General Terms and Conditions – Payment Acquiring

Tabesto Pay on Legacy

Market Pay, a simplified joint-stock company with share capital of €15,340,000, headquartered at 9 rue du Quatre Septembre, 75002 Paris, listed on the Paris Trade and Companies Register under number 808 389 191, hereinafter "**Market Pay**" or the "**Service Provider**"

IT IS HEREBY AGREED AS FOLLOWS:

Market Pay is an electronic money institution authorised by the French Prudential Supervision and Resolution Authority under number 11508, and is authorised to execute payment services (including acquisition). In the context hereof, Market Pay intervenes on the part specific to regulated services (in particular the transfer of funds or "cash out" in favour of its respective beneficiaries).

To this end, the Service Provider markets a solution for acquiring proximity payments.

The Merchant runs a Business and markets its products and/or services on French territory to a clientele composed of professionals, non-professionals and consumers. As such, the Merchant, in its capacity as acceptor, is regularly required to allow cardholders to make a payment via an electronic device duly certified or approved by a payment card system (e.g. electronic payment terminal).

In particular, the Merchant has decided to develop, for the benefit of its shops, its system for accepting and acquiring electronic means of payment in order to meet the objectives of security, flexibility and scalability in the processing of transactions.

To this end, the Parties have come together to discuss and enter into this contract for the processing of payment flows to manage all the processing related to the acquisition of proximity payments.

NOW, THEREFORE, THE PARTIES AGREE AS FOLLOWS:

ARTICLE 1. DEFINITIONS

For the purposes of applying and interpreting this contract, words and expressions beginning with a capital letter shall, notwithstanding any definition given in another document, have the meanings ascribed to them below, whether used in the singular or in the plural:

Acquiring Services: has the meaning given in Appendix 3.

Affiliate: means, for each of the Parties, any company controlled directly or indirectly within the meaning of the provisions of Articles L. 233-3 and L. 233-16 of the French Commercial Code.

Agreement: means these General Terms and Conditions, including the Special Terms and Conditions, the Form and the appendices with which they form an indivisible whole.

Bank Account: means the account opened in the books of a Payment Service Provider in the name of the Merchant, the contact details of which have been previously communicated to Market Pay, and intended for the receipt of the Transferred Funds under the conditions provided for in the Agreement.

Business: means any commercial act within the meaning of Articles L.110-1 et seq. of the French Commercial Code (i) carried out by the Merchant, and (ii) which must be lawful and comply with the legal and regulatory provisions in force. The Merchant's Business has been declared in the Form.

Card: means any payment or credit/debit card, prepaid or not, issued by an Issuer to a Payer, which must be used in accordance with the requirements defined by the Payment Networks and which is accepted by the Payment System in accordance with the terms set out in the Agreement.

Data Regulations: refers to all the provisions applicable to Personal Data, such as (i) those arising from Law No. 2018-493 of 20 June 2018 on the protection of personal data, including any changes to this text, (ii) those arising from European Regulation 2016/679 of 27 April 2016 on the respect for and protection of Personal Data as from its entry into force, and (iii) any opinion, recommendation, decision or instruction issued by the National Data Protection Commission or any other supervisory authority that may replace it at the conclusion or during the execution of the Agreement.

Data: means all information created, acquired, aggregated or archived by or for the Merchant, including Personal Data, which is the subject of processing via the Solution used by the Merchant, as well as the results of processing carried out on this data via said Solution. The Data also refers to the data communicated by the Merchant relating to their activities, know-how, etc. These data are confidential and are the exclusive property of the Merchant concerned for the data concerning it.

Equipment: means any electronic device (i) supplied by a third party and described in Section 5.1 of Appendix 3, compatible with and connected to the Solution and which will be used by the Merchant, including all the hardware, software packages and software that comprise it, and (ii) which has been duly certified or approved by the Payment Network.

Effective Date: has the meaning given in Clause 13.3 of these General Terms and Conditions.

Fees: means all costs for which the Merchant is liable to the Service Provider under the the performance of the Agreement.

Force Majeure Event: means any event beyond the will or control of the Parties and impeding the performance of all or part of their obligations, as provided for by Article 1218 of the French Civil Code according to the interpretations adopted by the case law of the Court of Cassation, it being specified that the Parties consider that the following events constitute a case of force majeure: social conflicts, intervention by civil or military authorities, natural disasters, fire, water damage, malfunction or interruption of access to the Internet, a telecommunications network or the power grid, a staff strike, failure of a subcontractor or service provider, civil disturbances, riots, war or occupation of the territory by foreign forces.

Form: means the form attached to these General Terms and Conditions, and from which (i) the Service Provider collects the information of the Merchant necessary for the performance of the Services, and (ii) the Merchant agrees to be bound by all the terms and conditions provided for in the Agreement.

General Terms and Conditions: means these general conditions applicable to the Service and accepted by the Merchant from the signing of the Form.

Initial Period: means the term of the Agreement as set out in the Form.

Issuer: means any Payment Service Provider duly authorised to issue a Card to a Payer.

Merchant: refers to the natural or legal person identified in the Form which carries out its Activity from its Site.

Non-payment: means any payment cancelled (i) by a Payer or at the request of an Issuer of a Product made by means of a Card, and (ii) where relevant in application of the requirements defined by the Payment Networks. It is recalled that a Non-payment is necessarily charged against the funds collected by Market Pay, in its capacity as acquirer and intended to be transferred to the Merchant under the conditions provided for in the Agreement.

Notice Period: has the meaning given in Clause 13.3 of these General Terms and Conditions.

Parties: collectively means Market Pay and the Merchant.

Party: means individually Market Pay or the Merchant.

Payer: means the Cardholder who (i) initiates a Payment Transaction, from the Site, to pay the Merchant for a Purchase, and (ii) may request a Refund if applicable.

Payment Network: any payment card scheme as defined in Article 2 of EU Regulation No. 2015/751

of 29 April 2015 and which is linked to a brand of cards such as Visa or Mastercard, it being specified that any payment card scheme may issue Penalties in the event of breach of the Statutory Regulations.

Payment Service Provider: means any payment service provider within the meaning of article L. 521-1 of the French Monetary and Financial Code, duly approved by a supervisory or supervisory authority and which is established within the European Union.

Payment system: means the software and protocols necessary for the registration, transmission and secure processing of proximity payment orders, in accordance with the specifications defined by the Payment Networks for Card payments.

Payment Transaction: retains the meaning assigned to it by article L. 133-3 of the French Monetary and Financial Code, it being specified that for the execution of these terms, a Payment Transaction is processed by Market Pay as soon as it is carried out by means of a Card for any Purchase made on the Site.

Penalties: means any sum of money fixed and claimed by the Payment Networks due to any breach of the Statutory Regulations by the Merchant, and which is attributable to the latter.

Personal Data: means any information relating to an identified or identifiable natural person. An "identifiable natural person" is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Product: means any material or immaterial goods or any provision of services lawful and regularly marketed for business purposes on the Site by the Merchant.

Purchase: means any purchase and/or subscription of Product(s) that is paid for by means of a Card by a Payer.

Refund: means any return of funds in favour of a Payer which has the effect in particular of cancelling the Payment Transaction initially carried out by the latter for a given Purchase. As such, this refund is attributable to the Merchant, it being specified that the Refund may be claimed through the Issuer.

Sensitive Data: means any Personal Data of the Payer, including any banking data, any information or data relating to a payment order or a payment transaction, and in particular those relating to the Card and the account to which it is attached, the processing, transmission and storage of which must be the subject of protective measures in application of the constraints of the Payment System, the PCI-DSS standard and the Data Regulations.

Services: means the Acquiring Services for the acquisition of proximity payment transactions.

Site: means the physical point(s) of sale, as declared by the Merchant in the Form, in which the Merchant markets its Products as part of its Business, and in accordance with the legal and regulatory provisions in force. The Site is deemed to be the point of operation from which (i) the Service Provider is authorised to connect the Solution to perform the Services, and (ii) which will in particular allow the Payment Networks to identify the Merchant as an acceptor (in particular in the event of the misuse or theft of Data carried out by a third party on the Site, which will be qualified by the Payment Networks as a "point of compromise").

Solution: means the solution for acquiring Payment Transactions, which will be made available to the Merchant by the Service Provider under the conditions set out in this Agreement.

Special Terms and Conditions: means the special conditions which supplement the General Conditions with additional and/or complementary services to the Services, and/or where applicable derogate from these latter.

Statutory Regulations: means all laws, regulations, rules, Data Regulations, as well as any regulatory or administrative requirements in force and/or any notice, recommendation, instruction issued by the Payment Networks and which are in particular applicable to the Parties and/or the Services.

Transferred Funds: retain the meaning given in clause 5.2 of these General Terms and Conditions.

ARTICLE 2. PURPOSE

The purpose of the Agreement is to specify the conditions under which the Service Provider provides the Merchant with the services of processing electronic money flows in exchange for a financial consideration. For all intents and purposes, it is recalled that this Agreement does not apply to the acceptance services of the Payment Transactions, which are processed by a service provider, third party hereto, with which the Merchant has concluded an acceptance contract.

The services mentioned above are provided through the Payment Transactions Acquiring Solution.

ARTICLE 3. CONTRACTUAL DOCUMENTS

This Agreement expresses the entire agreement between the Parties, excluding any other current or future document that does not constitute a formalised amendment. It cancels and replaces all oral or written agreements that may have been previously concluded between the Parties for the same purpose and may be amended only by an amendment concluded in writing and signed by the Parties.

The appendices cited below have no hierarchical legal order between them:

- ***Appendix 1:*** Protection of Personal Data;
- ***Appendix 2:*** Security framework and audit procedure;
- ***Appendix 3:*** Services Description

ARTICLE 4. OBLIGATIONS OF THE PARTIES

4.1. Obligations and representations by the Parties

4.1.1. The Parties represent that they have exchanged all the written and verbal information they consider necessary and decisive for the exchange of their consent, in accordance with Article 1112-1 of the French Civil Code. As such, the Parties have also taken the time necessary to study and analyse the above information before entering into this Agreement, including with the support of any outside counsel of their choice.

4.1.2. The Parties agree (i) to cooperate closely, with loyalty and with a concern for efficiency in their relations. In particular, each Party undertakes to inform the other of any difficulties, in particular technical, human, financial or organisational, which may have an impact on the performance of its obligations under the Agreement, and (ii) to seek with the other Party, as far as possible, a solution acceptable to all and that protects the interests of the other Party.

4.1.3. Each Party certifies on the date of signature and for the entire duration of this Agreement:

- That it is duly constituted and that it carries out its business activities in accordance with the law and/or the regulations applicable to it;

- That it has the authority and capacity for the purposes of entering into this Agreement and that it has been authorized to do so by its management bodies or any other competent body;

- That it is solvent and is not subject to a cessation of payment and/or any collective procedure;

- That, to its knowledge, there is no arbitral, judicial or administrative procedure against it, which may have an impact on the validity or proper performance of this Agreement.

4.2. Obligations of the

Merchant

a) Representations

The Merchant represents that it shall:

- comply with the laws and regulations (including in tax matters), the professional provisions and good practices applicable to its Business, to the sales and services carried out at the point of sale, in particular exchanges using the networks and the different communication terminals (e.g.: mobile phones and computers). To this end, the Merchant organises the adequate traceability of information related to payment of the Products sold on its Site;

- be personally responsible for obtaining all legal, regulatory or administrative authorisations or for carrying out all formalities that may be necessary for its Business;

- refrain from any activity which could be criminally sanctioned or contrary to the Statutory Regulations, such as the endangerment of minors, acts of paedophilia, acts of counterfeiting of works protected by an intellectual property right and/or payment instruments, non-compliance with the protection of Personal Data, attacks on automated data processing systems, acts of money laundering, non-compliance with the provisions relating to gambling, horse racing, lotteries and non-compliance with the provisions relating to the exercise of regulated professions;

- undertake to inform the Service Provider without delay of any modification relating to its business (nature of the Products offered) ;

- that all information and documents provided when entering into contact with the Service Provider as well as all those provided throughout the term of the Agreement are accurate, complete and up-to-date;

- undertake to communicate to the Service Provider, at the Service Provider's request, any documents recording its entry in the Trade and Companies Register or the Trade Register, the name, legal form, registered office and type of business of the company (K-Bis extract of less than three months, powers of directors, articles of association), as well as a copy of its civil liability insurance. The Service Provider reserves the right to request any other documents (Banque de France rating index, last three balance sheets, etc.) that it deems useful;

- waive, upon signature of the Form, the application of Articles L. 341-1 et seq. of the French Monetary and Financial Code if they would apply to the present;

- be aware of the conditions related to the Acquiring Services, as defined in Appendix 3, and accept them without reservations.

b) General obligations

The Merchant undertakes to (i) pay all the invoices sent to it by the Service Provider under the conditions provided for in this Agreement, and (ii) comply with all the terms of this Agreement as well as all the applicable laws and regulations incumbent upon it in respect of the use of the Solution and/or the Services.

In this context, the Merchant is solely responsible for (i) compliance with the obligations provided for in the acceptance contract it has concluded with the service provider of its choice, (ii) its use of the Solution as well as (iii) the harmful consequences of its interventions, in particular in the transmission of Data to the Service Provider, if the Service Provider has notified the Merchant of any malfunction or anomaly as soon as it becomes aware of it, or (iii) insufficient training of its staff.

4.3. Service Provider's Obligations

4.3.1 The Service Provider undertakes to provide the Merchant with a service in accordance with the applicable regulations for the Services provided by the Solution.

The Service Provider ensures, during the term of the Agreement, the permanence, continuity and quality of access to the Solution.

The Service Provider will make its best efforts to perform with the utmost care the services entrusted to it under this Agreement. As such, the Service Provider is required to implement all means recognized as necessary, in accordance with best practices, to achieve the objectives assigned to it under this Agreement.

The Service Provider shall comply with all the normative provisions applicable to its business. For all intents and purposes, it is recalled that the P2PE functionality of the Solution is only available with compatible equipment, failing which the Service Provider cannot be held responsible for the absence of this functionality.

4.3.2. Throughout the term of the Agreement, Market Pay agrees to perform the Services relating to the acquiring of Payment Transactions in accordance with the Statutory Regulations, in particular the requirements imposed by the Payment Networks as well as the practices of the payment industry.

As such, Market Pay will acquire all Payment Transactions and pay them on to the Merchant under the terms and conditions provided for in this Agreement.

In addition, Market Pay will respect the choice of the brand and the category of Card and the payment application, within the meaning of article 2.21 of EU Regulation No. 2015/751 of 29 April 2015, used to give the payment order made at the point of sale in accordance with the choice of the Merchant or the Cardholder.

ARTICLE 5. PAYMENT GUARANTEE AND PAYMENT SETTLEMENT

5.1. Payment guarantee

Payment Transactions are guaranteed subject to all the security measures and those relating to the settlement of Payment Transactions provided for herein, as well as the conditions specific to each of the Payment Networks.

All security measures are independent of each other. Thus, the authorisation granted by the authorisation server only constitutes a guarantee subject to compliance with the other security measures, and in particular the control of the confidential code.

In the event of non-compliance with only one of these measures, the registrations are only settled subject to the successful completion of collection.

5.2. Payment Transaction Settlement

Any payment order by Cards registered by the Solution and authorised by an Issuer on a non-working day is put in interbank clearing on the next working day from the receipt of the funds in accordance with Article L. 522-17 of the French Monetary and Financial Code.

Pursuant to article L. 133-11 of the French Monetary and Financial Code, the Merchant authorizes Market Pay to offset any sum resulting from a Payment Transaction with the Fees, Non-payments, Penalties and any Refunds (hereinafter the "Transferred Funds").

Subject to (i) the successful collection of funds by Market Pay, (ii) acceptance of Payment Transactions by Market Pay Tech, and/or (iii) applicable anti-money laundering and terrorist financing provisions, the Transferred Funds will be paid into the Bank Account no later than D+1 from the actual receipt of sums from a Payment Transaction.

For all intents and purposes, it is recalled that each Party remains liable for any tax and other duties that would be applicable to their own business (e.g. VAT).

ARTICLE 6. FINANCIAL TERMS AND CONDITIONS

Unless otherwise specified, all Fees appearing on the subscription form are established excluding tax and are payable in euros (€) including all taxes.

In consideration of the provision by the Service Provider of the Services expressly accepted by the Merchant, the latter shall pay the Service Provider the Fees set out in the membership form, it

being specified that the costs relating to the computer equipment as well as the connection of the Merchant's equipment to the Solution and, in general, any fees or costs relating to goods or services necessary for the Merchant's Business remain at the expense and at the sole risk of the Merchant (e.g. the Internet, electricity, etc.).

Invoices issued by the Service Provider shall be payable without discount, by bank transfer, according to the invoicing terms set out in the membership form.

Any reminder costs will be borne by the Merchant and charged to the first invoice following the reminder. In any event, and in particular in the event of late payment, the Service Provider reserves the right to request immediate payment of all sums owed and not yet due. As the Merchant is required to pay the invoices on their due date, and without which the Service Provider would not have contracted, it is expressly agreed between the Parties that in the event that a payment order issued to the Service Provider is not honoured in whole or in part, for any reason whatsoever, the sums remaining due to the Service Provider by the Merchant are, in accordance with Articles L.441-3 and L.441-6 of the French Commercial Code, automatically and without prior notice, amended by adding: (i) default interest on the basis of the interest rate applied by the European Central Bank to its most recent refinancing operation plus ten (10) percentage points, which may not be less than three (3) times the statutory interest rate in force on the date of issue of the invoice concerned; and (ii) a fixed recovery indemnity of forty (40) euros, or a higher amount on production of a receipt, not subject to VAT and payable without delay, for recovery costs. Interest on arrears is calculated from the day following the due date of the outstanding amount until its full payment.

ARTICLE 7. SECURITY

7.1. General

The Service Provider has the obligation to insure and to guarantee (and/or have a third party insure and guarantee) the security, integrity and confidentiality of the facilities and computer systems throughout the term of the Agreement and, to this end, it agrees to implement all applicable logical and physical security measures.

The Service Provider undertakes to notify the Merchant as soon as possible of any situation affecting the physical or logical security of its facilities or the data it administers, and must take all necessary measures to remedy this. The Service Provider also undertakes to inform the Merchant of the measures it takes.

7.2. Security incident management

The Service Provider, directly or through its own service providers, will maintain and comply with the appropriate security measures at the technical level in order to protect the Merchant's Data, to which the Service Provider may have access in the context of the performance of the Agreement, against any accidental or unlawful destruction, alteration, disclosure or unauthorized access (hereinafter a "**Security Breach**"), in particular when the processing involves the transmission of data or databases through a network, and against any other form of unlawful processing.

As soon as there is a proven Security Breach, the Service Provider will inform the Merchant without undue delay, and will immediately take all necessary measures to minimize the damage and secure all of the Merchant's Data.

In the event of a Security Breach, the Service Provider will work with the Merchant to determine the origin of the Security Breach.

7.3. PCI DSS Standard

The Service Provider undertakes to maintain the existing PCI DSS certification resulting from the PCI DSS certification specific to the platforms operated by its service providers.

The Merchant declares that its centralised acceptance system complies with the standards relating to the PCI-DSS, and undertakes to maintain the PCI-DSS certification during the performance hereof, and where applicable to provide a copy to the Service Provider on simple request of the latter.

7.4. Security obligations of the Merchant

7.4.1. The Merchant undertakes to (i) immediately inform the Service Provider in the event of abnormal operation of the Equipment or any other anomalies (e.g. absence of receipt or update of the black list, it not being possible to repair quickly, etc.), and (ii) cooperate with the Service Provider when it stores, processes or transmits sensitive payment data in the event of a major payment security incident or data compromise.

The refusal or lack of cooperation on the part of the Merchant may lead the Service Provider to terminate this Agreement in accordance with the article "Duration, amendment, suspension and termination of the Agreement".

7.4.2. The Merchant shall comply with the requirements of the PCI DSS security framework (appearing in Appendix 2) and its updates of which it can read about at the following address: https://fr.pcisecuritystandards.org/minisite/env2.

7.4.3. The aforementioned security measures may be modified and supplemented throughout the term hereof, in accordance with the procedure provided for in the article "Duration, modification, suspension and termination of the Agreement".

7.5. Preventive measures and sanctions applied by the Service Provider

7.5.1. In the event of the Merchant's failure to comply with the provisions of this Agreement or the laws in force, or in the event of an abnormally high rate of non-payments or the abnormal use of lost, stolen or counterfeit Cards, the Service Provider may take safeguard and security measures consisting, in the first place, of a warning to the Merchant that constitutes formal notice, specifying the measures to be taken to remedy the failure or to reduce the abnormally high rate of non-payments found.
If, within thirty (30) days of the issue of the warning, the Merchant has not remedied the failure which justified the warning or has not implemented the measures intended to reduce the rate of non-payments noted, the Service Provider may either suspend the acceptability of the Cards under the conditions specified in the article "Duration, modification, suspension and termination of the Agreement", or terminate automatically with immediate effect, subject to the outcome of the current operations, this Agreement, by registered letter with acknowledgement of receipt.
Similarly, if within a period of three (3) months from the warning, the Merchant is still confronted with an abnormally high rate of non-payments, the Service Provider may decide the termination ipso jure with immediate effect, subject to ongoing operations, of this Agreement, notified by registered letter with acknowledgement of receipt.

7.5.2. Notwithstanding the provisions of Article 7.5.1 above, the Service Provider may also take, at its discretion and with immediate effect, all or part of the Conservatory Measures below aimed at protecting the interests of Market Pay as the acquirer of the Payment Transactions if (i) the thresholds for rates of fraud and/or non-payments set by the Payment Networks are exceeded by the Merchant, or (ii) the Merchant refuses to apply or implement the measures to secure the Service requested by the Service Provider, or (iii) in the event of a risk of fraud or attempted fraud or a circle of fraud identified or suspected by the Service Provider, or (iv) if a Payment Network requires the Merchant to apply one of its anti-fraud programs, or (v) in the event of a modification of the Business or a payment order or a Payment Transaction, without the prior

written authorisation of the Service Provider.

The Protective Measures are as follows: (a) the Merchant must implement enhanced preventive and protective measures regarding the Payment Transactions, in particular with regard to the security parameters of Payment Transactions, (b) retain, in a contained manner, any sums resulting from the Payment Transactions and suspend any payments to the Bank Account during the period necessary to analyse the suspicious Payment Transactions and decide on the action to be taken, it being specified that this analysis may be carried out at the level of the Service Provider and/or any jurisdiction and/or supervisory authority and the suspension of payments may be imposed for a maximum period of thirteen (13) months or any other period decided by a supervisory authority and/or a Payment Network in order to clear the Non-payments or for the purposes of the investigation carried out by the court, (c) the suspension of any Refund functionality provided for by the Tools, it being specified that it will be up to the Merchant to carry out itself and by its own means any necessary diligence regarding the Payer, (d) the Merchant may be obliged to proceed with the refund of the Payment Transactions to Payers who have made a Purchase and have not received the Product(s) ordered, (e) the Service Provider may block the account opened in its books in the name of the Merchant and, if necessary, suspend all or part of the Service (for a maximum period of thirteen (13) months or any other period decided by a Payment Network in order to clear the Non-payments), (f) the Merchant may be required to provide a financial guarantee to cover Fees, Non-payments, Refunds and/or Penalties, (g) the Service Provider may terminate the Agreement for the Merchant's fault, without prejudice to any damages.

ARTICLE 8. CHANGES TO THE LEGISLATION OR REGULATIONS AND TO PAYMENT NETWORK RULES

If a change to all or part of the Payment System is made necessary during the performance of the Agreement due to a legal, regulatory obligation or a rule specific to the Payment Networks, the Service Provider will make or have a third party make all the necessary changes to the Solution for the purposes of complying with these new obligations, without additional cost to the Merchant.
The Parties agree that the Service Provider cannot be held liable for any non-compliance with these changes following the absence of validation or the refusal of validation by the Merchant of the terms of implementation.
The Service Provider will inform the Merchant as soon as possible before the change in question of the purpose of the changes that will be made, in order to enable it to identify and assess the impacts on electronic money flows.
It is agreed that the Merchant will bear any costs relating to the implementation in its own systems of the new version of the Payment System incorporating legal or regulatory changes or modifications decided by the Payment Networks.

ARTICLE 9. MAINTENANCE AND UPGRADE OF THE SOLUTION

The Service Provider shall be responsible for the maintenance of the Solution as well as any upgrades to the operation or related to the security of the Solution.
The Service Provider may also carry out technical upgrades, such as the acceptance of new payment cards, the modification of software, the adjustment of certain parameters.
Any upgrade to the Solution or additional maintenance service thereof that may be desired by the Merchant will be the subject of a feasibility study and will be accompanied, if necessary, by a quote.

ARTICLE 10. PROTECTION OF PERSONAL DATA

The Service Provider agrees to comply with the provisions incumbent upon it according to the Data Regulations.
The Service Provider will take the necessary measures to enable it to comply with the Data Regulations.
The Service Provider undertakes to the Merchant to process the Personal Data within the meaning of the applicable legislation within the strict and necessary framework of the services to be performed under the terms of the Agreement and, in any event, to act only on the Merchant's prior written instruction.
Consequently, the Service Provider undertakes, for the processing operations described in ***Appendix 1***, to:

- ensure the protection of Personal Data and related processing to which it has access, in accordance with the applicable regulations;

- take all necessary precautions to preserve the confidentiality and security of Personal Data to which it has access or which it collects during the performance of its services, and in particular to prevent accidental or unlawful destruction, accidental loss, alteration, unauthorised dissemination or access, in particular when the processing involves the transmission of data over a network, as well as against any form of unlawful processing, it being specified that these measures must ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected;

- inform the Merchant immediately in writing of any modification or change affecting it that may have an impact on the processing of the Personal Data it performs on behalf of the Merchant;

- not to use the Personal Data for purposes other than those provided for in this Agreement;

- put in place the necessary authorisations and/or segmentation, in order to allow access to Personal Data only to authorised persons to the extent strictly necessary for the processing of such Personal Data;

- that persons having access to the Personal Data are subject to an appropriate written confidentiality and security obligation;

- at the end of this Agreement, return immediately to the Merchant, on an appropriate medium, all the files, manual or computerized, of Personal Data that are in its possession and not to keep any copies.

The Service Provider is prohibited from communicating all or part of the Personal Data, even free of charge, to another unauthorised person.
The Service Provider acknowledges that it has technical and organisational security measures adapted to the processing and operations to be carried out in accordance with the Merchant's instructions.
As part of the services provided under the Agreement, the Parties agree that the Service Provider will only keep the Sensitive Data necessary for the proper execution of payment orders and the fight against fraud, in accordance with the Statutory Regulations. The Sensitive Data are kept by the Service Provider in accordance with Statutory Regulations, and will be destroyed at the end of the timeframes set by any supervisory or control authority (such as the CNIL) or by the Data Regulations.
The Data and databases of the Merchant containing or not Personal Data to which the Service Provider may have access in connection with the performance of the Agreement are the exclusive property of the Merchant.
The Service Provider shall refrain from (i) infringing the Merchant's property rights relating to the Data and databases referred to above and in this regard, (ii) communicating them to third parties, (iii) reproducing them, and (iv) carrying out extractions, except for the strict needs of the provision of the services covered by the Agreement to the Merchant or at the Merchant's express and prior written request or affecting the security of such Data, their processing and databases.
Similarly, the Service Provider shall refrain from any other exploitation of the Data and databases than those provided for in this Agreement, in particular the Service Provider shall refrain from marketing,

renting, transferring, assigning and/or making available said Sensitive Data to third parties for any purpose whatsoever, for consideration or free of charge, unless otherwise provided for by the Statutory Regulations (e.g. judicial requisition).

With regard more particularly to Personal Data, the Merchant alone has the capacity of data controller (unless otherwise agreed between the Parties, or if the factual situation also makes it possible to demonstrate a co-responsibility of processing of the Service Provider and the Merchant or the capacity of data controller of the Service Provider). Consequently, the Service Provider undertakes, under the terms of a performance agreement, to take the necessary measures to ensure the protection and confidentiality of the Data transmitted to it by the Merchant and to process this Data on the Merchant's exclusive behalf in compliance with the applicable legal and regulatory provisions, in particular those relating to Personal Data, of the Agreement and in accordance with the directives given by the Merchant. The Service Provider is a subcontractor of the Merchant, within the meaning of the Data Regulations, with regard to the Personal Data of the Merchant, which is the subject of the Services.

The Service Provider warrants that the Data that may be present on its facilities or that it may access from its facilities or those of third parties that it uses, on the date of signature of the Agreement, will be located in France or in a country offering an adequate level of protection according to the National Commission of Information Technology and Liberties and it is prohibited during the performance of the Agreement, in particular: (i) to change the country in which the Data is hosted, or (ii) to involve, in the provision of the services, third-party service providers such as subcontractors located in a country that does not offer an adequate level of protection according to the French Data Protection Authority, or (iii) to carry out any other act that may be interpreted as a transfer of Personal Data outside the European Union according to the French Data Protection Authority, without the prior written authorisation of the Merchant.

In addition to the provisions of the Article "Security", in general, the Service Provider will maintain and comply with the appropriate security measures from a technical point of view to protect the Data, to which the Service Provider may have access in the context of the performance of the Agreement, against any accidental or unlawful destruction, or accidental loss, damage, alterations, disclosure or unauthorized access in particular when the processing involves the transmission of data or databases through a network, and against any other form of unlawful processing. In addition, the Service Provider must comply with any reasonable special security measures required from time to time by the Merchant. In the event of loss or alteration of the Data by the Service Provider, the Service Provider shall restore them at its own expense.

At the end of the Agreement for any reason whatsoever, the Service Provider undertakes to return to the Merchant all the Data in its possession or under its control, including all Personal Data, in any form whatsoever, and not to keep a copy thereof.

Moreover, the Service Provider undertakes to:

- modify or delete, at the request of the Merchant and in accordance with its instructions, the Personal Data that may have been entrusted to it as a result, in particular, of the exercise by a natural person, of its right of access and rectification, so that the Data contained in the systems are accurate;

- inform the Merchant as soon as possible of any fact constituting a breach of the physical or logical security of its facilities and/or data (attempted intrusion or the appearance of a new virus for example) and to take any measure to remedy it, of which it must keep the Merchant informed and, with regard to Personal Data, in accordance with the Data Regulations applicable in the matter;

- assist the Merchant (with the exception of any legal assistance) in responding to any request for information from the supervisory authorities concerning the Merchant's Personal Data for which it is responsible for processing, and in particular:

  - assist the Merchant in providing everything relating to the identification, location, legibility and availability of the Merchant's Data and more generally the processing carried out relating thereto under the responsibility of the Service Provider, as requested by the supervisory authority,
  - cooperate fully to facilitate access to the Merchant and the supervisory authority to the Data under the responsibility of the Service Provider,
  - provide the Data to the supervisory authority only with the prior consent of the Merchant.

In the latter case, the Service Provider will process these exceptional requests, without additional invoicing provided that these requests do not involve the implementation of additional resources and disruption of the Services. All requests not falling within this framework, will be processed by the Service Provider, after agreement between the Parties on the applicable terms.

ARTICLE 11. COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

Market Pay is subject to all French regulations relating to the prevention of money laundering and the financing of terrorism.

Pursuant to the provisions of French law relating to the participation of financial institutions in the fight against money laundering and the financing of terrorist activities, Market Pay is required to collect all information relating to the identification and activity of the Merchant in order to fulfil its customer knowledge obligations (known as "Know Your Customer" or "KYC").

To this end, the Merchant agrees to transmit without delay and upon first request any information requested by Market Pay.

In addition, Market Pay is required to inquire with the Merchant, for any transaction or business relationship, about the origin, purpose and destination of the Payment Transaction.

The Merchant acknowledges that Market Pay may terminate or postpone at any time the use of personalized security data or the execution of a Payment Transaction in the absence of sufficient information on its purpose or nature. He is informed that a transaction carried out within the framework hereof may be the subject of the exercise of the right of communication of the national financial intelligence unit, in application of the Statutory Regulations.

The Merchant may, in accordance with the regulations, access all the information thus communicated, provided that this right of access does not call into question the purpose of combating money laundering and the financing of terrorism when this data relates to the applicant.

No suit or civil liability action may be brought or any professional sanction pronounced against the Service Provider, its officers or servants who have made in good faith the suspicious statements to their national authority.

ARTICLE 12. LIABILITY

12.1. The Parties are liable for any damage and direct harm they cause or that is caused by their personnel, suppliers, service providers or subcontractors in connection with the performance of this Agreement.

12.2. Consequently, the Parties undertake to compensate, for the part falling within their responsibility, for the damages and losses caused during the performance of their obligations, subject to the limits set by Article 1231-4 of the French Civil Code.

12.3. The Service Provider's liability shall be limited to the costs actually paid by the Merchant during the last twelve (12) months preceding the event incurring the Service Provider's liability.

The Parties expressly agree that the limitation of the Service Provider's liability (i) is reasonable, proportionate to the risks assumed and the benefits derived by each of the Parties from the performance of the Agreement, and (ii) is the condition of the provision of the

Service on the financial terms set out in the subscription form.

12.4. The Merchant shall bear all damages and losses, costs, charges or fees of any kind whatsoever (including attorneys' or experts' fees) and any costs and/or Penalty(s) decided and/or imposed by the Networks and any Payment System integrated into the Service that may be incurred by the Service Provider as a result of Merchant's breach of its obligations under the Agreement or in the event of legal action or threat of legal action by third parties (in particular, the Payer) caused by Merchant or for which Merchant is liable.

ARTICLE 13. DURATION, AMENDMENT, SUSPENSION AND TERMINATION OF THE AGREEMENT

13.1. This Agreement takes effect from the Commencement Date and shall expire at the end of the Initial Period. It may be renewed by tacit agreement for successive periods of (1) year, unless terminated by one of the Parties by registered letter with acknowledgement of receipt sent at least fifteen (6) months before the end of the Initial Period under way.

The Parties agree that this Agreement shall take effect from the date on which the Merchant's profile is duly declared compliant by Market Pay, in accordance with the Statutory Regulations and/or its internal procedures (hereinafter the "**Commencement Date**"), it being recalled that it is the Merchant's responsibility to deliver to Market Pay, as soon as possible, all the documentation required by the latter in order to be able to use the Solution and benefit from the Services provided herein. In addition, it is recalled that Market Pay may, in application of the Statutory Regulations, decide at its own discretion to reject the Merchant's profile, without any financial consideration for the benefit of the latter.

13.2. Any amendment of this Agreement shall be made by an amendment signed by the Parties.

However, the Parties agree that this Agreement may be amended by the Service Provider by sending written notice to the Merchant, in particular in one of the following cases:

- in the event of technical, legal, fiscal or regulatory changes;

- in the event of changes to the Services;

- in the event of changes to the rates of the Payment Networks;

- in the event of compliance with the requirements of the Payment Networks. As such, the Payment Networks may in particular impose technical modifications such as (i) acceptance of new Cards, software modifications, the modification of certain parameters, and (ii) security modifications such as modification of the authorisation request threshold, the suspension of membership in a Payment System or in the Payment Network(s).

These amendments to the Agreement shall enter into force on the expiry of a period of thirty (30) calendar days from the aforementioned written notification (or any other longer notice indicated in the said notification) (hereinafter the "**Notice Period**").

The Notice Period is however reduced to five (5) calendar days when the Service Provider or the Payment Network finds, in the Merchant's point of sale, an abnormal use of lost, stolen or counterfeit Cards.

Any refusal by the Merchant within the Notice Period must be notified in writing by the Merchant to the Service Provider, it being specified that the said refusal will result in the termination of the Agreement by operation of law and with effect from the first working day from the expiry of the Notice Period.

After the Notice Period, if the Merchant has not made a decision, it is deemed to have accepted the modification notified to it by the Service Provider.

13.3. Suspension/interruption:
13.3.1. The Service Provider may, for security reasons, without notice and subject to the outcome of ongoing transactions, suspend or interrupt the Services bearing certain brands accepted by the Merchant. Suspension or interruption is preceded if necessary by a warning to the Merchant, or even a reduction in its authorisation threshold. It shall be notified by any means and shall state the reasons on which it is based. Its effect is immediate, it being specified that the Merchant cannot claim the payment of any financial consideration.

The suspension or interruption may also take place at the end of the audit procedure referred to in ***Appendix 2*** in the event that the audit report reveals one or more breaches both of the clauses of this Agreement and of the security framework of the aforementioned Appendix and their updates.

The suspension may be decided due in particular to (i) repeated non-compliance with the obligations of this Agreement and the refusal to remedy it or a risk of significant malfunction of the acceptance system(s), (ii) participation in fraudulent activities, in particular an abnormal use of lost, stolen or counterfeit Cards, (iii) repeated complaints from other members or partners of the Payment Networks concerned and which could not be resolved within a reasonable time, (iv) the exceeding of all or part of the fraud rates and/or non-payment rates set by the Payment Networks due to the Merchant's business, (v) deliberate or unjustified delay in the transmission of supporting documents (including in particular the delivery of a copy of any PCI-DSS certification), (vi) an incompatibility between the Merchant's profile and/or business with the Statutory Regulations (e.g. all or part of the Products offered by the Merchant are declared illegal), and/or (vii) an aggravated risk due to the Merchant's businesses.

The period of suspension or interruption is at least six (6) months, possibly renewable. On the expiry of this period, the Merchant may request the resumption of this Agreement from the Service Provider.

Apart from a Force Majeure Event, the Services (including the Solution) may also be suspended or interrupted (i) due to the maintenance operations of the Solution that would be required, in particular to remain in compliance with the Statutory Regulations, (ii) in the absence of delivery at the first request of the Service Provider of any proof that required by the Service Provider so that it can meet the requirements of the Statutory Regulations, or (iii) at the request of any Payment Network or any supervisory, control, judicial or administrative authority, it being specified that in such a case the Service Provider will make its best efforts, to the extent permitted by the Statutory Regulations, to notify the Merchant as soon as possible.

13.3.2. Notwithstanding the preceding paragraph, if the Merchant's profile presents a risk during the performance of the Agreement (in particular in the event of a change in the Merchant's Business, a change in the Merchant's shareholding, or a deterioration in the Merchant's financial situation), the Merchant will hand over to Market Pay, at the latter's request, any financial guarantee (e.g. security deposit) that will serve essentially to cover any risk to which Market Pay would be exposed under the performance of this Agreement.

The aforementioned request will be notified to the Merchant by email. The Merchant shall have fifteen (15) days from the receipt of the request (or any other period mentioned in the notice) to carry out the necessary tasks.

Otherwise, the Agreement may be suspended or interrupted in accordance with the procedures set out in the previous article.

13.4. Termination for breach: In the event of a serious breach by one of the Parties of any of its obligations under the Agreement, and failing this Party to have remedied it within thirty (30) calendar days from the sending by the other Party of formal

notice setting out the said breach, the latter may at any time pronounce the termination of the Agreement with immediate effect, without prejudice to the payment of any amounts remaining due and any damages to which it may be entitled in accordance with this Agreement.

13.5. Termination without fault and on any other grounds: To the extent permitted by the Statutory Regulations in force, the Service Provider may terminate this Agreement with immediate effect and ipso jure in the event of one of the following events:

- If a Payment Network requires the termination hereof for failure to comply with the Statutory Regulations;

- If the Business of the Merchant has been modified without it having been previously approved by the Service Provider or if the business of the Merchant or its profile no longer complies with the Statutory Regulations;

- In the event of a change of control in the Merchant's shareholding, without having been previously approved by Market Pay, it being specified that the concept of "control" is understood within the meaning of Article L.233-3 of the French Commercial Code;

- If one of the officers of a Party is the subject of a judicial conviction no longer allowing the maintenance of this Agreement;

- If Merchant refuses or fails to provide any information requested by the Service Provider within forty-eight hours (48 hours) of the issue of the request, in particular to enable the Service Provider to meet the obligations provided for in the Statutory Regulations;

- If an essential element communicated by the Merchant and to which it has committed proves to be inaccurate or misleading;

- If the financial position of either of the Parties becomes irreparably compromised.

13.6. Any termination of Merchant's business or loss, suspension or interruption of the authorisations or approvals of either Party shall result in the immediate termination of this Agreement by operation of law subject to the termination of current operations.

13.7. Consequences of termination of the Agreement:

In the event of termination of the Agreement, for any reason whatsoever, the Merchant acknowledges and agrees that any invoice issued and not yet paid in whole or in part by the Merchant, or issued after the termination of the Agreement for Services prior thereto, shall be due and payable immediately to the Service Provider.

Any debt not paid to the Service Provider by the Merchant and which is revealed after the termination of the Agreement, shall be paid without delay by the Merchant, and may be the subject of a declaration of debt in favour of the Service Provider, and/or, where applicable, any recovery procedure initiated by the Service Provider against the Merchant, without prejudice to any damages.

ARTICLE 14. INTELLECTUAL PROPERTY

During the term of the Agreement and in return for the payment of the Services, the Service Provider grants the Merchant a non-exclusive right to use and access the Solution for the processing of their payment transactions and to have access to the relevant documentation subject to compliance with the following conditions, it being recalled that the aforementioned right is personal, non-assignable and global. As such, the Service Provider guarantees the Merchant against any recourse, action or claim that may arise in this regard.

Any right granted and/or any use of trademark and/or trade name by one of the Parties during the performance of the Agreement will automatically cease without prior formality at the same time as the termination of the contractual relationship between the Parties, for any reason whatsoever.

The Merchant shall refrain from:

- modifying, translating, arranging, copying, back compiling or adapting the Solution or any element thereof or related documentation;

- assigning, leasing, encumbering, marketing, exploiting in any way, making available to third parties or using on behalf of third parties the Solution or any element thereof or the documentation or any intellectual and industrial property rights related to the Solution or the related documentation other than at and to the extent expressly permitted by this Agreement;

- disclosing or giving access to the Solution or any part thereof or related documentation, to any third party other than the Merchant who has not received prior written authorisation from the Service Provider to this effect;

- using the Services and/or the Solution for purposes other than those provided for in this Agreement.

This Agreement does not imply the assignment of any right of reproduction, modification, adaptation or representation, with the exception of that necessary for the loading, display, execution, transmission or storage of the software under the conditions provided for in the Agreement. In accordance with Article L. 122-6-1 of the French Intellectual Property Code, the Merchant may make a backup copy of the software of which the Service Provider authorises the storage by the Merchant on its servers. The Service Provider reserves the exclusive right to provide the Merchant, for a reasonable consideration, with the information necessary to allow the interoperability of its software with the software of third parties. The right to use the software may not be assigned or granted by the Merchant to a third party, whether for a fee or free of charge.

The Service Provider represents and warrants that it holds all the rights and authorisations necessary to enable the Merchant to use the Solution and the Services made available to the Merchant as part of the Service. The Service Provider undertakes to guarantee and indemnify the Merchant against any final order for damages pronounced in France for the benefit of a third party claiming a violation of its intellectual property rights caused by a normal use of the software by the Merchant within the framework of the Service, as an exclusive remedy for the Merchant and provided that:

- the Merchant promptly informs the Service Provider as soon as it becomes aware of such action;

- the Merchant reserves to the Service Provider the conduct of the trial, does not make any total or partial acknowledgement of liability and refrains (except at the express request of the Service Provider) from compromising, attempting to compromise and in general speaking on the subject of the dispute and the circumstances of the dispute; and

- the Merchant acts in accordance with the instructions of the Service Provider and provides the Service Provider with all the assistance it may reasonably request or require for the conduct of the trial and the defence. This assistance includes in particular the transmission of all required documents and documents.

Subject to the Merchant's compliance with the above provisions, the Service Provider shall bear the costs incurred for the defence. The Service Provider shall not be bound by any guarantee if the infringement of the intellectual property rights claimed by the third party results from a violation by the Merchant of its obligations under the Agreement, or from a modification of the software by the Merchant or a third party.

The protection owed by the Service Provider to the Merchant under this article shall apply only if the software granted by the Service Provider has not been modified by the Merchant without the prior written consent of the Service Provider, or in the

event of the use of such software not provided for in this Agreement.

In the event of an infringement during the performance of the Agreement, the Service Provider shall, at its choice and expense, and within a time frame compatible with the needs of the Merchant: (i) modify all or part of the disputed elements in order to avoid infringement, (ii) obtain the authorisation of the Merchant to continue using the said software, or (iii) provide a replacement solution provided that such a replacement does not affect the operation of the said software.

The Merchant acknowledges and agrees that the provisions of this article constitute essential provisions without which the Service Provider would not have contracted.

ARTICLE 15. AGREEMENT ON PROOF

By express agreement between the Parties, the electronic records constitute proof of the payment transactions delivered to the Service Provider. In the event of a conflict, the electronic records produced by the Service Provider or the Payment System whose rules apply to the payment transaction concerned shall prevail over those produced by the Merchant, unless the latter demonstrates the lack of reliability or authenticity of the documents produced by the Service Provider or the Payment System.

ARTICLE 16. OTHER PAYMENT NETWORK REQUIREMENTS

16.1. Withdrawal from its holder of a Card subject to blocking or cancellation

In the event of withdrawal from its holder of a Card subject to blocking or cancellation (the withdrawal having taken place in particular at the instruction of the authorisation server due to the presence of the Card on the list of Cards subject to blocking or cancellation and/or counterfeit), the Merchant uses the procedure for management and return of the captured Cards.

For any capture of a Card subject to blocking or cancellation and/or counterfeit and at the instructions of the Equipment, a bonus will be paid to the Merchant or any person indicated by it and carrying out an activity within its place of business.

16.2. The holder forgets his Card

In the event that the holder forgets his Card, the Merchant may return it to him within a maximum of two working days after the date of forgetting the Card, upon proof of his identity and after obtaining an agreement requested in accordance with the procedure communicated by the Service Provider. Beyond this period, the Merchant uses the procedure for the management and return of forgotten Cards

16.3. Refunds

The partial or total refund of a purchase of goods or services paid for by Card must, with the agreement of its holder, be made to the holder of the Card used for the initial transaction.

The Merchant must then use the so-called "credit transaction" procedure, and within the period provided for in the rules of the Payment System that apply to the payment transaction in question, make the corresponding delivery to the Service Provider to whom it had delivered the initial transaction. The amount of the "credit transaction" must not exceed the amount of the initial transaction.

16.4. Unsigned card

In the case of an unsigned Card and if there is a signature panel on the Card, the Merchant must ask the Cardholder to prove his identity and to affix his signature on the signature panel provided for this purpose on the back of the Card and finally check the conformity of this signature with that appearing on the identity document presented by the Cardholder. If the Cardholder refuses to sign his Card, the Acceptor must refuse payment by Card.

ARTICLE 17. CONFIDENTIALITY – BANKING SECRECY

17.1. General

Each of the Parties acknowledges that they will be required to communicate to each other (as well as to their managers, employees, advisors and subcontractors who directly need to know this information) (together the "**Authorised Persons**") certain technical, commercial, financial or other information relating to their respective activities, as well as the Agreement and all its Appendices and amendments, whether this information has been delivered in writing, orally or by any other means (the "**Confidential Information**") within the framework of the Agreement.

In order to protect the confidential nature of the Confidential Information, each Party undertakes under the terms of the Agreement to:

a) maintain absolute confidentiality of the Confidential Information and not to disclose it to any third party to the Agreement (other than the Authorised Persons), subject to the prior written consent of the Party owning the Confidential Information concerned;
b) use the Confidential Information only in the context of the Agreement, and therefore to refrain from any other use, directly or indirectly, in any form whatsoever, either for itself or on behalf of any third party;
c) ensure that the Authorised Persons to whom all or part of the Confidential Information has been communicated are informed by this Party of the obligations under the Agreement relating to this Confidential Information;
d) return, at the request of either Party, any Confidential Information in its possession, and destroy any copy of any Confidential Information in its possession (however, this obligation does not extend to documents or reports prepared on the basis of the Confidential Information or incorporating certain Confidential Information, provided that such documents and reports remain confidential under the conditions stipulated in paragraphs (a) to (c) above).

it being understood that the obligations referred to in paragraphs (a) to (d) above shall not apply to Confidential Information communicated by a Party and which:

- has fallen into the public domain at the time of their communication or after their communication, provided, in the latter case, that this communication is not the result of a breach of confidentiality by the Party having knowledge of the Confidential Information concerned;

- was known by the other Party in a lawful and peaceful manner, prior to the date on which such Confidential Information was communicated to it;

- should be communicated by the other Party under any applicable law or regulation or at the request of any supervisory or regulatory body, administration or court;

- is legitimately obtained by the receiving Party from a third party, which in making such disclosure does not breach any obligation of confidentiality;

- is developed autonomously by the receiving Party;

- is disclosed by the Disclosing Party to a third party without any obligation of confidentiality;

- is disclosed by the receiving Party with the prior written consent of the Party to which it belongs.

This confidentiality obligation applies for the entire term of the Agreement as well as for a period of two (2) years upon expiry or termination of the Agreement, for any reason whatsoever, with the exception of the Merchant's Personal Data for which the confidentiality obligation continues for the entire period during which they are not disclosed to the public by the Party that is the original holder or the data subject within the meaning of the applicable provisions on personal data protection.

17.2. Bank secrecy

When signing or executing this Agreement, each Party may have access to information covered by banking secrecy, in addition to Personal Data.

By express agreement, the Merchant authorises the Service Provider to store, where applicable, secret or confidential data relating to it and to communicate them to entities involved in the operation of the payment system for the sole purpose of processing Payment Transactions, preventing fraud and processing complaints, whether from the Payers or other entities.

ARTICLE 18. FORCE MAJEURE

18.1. For any case of Force Majeure Event or any other cause beyond the foresight and control of one of the Parties and likely to prevent it from performing its contractual obligations, the prevented Party shall inform the other Party by any means as soon as possible with confirmation by registered letter with acknowledgement of receipt within five (5) following working days.

18.2. The obligations of the Parties shall be suspended for the duration of the Force Majeure Event and the Parties shall use their best efforts to limit the duration and effects of the cause of the Force Majeure Event. Upon the disappearance of the Force Majeure Event, the prevented Party shall inform the other Party of such disappearance and shall immediately resume the performance of its contractual obligations.

18.3. Should the duration of the Event of Force Majeure Event exceed thirty (30) consecutive calendar days, the Parties will consult on the terms of the continuation or eventual termination of this Agreement.

Each of the Parties may notify the other of the automatic termination of the Agreement by registered letter with acknowledgement of receipt without any compensation being claimed by either of the Parties.

Any termination of the Agreement pronounced by one of the Parties due to a Force Majeure Event under the conditions provided for in this article will have the effect of enabling the Merchant to trigger the reversibility measures, as provided for in the Agreement.

18.4. The Parties agree that the Service Provider cannot be required to carry out the following actions, the list of which cannot be considered exhaustive, to limit the duration and/or the effects of the Force Majeure Event (i) to record and safeguard the integrity of any Data relating to the payment orders received, pending the return to normal conditions of performance of the Agreement, or (ii) to preserve the funds relating to the Payment Transactions in accordance with the Statutory Regulations.

ARTICLE 19. SUBCONTRACTING

It is recalled that the Solution and the associated Service are composed of complex operations that involve many stakeholders. In this context, the Service Provider is free to subcontract all or part of the services necessary for the Solution and/or the Service, and to call on any intermediate and third-party service provider of their choice without having to inform the Merchant in advance, and subject to remaining the sole contact of the Merchant for all matters relating to the proper performance of the Agreement.

ARTICLE 20. ASSIGNMENT OF THE CONTRACT

The Parties may not transfer or assign all or part of their rights and obligations under the Agreement, or the Agreement itself, to a third party, without the prior written consent of the other Party, who may not refuse or delay it without valid reason.

Any transfer or assignment made in breach of this clause shall be considered null, void and without effect.

ARTICLE 21. ADDRESS FOR SERVICE

21.1. For the performance of the Agreement, each of the Parties elects domicile at the address of its registered office.

21.2. The Service Provider draws the Merchant's attention to the need for the latter to communicate to it a valid main email address, and to inform it as soon as possible of any change in this address.

21.3. Each of the Parties undertakes to regularly consult the email addresses, any email that has not been rejected by the recipient's email server being deemed to have been read by its recipient within twenty-four (24) hours of its sending.

ARTICLE 22. NON-SOLICITATION

The Merchant is prohibited from poaching or hiring the employees of the Service Provider throughout the term of the Agreement and for a period of one (1) year from the end date of the Agreement, unless expressly agreed between the Parties. In the event of non-compliance by the Merchant with this obligation, the latter undertakes to pay the Service Provider a penalty equal to twenty-four (24) months of the last gross salary of the person(s) in question.

ARTICLE 23. GOVERNING LAW, MEDIATION AND COMPETENT COURTS

23.1. This Agreement is governed by the laws of France and the competent courts of Paris.

23.2. Prior to any litigation, the Parties will attempt, in good faith, to amicably resolve their disputes related to the validity, performance and interpretation of the Agreement. The Parties must meet in order to compare their views and make any useful findings to enable them to find a solution to the conflict between them. In the event of a dispute, the Parties shall endeavour to reach an amicable agreement within thirty (30) days of notification by one of them of the need for an amicable agreement, by registered letter with acknowledgement of receipt.

23.3. If no amicable agreement is reached, the Parties agree to submit their dispute under the aegis of the mediation and arbitration centre of the Chamber of Commerce and Industry of Paris. The Parties shall organise the mediation in accordance with the mediation rules in force. The Parties undertake to share equally the costs of such mediation, while retaining the costs and fees of their respective lawyers.

23.4. The Parties intend to confer on this procedure, provided for in the above subparagraphs, full contractual force. By common will of the Parties, legal action brought by one of them that ignores this procedure shall be inadmissible.

23.5. It is also agreed that, notwithstanding the provisions of this Article, the Parties retain the right to bring proceedings before the court of summary jurisdiction under Articles 145-872 and 873 of the French Code of Civil Procedure.

23.6. If mediation fails, any dispute arising out of this Agreement shall be submitted to the competent courts of Paris.

ARTICLE 24. General

24.1. Non-waiver The fact that each of the Parties does not require at any time the strict execution of a provision of this Agreement may not be considered as constituting a waiver, whatever it may be, of the execution thereof.

24.2. Independence of the Parties The Parties expressly declare that they act independently to carry out their own business activities. Nothing in this Agreement constitutes an employment, agency, commission, partnership or joint venture relationship. Neither Party has any authority to make any commitments on the other Party's behalf.

24.3. Single Agreement. This Agreement and its appendices constitute a single legal instrument, namely the sole agreement validly binding the Parties. Consequently, any commitment or communication, oral or written, prior to the signing of this Agreement, not expressly included in this Agreement or its appendices, is cancelled and void.

24.4. Severability If any non-essential clause of this Agreement

is declared in whole or in part null or void by a judicial or other decision, this shall not affect the other clauses which shall continue to have full effect. The Parties agree to replace any clause declared invalid or ineffective by another valid and effective clause, striving for the latter to have effects as close as possible to those of the replaced clause.

24.5. **Reference** The Merchant grants the Service Provider, during the performance of the Agreement, a non-exclusive, non-assignable and limited right to use the brand and/or the trade name that it uses primarily on the Site for the sole purpose of performing the Agreement and promoting the Service. This right of use does not entail any transfer of the right of ownership over the trademark or the Merchant's logo. Any other use of the trademark and/or the commercial name of the Merchant by the Service Provider will be the subject of a request sent in writing to the Merchant and must be authorized by the latter in writing, it being specified that in the event that the Merchant gives its authorization the aforementioned use must in all circumstances be in accordance with the instructions given by the Merchant

Exhibit 1 –Personal data processing

1. The Service Provider, as a sub-contractor, agrees to put in place all the necessary procedures to ensure confidentiality and maximum security.

1. Description of the Processing

2. The Service Provider will be required to process personal data in the context of the processing described below. The Merchant may at any time modify the description of these treatments and will notify the Provider.

1.1 Processing Activity

A) Know Your Customer Data Processing;

(B) Processing of data on card payment transactions;

C) Processing of customer relationship management data.

1.2 Term

Period during which the personal data collected are kept in the absence of any other retention period provided for by the applicable laws and regulations or imposed by a supervisory authority: five (5) years (compliance with the legal and regulatory requirements applicable to the sub-contractor in terms of anti-money laundering and terrorist financing).

1.3 Nature and purpose of the processing operations

For the nature of the processing: Processing carried out on Personal Data or on sets by Data Regulations are: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure and destruction.

For the purposes of the processing: (a) the processing consists of the collection, analysis and retention of data intended to know the customer, and in particular to fulfil our legal obligations relating to the fight against money laundering and the financing of terrorism; (b) the processing consists of the collection, transmission and retention of secure Card data allowing the execution of payment transactions within the context of the Services, in particular the execution of SEPA direct debits, credit transfers and the acquisition of payment orders via Card and other regulated means of payment; (c) the processing consists of the collection and retention of the data of the customer's employees used within the context of the customer relationship.

1.4 Types of Personal Data processed

1) The data processed in the context of customer knowledge (as required by the Statutory Regulations) are the following: surname, first name, date of birth and place of birth of the effective manager(s) of the Merchant.

The Service Provider also collects and maintains a valid identity document to verify the identity information collected.

2) The data of the Merchant's employees collected and stored as part of the customer relationship are: surname, first name and professional contact details (telephone and email)

1.5 Categories of data subjects

1) The processing concerns any legal or contractual representative of the Merchant as well as its sales outlet(s). It also concerns any beneficial owner of the Merchant (i.e. any person holding at least 25% of the capital of the Merchant or any other minimum holding threshold provided for by a Statutory Regulation).

2) The processing concerns Payers who pay via their Cards to the Merchant.

3) the processing concerns any employee of the Merchant (employee, manager, executive).

2. Warranty

3. The Service Provider guarantees the Merchant compliance with the legal and regulatory obligations incumbent on it under the regulations on data protection and compliance with its obligations under this appendix.

4. The Merchant will carry out any formalities required by the data protection regulations with a data control authority and will inform, where appropriate, the data subjects concerned by the processing of personal data.

3. Obligations of sub-contractors

5. The Service Provider undertakes to take all necessary measures to ensure compliance by itself and its staff with its obligations and in particular to:

- not process, consult the data or files for purposes other than the performance of the services it performs for the Merchant hereunder;

- not process, consult the data outside the framework of the documented instructions and authorisations received from the Merchant, including with regard to transfers of personal data to a third country or an international organisation, unless the Service Provider is required to do so by virtue of a mandatory provision resulting from Community law or from the law of the Member State to which it is subject; in this case, the Service Provider shall inform the Merchant of this legal obligation before processing the data, unless the law concerned prohibits such information on important grounds of public interest;

- not to insert foreign data in the files;

- take all measures to prevent any misuse, or malicious or fraudulent use of Personal Data and files;

- not carry out any statistical study on the data or processing other than that requested by the Merchant;

- immediately notify the Merchant of any modification or change that may have an impact on the processing of personal data;

- inform the Merchant immediately if, in its opinion, an instruction violates the Data Protection Regulations.

6. The Parties agree to define the concept of "instruction" as applicable only when the Service Provider is acting under the Agreement;

7. In addition, the Service Provider shall refrain from:

- the consultation and processing of data other than those covered by this Agreement, even if access to this data is technically possible;

- disclosing, in any form whatsoever, all or part of the data used;

- taking a copy or storing, whatever the form and purpose, all or part of the information or data contained in the media or documents entrusted to it or collected by it during the performance of this agreement, except in the cases covered by this agreement.

8. The Service Provider undertakes to take all appropriate measures to ensure that natural persons acting under its authority and having access to personal data do not process them, except on instructions from the Merchant, unless they are required to do so by a mandatory provision resulting from Community law or from the law of a Member State of the European Union applicable to the processing operations covered herein. The Service Provider shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

9. It acknowledges and agrees that it may only act in respect of the processing of the data and files to which it may have access in accordance with this appendix and the Agreement.

4. Safety

10. The Service Provider undertakes, in accordance with the data protection regulations, to take all appropriate precautions with regard to the nature of the data and the risks presented by the processing, to preserve the security of the data in the files and in particular to prevent any distortion, alteration, damage, accidental or unlawful destruction, loss, disclosure and/or any access by third parties not previously authorised.

11. It implements all appropriate technical and organizational measures to protect personal data, taking into account the state of knowledge, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks, whose degree of probability and seriousness varies, to the rights and freedoms of natural persons, in order to guarantee a level of security appropriate to the risk.

12. The means implemented by the Service Provider to ensure the security and confidentiality of the data are agreed with the Merchant.

13. The Service Provider undertakes to maintain these means throughout the performance of the Agreement and, failing this, to inform the Merchant immediately.

14. In any event, the Service Provider undertakes, in the event of a change in the means intended to ensure the security and confidentiality of the data and files, to replace them with means of superior performance. No change can lead to a decrease in the level of security.

5. Data breaches

15. The Service Provider undertakes to notify the Merchant, as soon as possible after becoming aware of any personal data breach leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of Personal Data transmitted, stored or otherwise processed, or unauthorised access to such Data.

16. This notification must be sent to the person designated as the point of contact, by telephone and e-mail, and then confirmed by registered letter with acknowledgement of receipt. It must specify the nature and consequences of the data breach, the measures already taken or proposed to remedy them and the persons from whom additional information can be obtained, and where possible, an estimate of the number of persons likely to be affected by the breach in question.

17. In the event of a data breach, the Service Provider undertakes to carry out all appropriate investigations into breaches of the protection rules in order to remedy them as soon as possible and reduce the impact of such breaches on the data subjects. The Service Provider agrees to inform the Merchant of its investigations on a regular basis.

18. The Service Provider undertakes to actively collaborate with the Merchant so that the Parties are able to meet their regulatory and contractual obligations. The Merchant alone, as Data Controller, is responsible for notifying this Data Breach to the competent supervisory authority and, where applicable, to the Data Subject.

6. Subcontracting

19. The Service Provider may only subcontract, within the meaning of the data protection regulations, all or part of the services, in particular to a country which is not located in the European Union, after having obtained the prior written and express consent of the Merchant.

20. In the event that the Service Provider has been authorised to subcontract the services covered by the Agreement, it undertakes to:

- inform and sign with its sub-processor a written agreement referring to the Agreement and this Annex, and imposing on the sub-processor the same data protection obligations as those set out in this Appendix and the Agreement;

- impose on its sub-contractor all obligations necessary to ensure that the confidentiality, security and integrity of the data are respected, and that said data cannot be transferred or leased to a third party, whether free of charge or not, nor used for any purpose other than those defined in this appendix and in the Agreement;

- provide the Merchant with a copy of the agreement with its sub-contractor (s) and, failing this, a description of the essential elements of the agreement, including the implementation of obligations relating to the protection of personal data;

- in the case of general written authorisation, inform the Merchant of any intended changes concerning the addition or replacement of other sub-contractors, in order to allow the Merchant, if necessary, to object to such changes;

- keep at the disposal of the Merchant a list of the sub-processor (s) involved in the processing of personal data.

21. The data processed in execution of the Agreement may not be the subject of any disclosure to any third party, including the sub-contractors of the Service Provider, except in the cases provided for in this appendix and in the Agreement or those provided for by a provision of law or regulation.

22. If the Sub-Processor fails to fulfil its Personal Data protection obligations, the Service Provider shall remain fully liable towards the Client for the performance by the Sub-Processor of its obligations.

7. Cross-border data flows

23. In the event of transfer of Personal Data to a third country, not belonging to the European Economic Area, the Service Provider must obtain the prior written consent of the Merchant. If this Agreement is given, the Service Provider agrees to co-operate with the Merchant to ensure that:

- compliance with the procedures for complying with the Data Protection Regulation, for example in the event that authorisation from CNIL is required;

- where necessary, the conclusion of one or more agreements to regulate cross-border data flows. The Service Provider undertakes in particular, if necessary, to sign such agreements with the Merchant and/or to obtain the conclusion of such agreements by its subsequent sub-contractors. To this end, it is agreed between the Parties that the standard contractual clauses published by the European Commission will be used to regulate cross-border data flows.

8. Keeping of the register

24. The Service Provider, as a processor, undertakes to maintain a record of all the categories of processing activities carried out on behalf of the controller, in accordance with the provisions of the General Data Protection Regulation. The Service Provider will give the Merchant access to the register on request.

9. Data retention

25. At the end of the Agreement, and unless otherwise required by Community law or the law of a Member State of the European Union applicable to the processing operations covered by this Agreement, the Service Provider undertakes to destroy all manual or computerized files storing the information collected, after ensuring that the Merchant has access to this information.

26. In the event that Community law or the law of a Member State requires the retention of personal data, the Service Provider shall inform the Merchant of this obligation.

27. The Service Provider undertakes to provide the Merchant, on first request, with a certificate of deletion of personal data.

10. Audits

28. At the request of the Merchant, the Service Provider must draw up a certificate or transmit any information necessary to demonstrate that the rules provided for in this appendix have been complied with.

29. The Merchant reserves the right to carry out any checks that it deems useful to establish compliance with the aforementioned obligations, and in particular by carrying out a security audit with the Service Provider or directly with a subsequent sub-contractor.

30. The Service Provider undertakes to respond to the Merchant's audit requests made by itself or by a trusted third party that it has selected, recognized as an independent auditor, that is to say independent of the Service Provider, having an adequate qualification, and free to provide the details of its remarks and audit conclusion to the Merchant.

31. The audits must allow an analysis of the Service Provider's compliance with its obligations under this Annex and the Agreement, as well as under the regulations on data protection. In particular, they must make it possible to ensure that the security and confidentiality measures put in place cannot be circumvented without this being detected and notified.

11. Cooperation

32. The Service Provider agrees to cooperate with the Merchant to allow:

- the management of requests from data subjects for the exercise of their rights and in particular their right of access to data concerning them. If a data subject were to contact the Service Provider directly to exercise its rights of access, rectification, deletion and/or opposition or for any other request related to the protection of personal data, the Service Provider will communicate to the Merchant within a maximum of 72 hours the requests that have been received. The Service Provider may only respond to the request of a data subject on the instructions of the Merchant;

- the carrying out of any impact assessment that the Merchant may decide to carry out in order to assess the risks that a processing operation poses to the rights and freedoms of individuals and to identify the measures to be implemented to deal with these risks, and the consultation of the supervisory authority;

- more generally, compliance with the Merchant's obligations under the IT regulations and freedoms, such as in particular its obligations to notify the supervisory authority and to communicate a data breach to the data subjects.

33. In the event of an inspection by a competent supervisory authority, the Parties agree to co-operate with each other and with the supervisory authority.

34. In the event that the inspection concerns only the Processing implemented by the Service Provider as Data Controller, the Service Provider shall be responsible for dealing with the inspection and shall refrain from communicating or reporting the Merchant's Personal Data.

35. In the event that an inspection carried out at the Service Provider's establishment concerns the Processing carried out on behalf of the Merchant, the Service Provider agrees to inform the Merchant immediately and to make no commitment on its behalf.

36. In the event of an inspection by a competent authority at the Merchant's relating in particular to the Services delivered by the Service Provider, the Service Provider undertakes to co-operate with the Merchant and to provide it with any information that it may need or that may prove necessary.

Appendix 2 – Security repository

1. Security standard

The Merchant, in its capacity as acceptor, represents that it has read and unreservedly accepts the requirements constituting the acceptor security repository reproduced below:

Manage the security of the commercial and acceptance system within the company	To ensure the security of payment transaction data and in particular, sensitive personal data and payment data relating to the Cardholders' cards, an organisation, procedures and responsibilities must be established. In particular, a person responsible for the security of the commercial and acceptance system must be appointed. It is responsible, inter alia, for the application of the legislation on the protection of personal data and banking secrecy in the context of their use and their environment. Holders of rights to use the information and the system must be identified and are responsible for granting access rights to the system. Compliance with the safety requirements relating to the commercial and acceptance system must be checked. An organisation responsible for handling security incidents, monitoring them and recording them must be established.
Manage human and internal activity	The obligations and responsibilities of the Personnel regarding the use of banking and confidential data, its storage and its circulation internally or externally must be established. The same applies to the use of workstations and the internal network as well as the Internet. The obligations and responsibilities of the Personnel regarding the protection of bank and confidential data must be established. All these rules must apply to all the personnel involved: employees of the company and third parties. Personnel must be made aware of the risks involved, including the disclosure of confidential information, unauthorised access to information, media and documents. Staff must be regularly made aware of the special risks associated with the use of IT resources (networked workstations, servers, access from or to the Internet) and in particular, the introduction of viruses. Personnel should receive appropriate training on the correct use of the operating system and the commercial and acceptance application system.
Manage access to premises and information	Any device (network equipment, server, etc.) which stores or processes data relating to a payment transaction and, in particular, sensitive payment data linked to the Cardholder's card must be hosted in a secure premises and meet the requirements laid down by the rules and recommendations of the CNIL. Small sensitive computer equipment or media must be made inaccessible to third parties during periods of non-use. In particular, backup cartridges must be stored in a safe. In the event that these small sensitive computer equipment or media are no longer operational, they must be destroyed and proof of their destruction must be established. The policy on access to sensitive premises must be formalised and procedures established and controlled.
Ensuring the logical protection of the commercial and acceptance system	Security rules relating to access and egress to and from the commercial and acceptance system shall be established and their observance shall be monitored. Only the server supporting the commercial application must be accessible by Internet users. The client database server as well as the server hosting the acceptance system must only be accessible by the front-office commercial server and only via a firewall. Internal access to these same servers by both users and administrators must be through the firewall. The network architecture shall be organised in such a way that the defined security rules are implemented and monitored. The firewall must be systematically updated when vulnerabilities are identified on its software (firewall software and operating software) and remediable. The server supporting the firewall must have an integrity control tool. The firewall must ensure that accesses and access attempts are recorded in an audit log. This must be analysed daily.
Control access to the commercial and acceptance system	The principle of authorizing the use of the system must be defined and based on the notion of access of user classes to resource classes: definition of user profiles and rights granted. Responsibilities and roles for attribution, use and control must be identified. In particular, the associated profiles, rights and privileges must be validated by the owners of the information and the commercial and acceptance system. The rights of users and administrators and their privileges must be managed and updated in accordance with the rights management policy.
Manage authorized access to the commercial and acceptance system	No rights may be acquired without proper authorisation procedures. The authorisations given must be archived and checked regularly. In addition to customer access, any access to the commercial and payment system must be based on identification and authentication.

	Identification must be personal, including for administrators and maintenance personnel. The rights granted to them must be limited to the operations authorized to them. The use of identification codes assigned to groups or functions (technical processes such as automatic feeding of antiviral signatures) is only allowed if it is appropriate for the work performed. Changes in the situation (change of position, departure, etc.) of staff must systematically result in control of the access rights allocated. The removal of access rights must be immediate in the event of the departure of a person. Access control must be provided at the network level by the firewall, at the system level by the operating systems of the machines accessed and at the application level by the application software and by the database manager. Access attempts shall be limited in number. Passwords must be changed regularly. Passwords must contain at least 8 characters and include special characters.
Monitor access to the commercial and acceptance system	Accesses and attempts to access the system must be recorded in audit logs. The record must include at least the date and time of access (or attempt) and the identification of the actor and the machine. Special operations such as changing configurations, changing security rules, using an administrator account must also be recorded. Registration systems must have at least the firewall function for the system supporting the customer database as well as the system supporting the Payments database. Audit logs must be protected from unauthorized deactivation, modification or deletion. Responsibilities and roles for auditing recorded data are identified. This is to be done on a daily basis.
Controlling the introduction of harmful software	Procedures and management responsibilities relating to virus protection and the recovery of data and software in the event of a virus attack must be defined and formalized. Installation and regular updating of virus detection and removal software must be carried out on all machines with access to the commercial and acceptance system. Anti-virus verification shall be performed daily on all machines.
Apply security patches to operating software	Security patches must be systematically applied to security equipment and front-end application servers to fix the code when vulnerabilities could allow unauthorized and unseen access. These corrections must be applied on the basis of a formal and controlled procedure.
Manage operating software version changes	A procedure for installing a new version must be established and controlled. This procedure must provide for, among other things, tests of non-regression of the system and a reversal in the event of malfunction.
Maintain the integrity of application software related to the commercial and acceptance system	Responsibilities and procedures for operational changes to applications should be established. Changes to application software must be precisely defined. The change request must be approved by the System Functional Owner. New versions of application software must be systematically submitted to acceptance and approved by the functional manager of the application concerned before any release into production.
Ensuring the traceability of technical operations (administration and maintenance)	The technical operations carried out must be recorded chronologically, in a logbook to allow for the timely reconstruction, review and analysis of treatment sequences and other activities related to these operations.
Maintain the integrity of commercial system and acceptance information	The protection and integrity of the elements of the payment transaction must thus be ensured when they are stored and when they are routed on networks (internal or external). The same applies to the secret elements used to encrypt these elements. The safety record specific to the commercial and acceptance system must describe the means put in place to meet this requirement.
Protecting the confidentiality of bank data	The sensitive payment data linked to the cardholder's Card may only be used to execute the payment order and to process complaints. The visual cryptogram of a Cardholder must not be stored by the Merchant. Banking and personal data relating to a payment transaction, and in particular sensitive payment data linked to the cardholder's Card, must be protected when they are stored and when they are routed on the networks internal and external to the hosting site in accordance with the provisions of the French Data Protection Act and the recommendations of the CNIL. The same applies to the Merchant's authenticator and the secret elements used to encrypt. The safety record specific to the commercial and acceptance system must describe the means put in place to meet this requirement.

Protect credential confidentiality - credentials of users and administrators	The confidentiality of credentials must be protected when they are stored and circulated. It should be ensured that administrators' authentication data cannot be reused. For external maintenance, the passwords used must be systematically changed following the intervention.
PCI DSS Standard	The PCI DSS standard to which the Merchant is bound (as far as it is concerned) must be consulted by the Merchant and is available at the following address: https://www.pcisecuritystandards.org/security_standards

In the event that the Equipment is equipped with "contactless" technology, the Merchant must meet the following operating conditions:

- Equipment with "contactless" technology allows for the rapid payment of goods or services by Cardholders with a remote reading of the Card and without entering the PIN;
- In all circumstances, Merchants must comply with the guidelines that appear on the Equipment;
- The maximum unit amount of each payment transaction in "contactless" mode is limited to 30 euros (or, if applicable, any other amount subsequently decided by the Payment Network). Beyond this maximum unit amount, the conditions of the payment transaction prescribed by the Payment Networks in the Agreement remain unchanged. When a certain number of successive payments in contactless mode is reached, the Merchant may have to switch to contact mode even for a transaction of an amount lower than the maximum unit amount of a transaction in "contactless" mode.
- For Cards, when the chip requests it from the Equipment, have the Cardholder enter his PIN code in the best conditions of confidentiality. Proof of the PIN being entered is provided by the certificate which must appear on the purchase receipt.
- In the event of a "contactless" transaction enabled by the Equipment, the payment transaction is guaranteed even if the PIN is not verified, subject to compliance with all other security measures to be taken by the Merchant.

2. Audit procedure

The audit procedure below required by the GIE CB Payment Network may be modified at any time by the latter.
GIE CB is responsible for auditing all participants in the "CB" system with regard to compliance with community security rules. The Merchant, in its capacity as an acceptor, must respond favourably to any request made by GIE CB in this regard and give its auditors the best possible welcome, as well as implementing any recommendations made.
In this respect, CB EIG defines the terms and conditions of these audits and guarantees their regularity.

There are two types of missions:

- Annual or multi-year audits (preventive audits). These missions are planned on an annual basis. They focus on internal control within the audited entities, particularly with regard to compliance with procedures relating to CB approvals and CB security requirements. They may also cover a specific topic common to the entire CB system;
- Specific audits (corrective audits): these are triggered as soon as incidents, malfunctions or payment fraud are observed in the CB system or to check compliance with a particular security measure ("field" audits).

Concerning the audit procedure:

- Preparation - the mission is (i) announced by a letter, (ii) defined (the mission objectives with identification of the most important risks), (iii) planned (evaluation of the audit duration), and (iv) documented (knowledge of the activity, previous audit reports, reference documents).
- Implementation - The controls and analyses are referenced and written down, and their results give rise to the drafting of findings.
- Recommendations - recommendations or actions to be taken are followed up, and their implementation must take place within the given deadlines.

Appendix 3 - Services Description

1. PREAMBLE

Capitalised terms not defined in this Appendix shall have the meanings given to them in this Agreement.

This appendix relates to the Acquiring Services (as defined hereunder).

Acquiring services are, within the meaning of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, payment services provided by a payment service provider (in this case, Market Pay) contracting with a payee (in this case, the Merchant) to accept and process payment transactions, which results in a transfer of funds to the payee ('**Acquiring Services**').

The Acquiring Services provided by Market Pay are intended to ensure the processing of the authorisations of Card Payment Transactions and to ensure their financial settlement for the benefit of the Merchant on the Bank Account.

The Acquiring Services finance Transactions carried out in euros with Cards bearing the Payment Networks brand (in particular Visa and Mastercard and CB).

Acquiring Services allow the financing of all physical acceptance activities at points of sale, in a "*card present*" context:

- Site Transactions: including in particular Payment Transactions, and Refunds;

The Acquiring Services are responsible for:

- the management of exchanges with the acceptance and pre-acquiring bricks in a "*card present*" context;
- the management of remote configuration of the acceptance points related to the Acquiring Services (risk management ceilings, etc.);
- exchanges with international and domestic Payment Networks (authorisation, clearing, fraud, Non-payments and dispute management);
- management of electronic banking contracts.

2. SCOPE COVERED

Market Pay carries out the acquirer processing of the flows for the Payment Networks, specified in the Form, receives the payment and transfers it to the Merchant.

3. Prerequisites

3.1 The use of a Bank Account

The acquiring of Payment Transactions by Market Pay (who acts as **acquirer**) requires the opening of a Bank Account opened in the name of the Merchant (who acts as **acceptor**) in the books of a credit institution established within the European Union.

Amounts received by Market Pay and resulting from the acquiring of Payment Transactions accepted by the Acceptor are credited to the Bank Account.

3.2 Use of an acceptance system

The Merchant must have and use an acceptance system approved by the Payment Networks that it wishes to use for acquiring its Transactions.

3.3 Integration Architecture

3.3.1 Integration of physical acceptance services

Market Pay Acquiring Services may be integrated:

- either with the physical acceptance services provided by Market Pay Tech;
- or with an acceptance service that interfaces as defined between the Merchant and Market Pay.

3.3.2 Information System Integration

The Service Provider provides the Merchant on a daily basis with the *reports* necessary to reconcile the Purchases made by the Merchant's Payers with the Card Transactions made by these same Payers.

4. ADDITIONAL OBLIGATIONS OF THE MERCHANT AS ACCEPTOR

In addition to the obligations set out in clause 4.2 of the Agreement, the Merchant agrees to make the following commitments, as they are in particular required by the Payment Networks:

The Merchant undertakes not to hold the Service Provider liable for any commercial dispute that may arise with the Payer and whose nature is foreign to the subject matter of the Agreement.

The Merchant must comply with the following PCI-DSS requirements:

- write in its contractual relations with third parties, such as technical service providers or subcontractors involved in the processing and storage of data related to the use of the Cards, that the latter undertake to comply with the PCI-DSS requirements available on the pcisecuritystandards.org website, and accept that the audits be carried out on their premises and that the reports may be communicated;
- declare the aforementioned technical service providers or subcontractors to Market Pay on an annual basis and in the event of a change;
- read the PCI-DSS Security Guidance Document regarding the protection of Electronic Payment Sensitive Data available on pcisecuritystandards.org and make every effort to comply with its requirements;
- allow Market Pay to carry out on its premises or those of its service providers, verification by an independent third party of compliance with the Agreement as well as the PCI-DSS security requirements available on the pcisecuritystandards.org website. This verification, called "*audit procedure*", may occur in the event of suspicion of fraud or compromise of data as soon as the Agreement is concluded and/or during its validity;
- in the event that the report delivered to the Parties by the independent third party at the end of the audit procedure reveals one or more breaches of the Agreement or the aforementioned requirements, the Payment System may request Market Pay to proceed with the suspension of the Service in the Site concerned; and
- inform Market Pay immediately in the event of abnormal operation of the acceptance system and any other anomalies (non-application of payment order security procedures, malfunction of the acceptance system, etc.).

Merchant acknowledges and agrees that in the event of dispute, unpaid or abnormally high fraud (under the rules of the Payment Systems) or abnormal use of lost, stolen or counterfeit Cards or any other breach under the Agreement, the Payment Systems will alert Market Pay.

In this case, Market Pay warns the Merchant who undertakes, on the basis of the information previously transmitted by Market Pay, to implement within the time limit set by Market Pay (according to any time limit dictated by the Payment Systems), the measures intended to justify the cause or to eliminate them.

In the event that the Merchant does not implement the aforementioned measures or does not provide the necessary supporting documents, the Payment Systems may apply Penalties to Market Pay, calculated on the same basis regardless of the acquirer, in particular:

- in the event of exceeding a certain number of non-payments and/or a rate of non-payments generated with the Merchant;
- in the event of exceeding a certain number of frauds and/or a rate of frauds generated with the Merchant;
- when it exceeds a certain number of credit invoices (refund of items);
- in the event of the performance of any illegal activity or activity not in accordance with the rules laid down by the Payment Systems or for any other reason as a result of the Payment Transactions generated at the Merchant.

To this end, the Merchant expressly and irrevocably agrees to bear all of these Penalties. These Penalties will be invoiced to the Merchant and settled within a period which must not exceed ten days.

For cases where the Merchant's Business consists of the rental of goods and services, the Merchant agrees to:

- not use the Card to provide a security deposit (or any other form of security);
- assign, on the occasion of the initialisation of the Payment Transaction for the rental of goods and services, a file number independent of the Card number;

- obtain the Payer's acceptance to be debited with the amount of the actual costs of the rental, the estimated amount of which is itself specified. The Merchant associates a file number with the rental Payment Transaction thus initialized;
- use the Equipment or the acceptance system equipped with the "*Payment for the rental of goods and services (PLBS)*" service extension in accordance with the specifications in force;
- systematically obtain an authorization in an amount identical to that known and accepted by the Payer;
- after the execution of the payment transaction, close the Payment Transaction by searching via the file number, the Payment Transaction initialized upon the provision of the good and finalize it for the final amount of the actual costs known and accepted by the Payer which must not exceed the value of the amount authorized by the latter.

5. ADDITIONAL OBLIGATIONS OF MARKET PAY

Market Pay undertakes to make available to the Merchant, access to the authorisation acquiring system.

Market Pay agrees to provide Merchant with information on the amount of Merchant Service fees, interchange fees and Payment System Fees applicable to each Card category and each brand of Payment Networks.

By default, Payment Transactions are invoiced according to a grouped pricing regardless of the brands, payment applications, categories of Cards and regardless of the interchange commission rate applicable to the Payment Transaction. However, the Merchant may request that these be invoiced separately;

- communicate to the Merchant on a durable medium the following information relating to the Payment Transactions linked to a Card and executed during the period that has elapsed:
    - the reference enabling it to identify the Payment Transaction;
    - the amount of the Payment Transaction in the currency in which its account is credited;
    - the amount of all Fees applied to the Payment Transaction, the amount of the service fee paid by the Merchant and the amount of the interchange fee.

The information relating to the invoicing grouped by brand, application, category of Cards and by interchange commission rate applicable to the Payment Transaction is called "RMFEC" (monthly statement of collection fees per Card) and is submitted monthly;

- provide at the start of each year a statement called "Annual Statement of Card Collection Fees (RAFEC) ", which summarizes for the past year the Payment Systems Fees, the service fees paid by the Merchant and the interchange fees in force by brand and by Card category.

For all intents and purposes, Market Pay informs the Merchant that the interchange fee rates charged by the various Payment Systems are public and can be consulted on the following websites:

- For VISA: www.visaeurope.com/about-us/interchange-fees
- For Mastercard: www.mastercard.com
- For the Groupement des Cartes Bancaires are public and can be consulted on the website: www.cartes-bancaires.com

6. ACQUIRING SERVICES

6.1 Acceptor Web Portal

Aim of the Service	This Service provides a comprehensive and analytical view of transactions by period. It provides access to accounting files facilitating the control and validation of charges levied by acquirers. It allows the creation of customized *reports* and the possibility of configuring the acquirer rates via dynamic management of the applied rates (creation, modification, deletion). This service also makes it possible to report and monitor incidents.

Prerequisites	- Have an administrator declared by a super administrator of Market Pay; - The administrator manages user rights by profiles.

6.2 Provisioning service for acquirer parameters

Aim of the Service	This Service provides the acceptance system with real-time acquirer parameters (BIN tables, AID list, authorisation threshold, etc.). The complete list of acquirer parameters is described in the specification documents.
Prerequisites	An acceptance system that uses the acquirer WS (defined by the Service Provider) to retrieve the acceptor parameters. An acceptance system which itself remotely configures the payment terminals once the acquirer parameters have been retrieved.

6.3 Acquirer permissions ("Acquirer authorization Server" SAA)

Aim of the Service	The acquirer authorisation Service provides the necessary processing to handle applications for x-Pay wallets, chip, magnetic strip, e-commerce and MOTO (Mail Order / Telephone order) authorisations from the accepting system. To do this, it is connected to the various Payment Systems whose cards are accepted by the acceptor system.
Prerequisites	Compliance with acceptor/acquirer protocols defined between Merchant and Market Pay *Provisioning* service for acquirer parameters.

6.4 Cash Announcement

Aim of the Service	This Service allows to inform the Merchant of the amount to be financed each business day.
Prerequisites	Compliance with financing protocols defined between the Merchant and Market Pay Compliance with the acceptor / acquirer protocols defined between the Merchant and Market Pay; *Provisioning* service for acquirer parameters.

6.5 Financing

Aim of the Service	This Service allows to finance the Merchant for Card Transactions carried out on its acceptance system.
Prerequisites	Compliance with financing protocols defined between the Merchant and Market Pay Compliance with the acceptor / acquirer protocols defined between the Merchant and Market Pay; Compliance with the hourly cut-off for the delivery of flows before 10.30 p.m. or defined between the Merchant and Market Pay. *Provisioning* service for acquirer parameters.

6.6 Monitoring

Aim of the Service	This Service makes it possible to supervise the proper execution of Site Transactions, to detect incidents and, where appropriate, to alert the Merchant.
Prerequisites	Delivery of the Service Provider's monitoring tool.