PERSONAL DATA PROCESSING AGREEMENT

Preamble

As the Provider is required to process Personal Data within the framework of its contractual relationship with the client, the Parties wish to specify their rights and obligations. Within the framework of this agreement, the Provider shall hereinafter be referred to as the "Processor".

1. Definitions

In this Agreement, words or expressions starting with a capital letter shall have the following meaning:

- "Agreement": refers to this personal data processing agreement which specifies the rights and obligations of the Parties regarding the processing of personal data.
- "Contract": refers to the Framework Contract and the Application Contracts concluded with the Provider within the framework of which this Agreement is established.
- "Personal Data or PD": refers to any information relating to an identified or identifiable natural person (hereinafter "Data Subject"), directly or indirectly, in particular by reference to an identification number, location data, online identifiers (for example, username and password) or to one or more factors specific to their physical, physiological, mental, economic, cultural, or social identity.

- "Data Subject": refers to the natural person whose PD is the subject of Processing;

- "Data Controller": refers to the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of

the processing. In the context of the Contract and this Agreement, the Data Controller is the Customer.

- "Processor": refers to the natural or legal person, public authority, agency, or other body which processes PD on behalf of the Data Controller and in accordance with its instructions. In the context of the Contract and this Agreement, the processor is the Provider.
- "Regulations": refers to all laws and regulations applicable in the European Union regarding PD, including the French Data Protection Act No. 78-17 of January 6, 1978, as amended, and the General Data Protection Regulation (GDPR) 2016/679 dated April 27, 2016, from its entry into force (hereinafter the "GDPR").
- "Processing": refers to any operation or set of operations performed or not performed using automated processes and applied to Personal Data or sets of Personal Data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The terms and expressions "PD Breach," "Process," "Data Subject," "Member State," "Supervisory Authority," and "Standard Clauses" have the same meaning as given to them in the Regulations, and related expressions must be interpreted in the same manner.

2. Obligations of the Customer

The Customer agrees to respect the obligations incumbent upon it as Data Controller under the Regulations.

The Customer acknowledges that the Processor is limited to following the Customer's instructions, subject to informing the Customer in case of instructions given that are not compliant with the Regulations.

The Customer shall maintain a record of all processing operations it carries out as a Data Controller. This record contains at least the mandatory information required by the Regulations.

3. Obligations of the Processor

3.1 General Obligations

The Processor agrees to comply with the Regulations within the framework of the Contract. It specifically undertakes, without this list being exhaustive, to:

- Process the Customer's PD only on instructions from the Customer in order to provide the services and fulfill its obligations under the Contract. It is specified here that the description of the PD processing entrusted to the Processor appears in each Application Contract according to the model appearing in Appendix A of this Agreement. The Appendix may be subject to modifications by the Customer. Any modification to Appendix A will be communicated in writing to the Processor. In the event that the Processor is required to proceed with a processing of Personal Data by virtue of a mandatory provision resulting from Union law or the law of the Member State to which it is subject, the Processor will inform the Customer of this legal obligation before the processing of the Data, unless the relevant law prohibits such information for important reasons of public interest.

- Refrain from acting in a way that would constitute or lead to a violation of the Regulations by the Customer and alert the Customer without delay in the event of detection by the Processor of a compliance issue or a risk of non-compliance;

- Guarantee and indemnify the Customer in the event of action, claim, or demand from any third party resulting from its breach or failure with regard to the Regulations within the framework of this Contract;

- Maintain a record of all categories of processing activities carried out on behalf of the Customer. This record contains at least the mandatory information required by the Regulations, notably:

(i) the name and contact details of the Data Controller on whose behalf it acts, any Sub-processors and, where applicable, the data protection officer;

(ii) the categories of processing carried out on behalf of the Data Controller;

(iii) where applicable, transfers of Personal Data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in Article 49, paragraph 1, second subparagraph of the Regulation, documents certifying the existence of appropriate safeguards;

(iv) as far as possible, a general description of technical and organizational security measures, including, among others, as needed :

- pseudonymization and encryption of Personal Data;
- means ensuring the constant confidentiality, integrity, availability, and resilience of processing systems and services;
- means allowing the restoration of availability of Personal Data and access to them within appropriate timeframes in the event of a physical or technical incident;

- a procedure for regularly testing, analyzing, and evaluating the effectiveness of technical and organizational measures to ensure the security of processing.

The Processor makes this record available to any supervisory authority that requests it and to the Customer upon first request.

The Processor also guarantees:

- to implement sufficient human, technical, and organizational resources to operate the processing in compliance with the Regulations, such as, and without this list being exhaustive: training its personnel, appointing a DPO, where applicable, applying the principles of privacy by design and by default, etc.
- to guarantee the confidentiality of Personal Data processed within the framework of the Contract.
- to ensure that persons authorized to process Personal Data under the Contract:
  - commit to respecting confidentiality or are subject to an appropriate legal obligation of confidentiality;
  - receive the necessary training in Personal Data protection.

3.2 Cooperation and Assistance Obligations

The Processor assists the Customer and actively cooperates with the Customer to enable it to ensure the compliance of the Processing with the Regulations, particularly regarding requests for exercising data subjects' rights. The Processor specifically undertakes to comply with the following provisions.

✔ **Right to be informed**

It is up to the Customer to provide information to the data subjects at the time of PD collection or, at the Customer's choice, to ask the Processor, at the time of PD collection, to provide information relating to the PD processing it carries out to the data subjects. In the latter case, the wording and format of the information will be agreed upon by the Customer before any PD collection.

✔ **Exercise of individuals' rights**

As far as possible, the Processor must help the Customer fulfill its obligation to respond to requests for exercising data subjects' rights under the PD protection Regulations, namely mainly: right of access, rectification, erasure and objection, right to restriction of processing, right to PD portability, right not to be subject to an automated individual decision (including profiling).

When data subjects exercise requests for their rights with the Processor, the Processor must send these requests upon receipt by email to the person designated by the Customer in

Appendix A or communicated by any other means at the Customer's choice. The Processor may only respond directly to a data subject's request upon instruction from the Customer.

✔ Notification of Personal Data breaches

A Personal Data breach means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of PD transmitted, stored, or otherwise processed, or unauthorized access to such PD.

In the event of a Personal Data breach, the Processor undertakes to proceed with all useful investigations into breaches of protection rules in order to remedy them as soon as possible and to reduce the impact of such breaches on the data subjects.

The Processor notifies the Customer of any Personal Data breach within 24 hours after becoming aware of it. This notification is accompanied by all useful documentation to allow the Customer, if necessary, to notify this breach to the competent supervisory authority. On this point, the Processor is informed that in case of notification of a Personal Data breach by the Customer to the competent supervisory authority, the notification must contain at least:

(i) a description of the nature of the Personal Data breach, including, if possible, the categories and approximate number of data subjects affected by the breach and the categories and approximate number of Personal Data records concerned; the name and contact details of the data protection officer or another contact point from whom additional information can be obtained;
(ii) a description of the likely consequences of the Personal Data breach;
(iii) a description of the measures taken or that the Data Controller proposes to take to remedy the Personal Data breach, including, where applicable, measures to mitigate its possible negative consequences.

If, and to the extent that it is impossible to provide all this information simultaneously, the information may be provided in stages without undue delay. In any case, the Processor undertakes to inform the Customer of its investigations into the breaches of protection rules that led to the Personal Data breach, the evolution of the nature and consequences of the breach, as well as the measures taken or envisaged to reduce the impact of the identified breaches, on a regular basis.

The Processor undertakes to collaborate actively with the Customer so that they are able to meet their regulatory and contractual obligations. Only the Customer can notify the Personal Data breach to the competent supervisory authority and communicate information on this

breach to the data subjects; the Processor consequently refrains from proceeding with such notification and communication.

- ✔ **Processor's assistance with the impact assessment**

The Processor assists the Customer in carrying out data protection impact assessments that the Customer decides to perform.

The Processor assists the Customer within the framework of the prior consultation with the supervisory authority, following the completion of impact assessments.

- ✔ **Processor's assistance within the framework of Customer's compliance with its accountability obligation**

The Processor provides the Customer, upon first request, with the documents and information necessary to demonstrate compliance with all its obligations under this Agreement. In the event of an audit by a competent authority, the Parties undertake to cooperate with each other and with the supervisory authority.

In the event that the audit conducted only concerns the processing implemented by the Processor as a data controller, the Processor will handle the audit and refrain from communicating or disclosing the Customer's Personal Data.

In the event that the audit conducted at the Processor's concerns the processing implemented in the name and on behalf of the Customer, the Processor undertakes to inform the Customer immediately and to make no commitment for it.

In the event of an audit by a competent authority at the Customer's specifically concerning the services delivered by the Processor, the latter undertakes to cooperate with the Customer and provide it with any information it might need or that proves necessary.

4. <u>Security and Confidentiality Obligations</u>

The Processor implements the security and confidentiality measures necessary for the compliance of the Processing with the Regulations.

Without prejudice to the provisions of the body of the Contract, the Processor implements all appropriate technical and organizational measures to protect Personal Data, considering the state of knowledge, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risks, the degree of probability and severity of which vary, for the

rights and freedoms of natural persons, in order to guarantee a level of security adapted to the risk.

The Processor thus undertakes, in particular, to take all appropriate precautions regarding the nature of the Data and the risks presented by the Processing, to preserve the security of the Data and files and notably prevent any distortion, alteration, damage, accidental or unlawful destruction, loss, disclosure and/or any access by unauthorized third parties.

In particular, the Processor undertakes to ensure total segregation between the Data Controller's Data and the data of other Processor's clients, through physical and logical separation.

The means implemented by the Processor intended to ensure the security and confidentiality of the Data notably include the following measures:

- pseudonymization and encryption of PD,
- means ensuring the constant confidentiality, integrity, availability, and resilience of processing systems and services,
- means allowing the restoration of access and availability of PD within appropriate timeframes in the event of a physical or technical incident,
- a procedure for regularly testing, analyzing, and evaluating the effectiveness of technical and organizational measures to ensure the security of processing.

The Processor undertakes to maintain these means throughout the execution of the Contract and, failing that, to inform the Customer immediately.

In any case, the Processor undertakes in the event of a change in the means aimed at ensuring the security and confidentiality of PD and files, to replace them with means of superior performance. No evolution may lead to a regression in the level of security.

5. Sub-contracting

The Processor may call upon another sub-contractor (hereinafter, "the Sub-processor") to carry out specific processing activities. In this case, it informs the Customer in advance and in writing of any planned change regarding the addition or replacement of other Sub-processors. This information must explicitly indicate the sub-contracted processing activities, the identity and contact details of the Sub-processor, the dates of the sub-contracting contract, and the possible existence of PD flows outside the European Union or to an international organization. The Customer has a maximum period of two calendar months from the date of receipt of this information to present its objections. This sub-contracting may only be carried out if the Customer has not issued an objection during this period.

The Sub-processor is required to respect the obligations of the Contract, and to process Personal Data only on behalf of and according to the Customer's instructions. Consequently, the initial Processor undertakes to sign a written contract with its Sub-processor referring to the

Contract, and imposing on the Sub-processor the same obligations in terms of PD protection as those set in the Contract.

It is up to the initial Processor to ensure, notably through this written contract, that the Sub-processor presents the same sufficient guarantees regarding the implementation of appropriate technical and organizational measures so that the processing meets the requirements of the Regulation.

If the Sub-processor does not fulfill its obligations in terms of PD protection, the initial Processor remains fully responsible to the Data Controller for the execution by the Sub-processor of its obligations, notably concerning the notification of Personal Data breaches.

6. Return or Deletion of Personal Data

At the end of the Contract, the Processor must, at the Customer's choice, either return all processed Personal Data or delete it and certify in writing to the Customer that the deletion has been carried out, subject to and within the limit of legal and regulatory storage obligations imposed on the Processor.

At the end of the provision of services relating to the processing of Data, the Processor undertakes to:

- return all Personal Data and files to the Customer in an exploitable format and under the conditions specified by the Customer or
- send the Personal Data to the processor designated by the Customer, and then
- destroy all PD and manual or computerized files containing the information collected within a period of two (2) months after the return, in order to allow the Customer to have the necessary time to verify that the returned Data are exploitable and readable, unless a contrary mandatory provision resulting from Union law or the law of a Member State of the European Union applicable to the processing objects hereof.

The Customer may request that this period of two (2) months be extended for a new maximum duration of two (2) months, subject to respecting a notice period of fifteen (15) calendar days before the expiration of the first period of two (2) months.

The return must be accompanied by the destruction of all existing copies in the Processor's information systems. Once destroyed, the Processor must justify their destruction in writing at the latest within one month.

7. Audit

The Processor undertakes to comply without delay with requests from the Customer or auditors it may have mandated:

- To access or inspect (i) the premises, (ii) the information systems, (iii) the records as well as (iv) all documents and information, and

- To interview the Processor's personnel, in order to allow the Customer to audit and verify that the Processor and its Sub-processors fully respect the provisions hereof.

The costs of the audit are borne by the Customer. As an exception to the foregoing, if the audit reveals breaches by the Processor or its Sub-processors, the Processor reimburses the Customer for the costs of the audit, without prejudice to any compensation that could be claimed by the Customer. The Processor ensures that the contract concluded with any Sub-processor allows the Customer to proceed or have audits proceeded with as provided in this article, at this Sub-processor's and its own sub-contractors' premises.

8. Localization and Transfers of Data

In the event of a transfer of Personal Data to a third country, not belonging to the European Union, or to an international organization, the Processor must obtain the prior written agreement of the Customer. If this agreement is given, the Processor undertakes to cooperate with the Customer to ensure:

- compliance with procedures allowing for compliance with PD regulation, for example, if an authorization from the competent supervisory authority appears necessary;
- if necessary, the conclusion of one or more contracts allowing to regulate the cross-border flows of PD. The Processor specifically undertakes, if necessary, to sign such contracts with the Customer and/or to obtain the conclusion of such contracts by its Sub-processors. To do this, it is agreed between the Parties that the standard contractual clauses published by the European Commission will be used to frame cross-border flows of Data.

9. Liability

The Processor fully indemnifies the Customer in the event of a conviction of the Customer resulting from non-compliance by the Processor with its obligations under this Agreement.

Appendix A :

DESCRIPTION OF PERSONAL DATA PROCESSING

This Appendix contains certain information relating to the Processing of PD, in accordance with Article 28.3 of the GDPR.

DP Processing Start Date

The start date of Processing is the date of commencement of the performance of the services covered by the contract by the Customer.

[Click or tap here to enter a date.]

Purpose of Processing:

The purpose is the goal pursued by the customer justifying the choice of solution made by the customer.

[Click or tap here to enter text.]

Nature of Processing
(article 4 GDPR)

Processing Operations (Article 4 GDPR)	YES/NO
Collection	
Recording	
Organization	

Structuring	
Storage/Structuring	
Adaptation/Alteration	
Retrieval	
Access/Consultation	
Use	
Communication by transmission	
Dissemination or any other form of making available	
Alignment or Combination	
Restriction	
Erasure/Destruction	
Others (to be completed)	

Processors	Others: [To be completed according to the nature of the project]

Category of Personal Data Recipients
(who handles, copies, views, reuses the data)

Ex: persons in charge of service execution/contract management/billing, etc.

[Click or tap here to enter text.]

Category of Data Subjects

(Specify and complete as necessary the categories of data subjects whose data is processed. Ex: customers and prospects, employees, users, etc.)

Categories of Data Subjects	YES/NO
Users of the solution at the customer	
Users of the solution at the customer's customer or partner	
Customer employees	
Others (to be completed)	

Category of Personal Data Processed

(Specify and complete as necessary the categories of personal data processed. For example, economic and

Categories of PD Processed	YES/NO
Identification data (title, last name, first name, identifier, employee ID)	

financial data, personal characteristics, cultural data, photos, etc.)	Professional or personal contact data (phone, email address)	
	Location data (postal address, geographic position)	
	Connection data (identifiers, IP addresses, URL)	
	Content data (screenshots, comments)	
	Others (to be completed	

Data Retention (start date and duration in months)	[Click or tap here to enter text.]
Contact Details of the Supplier's Representative, and where applicable, its Data Protection Officer:	Name : First name : Position : Email Address : Phone :
Contact Details of the Customer's Data Protection Officer:	Position : DPO Email Address : retailchains.privacy@orisha.com