditions of the Terms and capitalized terms which are used but not defined in this Addendum or in the DPA shall have the respective meanings ascribed to them in the Terms.

If the terms of this Addendum (including the DPA) contradict, conflict or are inconsistent with the terms of the Terms, the terms of this Addendum will prevail.

Annex 1

Data Processing Agreement ("DPA")

In performing its obligations under the Terms, **365** processes Personal Data in the name and behalf of Customer.

Within this framework, Customer acknowledges to act as Controller, and 365 acknowledges to act as Processor within the meaning of Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of personal data and the free movement of such data (General Data Protection Regulation) (the "**GDPR**").

The GDPR requires that Processors and Controllers enter into an agreement setting forth their rights and obligations in connection with the Processing of Personal Data.

In order to comply with the GDPR, the Parties have agreed to sign this DPA which includes the attached schedules. This DPA is entered into by Customer and 365 as of the date of the Addendum or at the date of the first Processing of Personal Data under the Terms, whichever is sooner. The DPA will apply in full force and effect until expiry or termination of the Terms.

This being reminded, the Parties have agreed as follows:

1. Definitions

Notwithstanding any contrary definitions in the Terms, capitalized terms used in the DPA whether in singular or in plural, shall have the following meanings in the context of this DPA:

Applicable Data Protection Law: means Data Privacy Laws applicable to the respective Parties as Controller and Processor of the Data.
Authorized Employees: means employees of 365 who have a need to know or otherwise access Customer Personal Data to enable the performance of the Terms.
Authorized Persons: means (i) Authorized Employees; and (ii) Sub-processor who have a need to know or otherwise access Customer Personal Data to enable the performance of the Terms.

Breach of Security: means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Customer Personal Data transmitted, stored or otherwise processed by the Data Processor or its subsequent Sub-processor.
Business Days: means any day other than Saturday or Sunday or a day which is an official legal holiday or on which financial institutions are authorized to close in France.
Customer Personal Data: means the Personal Data that 365 has access to or received from Customer while providing the Services.
Data Center: means the premises of a Hosting Entity rented by an entity of the 365 Group where the HSM is installed.
Data Privacy Laws: means all applicable laws, rules, regulations, governmental requirements, codes as well as international, federal, state, provincial and local laws which govern the use of Personal Data relating to a Data Subject residing in the European Economic Area (EEA), the United Kingdom and Switzerland, including the laws of the European Union ("EU"), the GDPR, the directive 2002/58/CE as amended or replaced from time to time, and any successor or replacement thereto as well as any applicable EU or Member State law relating to data protection or the privacy of individuals.
EU Model Contract: means the standard contractual clauses approved by the EU Commission for the transfer of Personal Data from Controller in the EU to Controller or Processor established in countries outside the EU or the EEA which do not ensure an adequate level of data protection.
Hosting Entity: means a legal entity, that is not party to the Terms, and that has entered into an outsourcing agreement with System Administrator to host the Solution.
Legal Process: means a data, including Personal Data, disclosure request made under law, governmental regulation, court order, subpoena, warrant, governmental regulatory or agency request, or other valid legal authority, legal procedure, or similar process.
365: means all entities of the 365 Group as such term is defined in the Terms.
Personal Data: means any information relating to a Data Subject.
Security Policy: means the technical and organizational measures required to be implemented by 365 which is attached as **Schedule 1** of this DPA.
Solution: means the Vault Solution as defined in the Terms. The Solution may be hosted in a Hosting Entity that is not controlled by 365.
Sub-processor: means legal entities engaged by Processor to provide Specific Services.
System Administrator: means 365 who is responsible for the upkeep, configuration, and reliable operation of the Solution.
Services: means the Solution as well as Specific Services provided by 365 as detailed in the Terms.
Specific Services: means, to the extent applicable, outside the scope of tasks of the System Administrator, certain services set forth in the Terms such as (a) the provision of technical support to solve specific reported problems, (b) the provision of aggregate analytic and statistical report.
Third Party Claim: means a demand or assertion by a third party seeking, as a matter of right, monetary damages, or other relief.

The terms "**Controller**", "**Processor**", "**Data subject**", "**Processing**" and "**Supervisory Authority**" have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

Any communication relating to this DPA or resulting from any of the obligations herein shall be sent to the other Party at the following email addresses:

- For 365: support@365smartshop.com

- For Customer: As indicated in the Purchase Order

2. Purpose of the DPA

The purpose of this DPA is to set forth the conditions under which 365 shall carry out the Processing of Customer Personal Data on behalf of Customer, as well as the respective obligations of the Parties.

The Processing of Personal Data carried out by 365 on behalf of Customer is set forth in **Schedule 2** ("**Personal Data Processing Description**").

Both Parties agree that they will provide each other with all useful information to comply with their respective obligations under this DPA.

3. Relationship between the parties

3.1 For the Processing of Customer Personal Data in connection with the Services, Customer is the Data Controller and 365 is the Processor of Customer Personal Data.

3.2 Consequently:

365 will comply with all obligations in connection with the Processing of Customer Personal Data applicable to Processors under Applicable Data Protection Law and under the terms of this DPA.

Customer will at all times comply with Applicable Data Protection Law and the terms of this DPA in connection with the Processing of Customer Personal Data in using the Services. Customer will have sole responsibility for the accuracy, quality and legality of the Customer Personal Data and the means by which the Customer Personal Data is collected and warrants 365 in that respect.

The obligations set forth in this DPA shall not supersede the Parties' respective obligations under Applicable Data Protection Law.

4. Documentation

4.1 **Schedule 2** to this Agreement "**Personal Data Processing Description**" describes:

- the type of Customer Personal Data to be processed by 365;
- the categories of Data Subjects;
- the nature and purposes for which Customer Data is processed; and
- the retention periods of said Customer Personal data.

4.2 365 must be able to reasonably demonstrate the implementation of measures to ensure compliance with the Applicable Data Protection Law.

To that end, 365 may be subject to audits, carried out by Customer or by any third party appointed by Customer, provided such third party is not a competitor of 365 and has duly executed a non-disclosure agreement with Customer, to demonstrate 365's compliance with the obligations laid down in this DPA.

Before the commencement of any such audit, Customer and 365 shall mutually agree upon the scope, timing, and duration of the audit, none of which shall adversely impact 365's business activities.

The audits shall solely be carried out via communication of documents by 365 to Customer: Customer may at any time request 365 to provide reasonably relevant documents relating strictly to its processing of Customer Personal Data. 365 has 30 Business Days from the date it receives Customer's request, notified by registered letter with acknowledgment of receipt, to reply.

Customer shall promptly notify 365 of any non-compliance by 365 discovered during the course of an audit. Such an audit will be limited to once in any twelve month period, except where Customer is able to evidence that an additional audit over this time period has been mandated by a Supervisory Authority.

5. Instructions by Customer

5.1 Customer Personal Data can only be processed by 365 for the purpose of providing the Services under the Terms and this DPA and within the scope of the Customer's written and documented instructions.

5.2 If 365 believes that any use of the Services by Customer, or any of Customer's instructions, is legally prohibited, requires material changes to 365's performance of the Service, creates a material increase in costs for 365 or infringes any Data Privacy Laws and Regulation or is inconsistent with the terms of the DPA or with the Terms, 365 will inform Customer and shall be entitled to suspend or stop the Services until this can be resolved or agreed by discussion between the Parties.

6. Sub-processing

6.1 Customer hereby generally authorizes 365 to engage additional Sub-processors for the provision of the Services. At Customer's written request, 365 must provide Customer in writing, including by email, the list of Sub-processors engaged by 365 ("**Sub-Processor List**"). According to the GDPR, Customer may object to 365's use of a new Sub-processor by notifying 365 in writing within five (5) business days following the receipt of the Sub-Processor List, if Customer can reasonably demonstrate that the use by 365 of the contemplated Sub-processor would create an objective, legitimate and material concern with regard to the security, integrity, confidentiality and/or availability of the Customer Personal Data (a "**Reasonable Objection**"). If 365 does not receive a Reasonable Objection from Customer within five (5) business days of Customer's receipt of the Sub-Processor List, Customer is deemed to have accepted the new Sub-processor. If a Reasonable Objection is received by 365 within this timeframe, the parties will come together in good faith to discuss a resolution. If Customer and 365 are unable to resolve Customer's objection in that good-faith discussion, then 365 may terminate the Terms upon fifteen days' prior written notice to Customer.

6.2 Where the Sub-processor is located in a non-adequate country (a country that is deemed not to provide an adequate level of protection for Personal Data), 365 shall procure that the Sub-processor enters into an EU Model Contract.

6.3 The Sub-processor is obliged to comply with the obligations provided in this DPA. 365 shall execute the appropriate written agreements with Sub-processors in accordance with the provisions of this DPA and the instructions hereto between the Customer and the Provider.

7. Transmission of Personal Data to other countries outside EU

7.1 As indicated in Section 1 above, the Solution is hosted at the Hosted Entity or the Data Center. In the event the use of the Solution by Customer triggers a cross-border transfer of Customer Personal Data outside the EU and toward a country that does not provide an adequate level of data protection, the Customer understands that such cross-border transfer of Customer Personal Data may be subject to

specific requirements imposed by the Applicable Data Privacy Laws with the burden of such specific requirements being carried by the Data Controller.

7.2 In the event such cross-border transfer of Customer Personal Data could require the entering into a specific cross-border transfer agreement in light of the Applicable Data Protection Law, 365 and Customer will collaborate in order to enter into an EU Model Contract directly with the data importer established outside EU or to make it sign any other document or procedure approved by the relevant Supervisory Authorities.

8. Customer Commitments

8.1 Customer represents and warrants that the Customer Personal Data it provides for Processing can be processed lawfully (e.g., lawful collection, compliance with obligation to inform and compliance with the applicable Data Privacy Law).

8.2 Customer shall not, by any of its act or omission, put 365, System Administrator, Sub-processor, Hosting Entity and Data Center in breach of any Data Privacy Laws in connection with the Processing of the Customer Personal Data.

8.3 It is the responsibility of Customer to ensure that the Customer Personal Data processed is accurate, adequate and complete.

8.4 Customer undertakes to provide 365 with the clearest possible instructions regarding the Customer Personal Data Processing activities carried out by 365 on behalf of Customer.

8.5 Customer undertakes to inform the Data Subjects concerned by the Processing operations at the time data are being collected.

9. Security Principles

9.1 In accordance and within the limit of the Security Policy, 365 implements technical and organizational measures to protect Customer Personal Data against Breach of Security. Acting as a Controller and according to the GDPR, Customer is solely responsible for its use of the Services and the Processing of the Customer Personal Data, including its account authentication. 365, System Administrator, Sub-processor, Hosting Entity and Data Center have no obligation to protect Customer Personal Data that Customer elects to store or transfer outside Sub-processor, Hosting Entity and Data Center.

9.2 365 will take all reasonably necessary steps to ensure compliance with the Security Policy by the System Administrator, Sub-processor, Hosting Entity and Data Center, to the extent applicable to their scope of performance.

9.3 (a) If 365 becomes aware of a Breach of Security, it will without undue delay notify Customer of the Breach of Security and take all reasonable and legally required steps to minimize harm to Customer and secure Customer Personal Data. Notification(s) of a Breach of Security will be delivered via the notification contact provided by Customer herein or, at 365's discretion, by direct Customer communication (e.g., by phone call or an in-person meeting). Customer acknowledges that it is solely responsible for ensuring that the contact information set forth above is current and valid, and for fulfilling any third party notification obligations. 365 obligation to report or respond to a Breach of Security under this Section 9.3 will not be construed as an acknowledgement by 365 of any fault or liability with respect to the Breach of Security.

(b) Promptly following 365's notification to Customer of a Breach of Security, Customer and 365 shall coordinate with each other to investigate the Breach of Security. 365 leads the investigation and agrees to reasonably cooperate with Customer in the handling of the Breach of Security, including, without limitation: (i) assisting with any investigation; (ii) facilitating interviews with Authorized Persons; and (iii) making available the relevant records, logs, files, data reporting and other relevant materials, concerning the Customer, required to comply with Applicable Data Protection Law.

9.4 Notwithstanding anything to the contrary in the Terms or the Security Policy, 365, Sub-processor, System Administrator, Hosting Entity and Data Center obligations extend only to those systems, networks, network devices, facilities and components over which they exercise control. The Security Policy does not apply to: (i) Customer Personal Data shared with either of 365, Sub-processor, System Administrator, Hosting Entity and Data Center, that is not stored in the Solution; (ii) Customer Personal Data in Customer's virtual private network (VPN) or a third party network, or (iii) Customer Personal Data processed by Customer or its users in violation of the Terms or the Security Policy.

10. Cooperation regarding requests and inquiries

10.1 365 will promptly inform Customer if 365 has received any complaints, requests or inquiries from Data Subjects related to the Processing of Customer Personal Data, including but not limited to requests to provide access to, correct, amend or delete Customer Personal Data. 365 shall not respond to the Data Subject directly unless specifically instructed by Customer to do so, and where 365 or Sub-processor, Data Center, Hosting Entity, or System Administrator is required by law, or Legal Process, to respond, in which case it shall respond within a reasonable period of time, and in any case as required by the Data Privacy Laws. 365 will cooperate with Customer to address and resolve any such complaints, requests or inquiries.

10.2 365 will deal promptly and appropriately with enquiries of Customer related to the Processing of Personal Data under the Terms. 365 will provide Customer with reasonable cooperation and assistance as needed to fulfil Customer's obligation under the GDPR to carry out a privacy impact assessment related to Customer's use of the Service, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to 365.

11. Confidentiality, Archiving and Destruction of Personal Data

11.1 365 shall not Disclose Customer Personal Data in any way to any third party without the prior written approval of Customer, except where, (i) the disclosure is necessary for the performance of the Terms, or (ii) where, in accordance with Section 10 above, Customer Personal Data needs to be disclosed to a competent public authority to comply with a Legal Process.

11.2 Customer shall notify 365 at least 30 (thirty) days before the end expiration or earlier termination of the Terms for any reason of its intent to have the Customer Personal Data returned to Customer or deleted. In the event Customer requested the deletion of Customer Personal Data, the Personal Data is deleted irretrievably or cease to be retained as Personal Data via the use of strong encryption and associated security measures. The parties agree that 365 may retain one copy of the Customer Personal Data to comply with any of 365's legal, regulatory, judicial, audit or internal compliance requirements.

12. Support Services

12.1 For, in particular, the administrative management of the contractual relationship and/or undertaking obligations to meet contractual, legal or regulatory obligations, as well as for security and business continuity purposes and the provision of Support Services, either party may from time to time process Personal Data (e.g., name, surname, mobile phone number, email address) of the other Party employee or agent. Each Party consents to such Processing.

12.2 In respect with Processing detailed in Section 12.1 above, either Party shall comply with all current Applicable Data Protection Law and shall implement appropriate measures to protect all such Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against other unlawful forms of processing.

12.3 Each respective Data Controller warrants that it has obtained all legally required consents and permissions in respect of such Personal Data. In the event that either party does not comply with this undertaking, it shall indemnify the other Party fully against any damage, loss, cost or liability (including, without limitation, legal fees and the cost of enforcing this indemnity) arising out of breach by a Party of this Section.

13. Indemnification and Liability

13.1 Each Party is liable towards the other Party in respect of all claims related to the Processing of Customer Personal Data under the conditions set forth in the Terms.

13.2 365, Sub-processor, System Administrator, Hosting Entity and Data Center, shall not have in any circumstances any liability to Customer for: any Losses or damages (whether direct or indirect) which may be suffered by Customer which fall within the following categories:

- loss of profits;
- loss of revenue;
- loss of transaction;
- loss of anticipated savings;
- loss of business opportunity;
- loss of goodwill or reputation;
- indirect, consequential or special loss or damages, regardless of the form of action, whether in contract, strict liability or tort (including negligence), and regardless of whether 365, Sub-processor, System Administrator, Hosting Entity and Data Center or Customer knew or had reason to know of the possibility of the loss, injury, or damage in question.

14. Changes

14.1 If 365:

a) determines that it, or a Sub-processor, Data Center, Hosting Entity, or System Administrator, is unable at any time and for any reason to comply with the obligations set forth in this DPA and cannot cure this inability to comply; or

b) becomes aware of any circumstance or change in the Applicable Data Privacy Law, that is likely to have a substantial adverse effect on 365, Sub-processor, Data Center, Hosting Entity, or System Administrator, ability to meet the obligations set forth in this DPA:

365 will promptly notify the Customer thereof, in which case the Customer will have the right to temporarily suspend the Processing of Customer Personal Data until such time the Processing is adjusted in such a

manner that the non-compliance is remedied. If such suspension were to occur and impact the availability of the Solution to Customer, it would not constitute a breach under the Terms and the obligations of the Parties under the Terms shall be suspended until 365 determines that the Processing of Customer Personal Data can resume.

Schedule 1

Security Policy

Preface:

This Schedule sets out the main elements of the 365 Security Policy dedicated to the safeguarding of the data entrusted to 365. 365 remains available to answer further questions from Customers.

Principles:

This Security Policy is meant to ensure that 365 follows the Applicable Data Protection Law in the jurisdictions in which 365 is conducting business.

The purpose of the Security Policy is to:

a) identify, potential threats to Customer information using risk analysis;
b) implementing security solutions (both processes and tools) to limit risks to 365's systems;
c) train 365 employees and third-party service providers to implement the Security Policy;
d) monitor the security of 365 systems and processes;
e) provide clear information on the processing of Customer information;
f) respond to customers queries and request on the protection of their information;
g) increase 365's crisis-readiness.

The following describe in greater details the main principles of the Security Policy protecting Customer information.

365 Security Policy governance is:

- Based on the several policies applicable to 365;
- Under the responsibility of the Security Department;
- Periodically reviewed and its implementation is checked during local and central security audits. Furthermore, technical security audits are undertaken at corporate and local levels. The periodicities of such audits vary depending on various factors such as the security level, sensitivity and vulnerability of the system being audited.

365 Security Policy focuses on the following:

Personal Information Identification and classification:

The purpose of the personal information identification and classification policy is to establish a system of priorities for protecting information and assets, in order to ensure that protection levels are commensurate with the value of the information or system being protected throughout their lifecycle. The use of classification levels allows 365 to focus protection costs on information of the highest value. This policy covers the following main elements:

- Establish 365's corporate rules for the management of information, depending on their sensitivity;
- Determine how confidential and sensitive are certain information with five classification levels from Secret (highest) to Public (lowest);
- Protection of the area where information are physically located is appropriate for each particular information classification level;
- Restricted logical access to computers and networks follow the same rules as physical access restrictions;
- Rules for the transmission of information;
- Rules for physical, electronic and media storage of information;

- Rules for destruction of information.

Physical and Environmental Security Policy:

Setting the primary means of defense against theft or misuse of products and services supplied by 365 are required to protect 365's know-how. This policy covers the protection of 365's personnel as well. This policy also covers the following:

- Applicable to all 365's sites. A site is a physical location where 365's employees are based or where 365's operations are conducted;
- 365 sites must comply with certain minimum security features depending on their activity and the identified risks of their processes;
- 365 sites are subject to regular audit performed by the Security Team to verify compliance with the policy.

Schedule 2

Personal Data Processing Description

This Schedule provides a non-exhaustive description of the service provided by 365 as Data Processor, the types of data to be processed and the purposes for which the data is being processed, and describes the purpose duration, mandatory retention requirements (if any).

Description of the Services:

Vault Services (as such term is defined in the Terms).

Categories of Data Subjects.

The Data Subjects are the Services' users and end-users.

Breakdown of Data:

Categories of data	Processing purposes	Retention periods (including archiving period)
IDENTIFICATION AND CONTACT INFORMATION		
Contact details incl. Email address Postal address Phone number	Billing Client support Shipping Legal	Minimum: 2 years following termination of the Terms Maximum: 10 years following termination of the Terms Unless otherwise required by Applicable Data Protection Laws
LOGS		
Application Logs (record of all activity taking place in the Vault platform (e.g., login, when user A initiated a transaction, user B approved it, etc.)	Debug Performance analytics Billing	Minimum: 2 years following termination of the Terms Maximum: 10 years following termination of the Terms Unless otherwise required by Applicable Data Protection Law
TRANSACTION DATA		
Assets under management	Billing Marketing Performance analytics Legal	Minimum: 2 years following termination of the Terms Maximum: 10 years following termination of the Terms TBD Unless otherwise required by Applicable Data Protection Laws

Transaction data such as: - amount - xpub (send and receive) - timestamps	Debug Performance analytics Billing	Minimum: 2 years following termination of the Terms Maximum: 10 years following termination of the Terms Unless otherwise required by Applicable Data Protection Laws
Transaction records i.e. operations carried out by Customer on the Platform	Debug Performance analytics Billing	Minimum: 2 years following termination of the Terms. Maximum: 10 years following termination of the Terms Unless otherwise required by Applicable Data Protection Law

Location of Customer Personal Data:

- _____