General Terms of Service

GREENWAY SAS

PREAMBLE

GREENWAY SAS (hereinafter the "Company") offers its professional clientele a comprehensive set of services (hereinafter "Services") tailored to the specific needs of their clients, as well as the provision of payment cards.

These General Terms and Conditions of Service (hereinafter "General Terms", "Contract" or "Framework Contract") apply when a professional Client (hereinafter "Client(s)") has chosen to subscribe to one or more services and/or payment cards offered by the Company.

The Company, in partnership with Enfuce License Services Ltd (hereinafter the "Issuer"), provides its professional Clients with a Mastercard or Visa payment card (hereinafter the "Card") to facilitate the settlement of professional expenses incurred by their employees (hereinafter the "Cardholder(s)" or "User(s)"). The Card will be issued within the framework of the Framework Contract subscription and in accordance with the Issuer's General Terms (Annex 10).

The Issuer is authorised as a payment institution by the Finnish Financial Supervisory Authority to execute payment operations, notably under point 4 of Annex I of Directive (EU) 2015/2366 (PSD2). This regulatory framework, which governs the provision of payment services by the Issuer within the European Economic Area, is distinct and independent from the legal qualification of the commercial relationship between the Company and the Client, which is governed by French law applicable to business-to-business relations.

Within the commercial relationship established by this Framework Contract, the Company grants the Client, on an ancillary basis to the Services and in consideration of the flat-rate pricing set out in Annex 1, a Deferred Payment facility for settlement of Transactions carried out by means of the Card. This Deferred Payment facility, non-onerous within the meaning of Article L.313-1 of the French Monetary and Financial Code, constitutes a commercial settlement arrangement granted under the conditions of Article L.511-7, I, 1° of the same Code. It shall not exceed sixty (60) days from the date of invoicing.

The regulatory qualifications applicable to the Issuer under PSD2 and those applicable to the Company under the French Monetary and Financial Code are independent of one another: they respond to distinct legal logics — the former concerning the execution mechanics of payment operations covered by the Issuer's authorisation, the latter concerning the legal nature of the settlement arrangements granted by the Company to the Client. The provision of the payment service by the Issuer does not confer on the Company any status as a credit institution, financing company or agent of any such institution.

ARTICLE 0 — DEFINITIONS

In these General Terms, the following words and expressions shall have the meaning set out below, unless the context requires otherwise:

Term / Expression	Meaning
Acceptor(s) / Supplier(s) / Merchant(s)	Any third-party legal entity or natural person providing a service to the Client in exchange for monetary payment.
Annex(es)	Contractual document(s) attached to these General Terms.
Card	Payment card under the Mastercard or Visa network.
Client(s)	The professional client signing these General Terms.

Term / Expression	Meaning
General Terms	This contract governing the relationship between the Company and the Client.
Framework Contract	Understood as the combination of the General Terms and the Annexes.
Issuer	Enfuce License Services Ltd, a company incorporated under Finnish law with its address at Metsänneidonkuja 12, 02130 Espoo, Finland, email issuing.support@enfuce.com. Enfuce is registered in the Finnish trade register under number 2992502-3 and is authorised as an electronic money and payment institution. Enfuce is supervised by the Finnish Financial Supervisory Authority, Snellmaninkatu 6, 00101 Helsinki, tel. +358 9 183 51, finanssivalvonta(at)finanssivalvonta.fi, acting as processor for the Company under the Framework Contract for the processing of personal data, and as principal for the issuance of Cards.
Deferred Payment	Commercial settlement arrangement granted by the Company to the Client for the payment of Transactions carried out by means of the Card, in accordance with Article L.511-7, I, 1° of the French Monetary and Financial Code. The Deferred Payment is strictly ancillary to the Services, non-onerous within the meaning of Article L.313-1 of the same Code, fully covered by the flat-rate pricing set out in Annex 1, and does not give rise to any interest charges or fees proportional to the amount or duration of the deferral. Its duration shall not exceed sixty (60) days from the date of invoicing.
Transaction	Any payment operation carried out by means of the Card or other accessories.
Blocking Payer Ceiling	Maximum amount that may be spent by the Client, set by the Company.
Cardholder(s) or User(s)	Natural person(s) attached to the Client and user(s) of the Services.
Client Manager	Natural person attached to the Client who is responsible for the Services.
Services	All services of the Greenway solution offered to the Client.
Site / Mobile Application	Web or mobile interface made available to the Client and Users.
Company	GREENWAY SAS.

ARTICLE 1 — PURPOSE OF THE GENERAL TERMS AND CONDITIONS OF SERVICE

The purpose of these General Terms and Conditions of Service is to govern the contractual relationship between the Parties, and in particular the terms under which the Company offers its Services to the Client.

These General Terms together with the Annexes below constitute the "Framework Contract" between the Company and the Client.

In the event of any divergence or contradiction between two or more of the aforementioned documents, the higher-ranking document shall prevail.

ARTICLE 2 — SUBSCRIPTION TO THE FRAMEWORK CONTRACT

The Client has taken full cognisance of the General Terms and of the other contractual documents referred to in Article 1.

In view, in particular, of possible extensions and improvements to the Services, the Company reserves the right to adapt or modify the content of the services offered. Any proposed amendment of these General Terms will be communicated to the Client by electronic means, at the latest two months before the envisaged date of application. The absence of any objection by the Client notified to the Company before the date of application of the amendments shall be deemed acceptance thereof. The new General Terms will also be presented to the Client and Users upon their first connection during the month following their entry into force. Should the Client disagree, it may, without any penalty, request termination of any optional subscriptions or of the Framework Contract and block its access under the conditions set out in Article 16. The Client is informed that use of the Site/Mobile Application and of the Services is exclusively reserved to professionals (within the meaning of point 3 of the preliminary article of the French Consumer Code), of legal age or emancipated minors, in possession of full legal capacity. The Client represents and warrants that the Users have such capacity. Legal information concerning the host and the Company, notably contact details and any information on share capital and registration, is provided in the legal notices of the Site and on the Mobile Application. The Company undertakes to maintain a host located in France.

Subscription to the Framework Contract is offered by the Company to professional clients for the use of the Card and ancillary Services.

The beneficiaries of the Framework Contract are the Client as designated at the head of these Terms, as well as:

- any other entity of the Client which, as of today or subsequently, directly or indirectly, controls, is controlled by, or is under common control with the Client. For the purposes of the Framework Contract, the term "control" and derivative expressions such as "controlled by" and "under common control" are defined (i) by reference to the provisions of Article L. 233-1 of the French Commercial Code, and/or (ii) include the direct or indirect power to manage, administer or determine the manner of managing or administering such entity by contract or otherwise; or
- any entity in which the Client holds, directly or indirectly, an interest and which has been designated as a beneficiary of the Framework Contract.

Any application to adhere to the Framework Contract must, on pain of inadmissibility, be accompanied by the supporting documents requested by the Company from the Client (compliance, financial documents, invoicing, etc.).

The Issuer, being a regulated entity subject to legal and regulatory provisions on anti-money laundering and counter-terrorist financing, is entitled to decline any application for adherence or to request from the Client and/or the Cardholder any additional supporting documents. In such case, including during the commercial relationship, the Issuer informs the Company, which in turn informs the Client and collects, where applicable, any additional supporting documents from the Client on behalf of the Issuer. Upon subscription to the Framework Contract, the Client designates at least one manager (hereinafter the "Manager") and, where applicable, a main user (hereinafter the "Principal User") of the Client Portal. If any of the previously designated person(s) changes, the Client undertakes to immediately inform the Company; such modification shall not give rise to the issuance of any document.

The Client undertakes to inform the designated persons of the arrangements for receiving, holding and delivering the Cards to Cardholders and of the resulting liability as specified in Annex 2, as well as of the articles concerning the protection of their personal data in Annex 4.

For the purposes of performing the Services, the Client also grants the Company a mandate (Annexes 4 and 5) to collect, in its name and on its behalf, data relating to Expenses and Vehicles in order to provide a smoother experience in connection with the performance of the Services.

Access to the Services and to the Deferred Payment is reserved to legal persons acting in a professional capacity within the meaning of point 3 of the preliminary article of the French Consumer Code. The Framework Contract is in no case subscribed by consumers, the provisions of Book III of the French Consumer Code on consumer credit not being applicable.

ARTICLE 3 — DESCRIPTION OF THE SERVICES OFFERED

3.1 Provision of Services

The Company offers its professional clientele a comprehensive set of services tailored to their specific needs and those of their clients, including the provision of payment cards. These various services are described in detail in Annex 2.

3.2 Settlement arrangements for Transactions

The Company grants the Client a Deferred Payment facility for the settlement of Transactions carried out by means of the Card. This Deferred Payment constitutes a commercial settlement arrangement, strictly ancillary to the Services provided by the Company. It does not constitute a credit transaction within the meaning of Article L.313-1 of the French Monetary and Financial Code, in the absence of any onerous consideration directly attached to the advance of funds, and is granted in accordance with Article L.511-7, I, 1° of the same Code.

The Deferred Payment is fully covered by the flat-rate pricing of the Services set out in Annex 1. No interest, fees proportional to the amount or duration of the deferral, or any other remuneration directly linked to the advance of funds is charged to the Client. The duration of the Deferred Payment shall not, in any event, exceed sixty (60) days from the date of invoicing.

The commercial receivables held by the Company against the Client in respect of invoiced Transactions may be assigned to Aria, in accordance with the conditions set out in Annex 11.

The Deferred Payment is granted solely as ancillary to the Company's commercial Services and may not be used on a stand-alone basis. It may not, in any event, be used for cash withdrawals or for transfers independent of a purchase of goods or services from an accepting merchant.

3.3 Issuance and Distribution of the Card

The Card is issued by the Issuer and distributed by the Company, acting in its own name and in the name and on behalf of the Issuer. Accordingly, the conclusion of the Framework Contract with a Client and the request for the issuance of a Card for the benefit of a Cardholder are subject to the prior approval of the Issuer, in all circumstances, without this being contestable by the Client or the Cardholders.

In addition, the Company grants the Client, on an ancillary basis and under the conditions set out in Article 3.2, a Deferred Payment facility for settlement of Transactions carried out by means of the Card.

3.4 Client Relationship

The Company is responsible for the relationship with the Client until termination and acts as the sole point of contact for the performance of the Framework Contract, including for exchanges relating to the relationship between the Client and the Issuer. The Company acts in the name and on behalf of the Issuer in this context.

3.5 Information on the Issuer

The Issuer is a principal member of Visa and Mastercard (registration number 2992502-3) and is authorised by the Finnish Financial Supervisory Authority as a payment institution. Its registered address is Metsänneidonkuja 12, 02130 Espoo, Finland.

3.6 Use of the Card

The Card is intended to be accepted for the payment of purchases of products and services (corresponding to the categories of products and services selected by the Client) from merchants (hereinafter also referred to as "Acceptors") accepting payment by payment card and equipped with Electronic Payment Terminals (hereinafter "EPTs") or self-service machines displaying the Mastercard or Visa logo. The Card may also be used for remote purchases.

ARTICLE 4 — FINANCIAL TERMS

4.1 Subscription and Service Fees

The Services are delivered in consideration of the payment of fees whose cost and invoicing terms are specified in Annex 1.

Subscription fees and service fees are firm and non-revisable during the term of the Framework Contract.

4.2 Settlement of Transactions carried out with the Card or Ancillary Services

Payment operations carried out with the Card or Ancillary Services are settled by invoice to the Company's bank account, the IBAN of which appears in Annex 1, under the conditions set out in this article. The itemised amount of the operations carried out with the Card (amount of operations, flat-rate service fees, currency conversion fees where applicable) appears on a disbursement note serving as a statement of operations, sent by the Company to the Client and made available electronically on the Client Portal at least once a month. A reporting file containing these items together with the analytical and accounting items supplied by the Client will be communicated.

It is the Client’s responsibility to verify the regularity of the payment operations appearing on the statement of operations.

4.3 CSR Contribution to the 1%ForAll® programme

As part of its commitment to corporate social responsibility, the Company operates the 1%ForAll® programme, aimed at financing initiatives with social, environmental or societal impact, through the Greenway Endowment Fund (SIRET 932 082 753 00017).

On this basis, the Client expressly authorises the Company to charge, on the all-inclusive amount of each payment transaction carried out using the Card or Ancillary Services, an additional contribution of a minimum of 1% (the "CSR Contribution").

This Contribution is collected by the Company on behalf of the Greenway Endowment Fund, to which it will be transferred in full.

Allocation of funds

The Client has the option to designate the area(s) to which its CSR Contribution will be allocated, from among the themes or beneficiaries proposed by the Company and the Foundation.

In the absence of specific instructions from the Client, the Contributions will be allocated in accordance with the strategic orientations defined by the Board of Directors of the Greenway Endowment Fund.

The Company undertakes to perform all necessary due diligence to ensure the integrity and compliance of the associations receiving the amounts collected.

The Company shall indemnify the Client against any claim, penalty, recourse or judgment that may result from a breach of these obligations.

Information and transparency

The Company undertakes to provide periodic information to the Client regarding the use and allocation of the CSR Contributions collected.

On this basis, the Company shall provide the Client, at least once a year, with an information report or summary statement indicating the total amount of Contributions transferred, the list of projects supported and the main results observed.

The Client may also, at any time, consult the public information relating to the projects supported and to the governance of the Greenway Endowment Fund on its official website.

Supporting document and tax treatment

Each CSR Contribution shall be the subject of the issuance, by the Greenway Endowment Fund, of a tax receipt or donation voucher in accordance with the applicable regulations, enabling the Client to benefit, where applicable, from a tax reduction under the conditions provided by the legislation of its country of tax residence.

Obligations of the Company

The Company acts as collector and agent of the Endowment Fund for the corresponding amounts, without retaining ownership thereof.

It undertakes to transfer the Contributions received within reasonable time frames and to comply with all accounting, tax and reporting obligations related to this operation.

Any substantial amendment to the mechanism or to the conditions for allocating the Contributions shall be the subject of prior written information to the Client.

4.4 Travel expenses

The Client shall reimburse the Company for travel expenses, including the actual cost of accommodation, meals, travel time, transport and rentals, subject to the Client's prior written approval of such expenses.

4.5 Invoicing

The Company shall send invoices to the Client electronically at the address duly notified in writing by the Client to the Company and will follow the invoicing process described in the "Invoicing best-practice guide" provided by the Client, or as otherwise notified in writing by the Client to the Company.

Such invoicing shall comply with the requirements of the electronic invoicing reform when it enters into force, scheduled in France on 1 September 2026.

ARTICLE 5 — BLOCKING PAYER CEILING

The Parties agree to set, by mutual agreement, a Blocking Payer Ceiling upon conclusion of the Framework Contract and at any time during its performance, and to make the provision of Products, Services and ancillary

Services, as well as of External Network products or services, conditional on the Client's compliance with this ceiling. The Blocking Payer Ceiling sets, for the entire Client account over a defined period, the maximum amount of transactions relating to products and services acquired from Acquirers. This means that the Cards attached to the Client Account are accepted on the Network as long as this Blocking Payer Ceiling has not been reached.

Due to the synchronisation system of the authorisation servers, transactions may be carried out up to two (2) business days after the maximum authorised ceiling is reached. The Client acknowledges being informed of this situation and shall be responsible for it, including for assuming the financial consequences of any such overrun.

This Blocking Payer Ceiling applies throughout the term of the Framework Contract and may be modified at any time by the Company. Any modification of the Blocking Payer Ceiling shall be communicated to the Client on its Portal. The fact of not setting a Blocking Payer Ceiling upon conclusion of the Framework Contract shall not be interpreted as a waiver by the Company of its right to set one subsequently.

ARTICLE 6 — GUARANTEE

As security for its payment obligations in respect of the payment operations carried out with the Cards and the Subscription and Service Fees referred to in Articles 4.1 and 4.2, the Client shall constitute, in favour of the Company, upon conclusion of the Framework Contract and/or at any time during its performance, a guarantee under the conditions set out below, valid throughout the term of the Framework Contract.

This guarantee may, by mutual agreement between the Company and the Client, take one of the following forms:

- ancillary cash guarantee;
- bank guarantee (surety or first-demand guarantee).

More generally, in the event of an unremedied payment incident, the Company shall be authorised to debit the sum paid as guarantee with the amount of unpaid invoices. The outstanding Deferred Payment granted to the Client shall then be automatically reduced by the amounts offset.

The Client may, at any time, adjust the amount of the guarantee paid and/or of the bank surety.

Where applicable, no later than two invoicing periods before the expiry of the aforementioned guarantees, the Client shall, at the Company's request, constitute new guarantees in order to ensure sufficient coverage of its obligations.

If the guarantees offered by the Client prove to be insufficient during the Contract, the Company may, at any time, request additional guarantees. The fact that the Company agrees to enter into the Framework Contract without the Client having provided a guarantee shall not be interpreted as a waiver by the Company of its right to subsequently request guarantees. Failing provision by the Client of the required guarantees, the Company may terminate the Framework Contract without notice.

The amount of the guarantee shall be returned, or the surety released, upon expiry of the contract and, at the latest, after definitive settlement of all invoices owed by the Client or after setting-off of the unpaid amounts with the amount of the deposit paid.

In addition, the Company reserves the right to obtain, from its credit insurer, any information deemed necessary on the Client in connection with the establishment of a guarantee.

ARTICLE 7 — COMPLAINTS AND SUPPORT

Any complaint or support request must be addressed to the Company's client service (hereinafter the "Client Service") on the Site via the dedicated form or by email at the following address: support@greenway.care.

For any dispute relating to unauthorised or incorrectly executed payment operations or not indicating the exact amount of the transaction, the provisions of Articles 11, 12 and 13 shall apply. For any complaint relating to compliance with the provisions of the Framework Contract and to use of the Card, the Client's requests are to be addressed to the Company, which shall transmit them to the Issuer as soon as possible and at the latest within two (2) months.

The Issuer's response is transmitted to the Company as soon as possible and at the latest within fifteen (15) business days following receipt of the complaint.

In exceptional situations, if no response can be given within that period for reasons beyond the Issuer's control, the Issuer shall send a holding response clearly setting out the additional period required to respond to the complaint and specifying the final date by which the Client will receive a definitive response, which may not exceed thirty-five (35) business days following receipt of the complaint.

ARTICLE 8 — INTELLECTUAL PROPERTY RIGHTS IN ELEMENTS INTEGRATED AND PUBLISHED ON THIS SITE AND ON THE MOBILE APPLICATION

All elements of this Site and of the Mobile Application belong to the Company or are used by the Company on the Site and on the Mobile Application with the authorisation of their owners. The trademarks and logos contained on the Site and on the Mobile Application are filed by the Company or, where applicable, by one of its partners. Any person engaging in their representation, reproduction, embedding, distribution or redistribution shall incur the sanctions provided by the French Intellectual Property Code, save with the express authorisation of the rights holder (the Company and/or the partner concerned). Any copying of logos, textual, pictographic or video content, without this enumeration being limitative, is strictly prohibited and amounts to counterfeiting. Any Client guilty of counterfeiting may have its Spaces and Accounts deleted without notice or compensation, the Company also being able to bring subsequent legal proceedings against it, on its own initiative or on that of its agent.

The Company shall indemnify the Client against any action for infringement of copyright, unfair competition or parasitic competition, based on an alleged breach of intellectual property rights.

On this basis, the Company shall indemnify the Client for all damages that the Client may be ordered to pay by a court decision having become final and recognising acts of infringement of copyright, and undertakes to modify the solution to the extent necessary to remove such infringement.

ARTICLE 9 — COMMERCIAL REFERENCE

The Client agrees that the Company may use its name as a commercial reference, subject to the Client's prior written consent, during the term of their commercial relationship. The Client shall have a right of review and withdrawal in respect of any publication mentioning it. In the event of withdrawal, the Company undertakes to remove the publication within one business day, the Company nevertheless retaining the right to anonymise such publication in order to retain it.

ARTICLE 10 — FRAUD

The Issuer and the Company have anti-fraud processes in place, in particular on the basis of the documents communicated to them upon conclusion of the Framework Contract or of any other communication medium exchanged during the performance of the Framework Contract.

If legal proceedings are initiated, the data of the Client and/or Cardholder will be retained until the end of the legal proceedings and then archived in accordance with the applicable statutory limitation periods. If the Client and/or Cardholder is listed on a proven fraudsters list, their data will be deleted after a period of 5 years from the date of listing.

Such listing entails the sharing of data with authorised persons from group entities, in particular those responsible for external fraud prevention. Data relating to proven fraud will be retained for a maximum period of 5 years from the closure of the fraud file. The Client and/or Cardholder may exercise their rights in accordance with the procedures defined in Annex 4 “Personal data protection” of this Agreement.

ARTICLE 11 — ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING — APPLICATION OF FINANCIAL SANCTIONS

Under legislation on anti-money laundering and counter-terrorist financing, the Issuer is required to verify the identification of its clients, their representatives and the beneficial owner(s) of the business relationship, as well as to verify the subject and nature of that relationship.

The Client therefore undertakes to provide, at the Issuer’s first request, any information and supporting documents necessary for the Issuer to comply with its obligations. If the Client cannot provide the elements requested by the Issuer in order to meet its identification and know-your-client obligations, no business relationship may be entered into.

The Client is informed that the Card may not be used in the high-risk countries identified by FATF and/or the European Commission whose legislation or practices hinder anti-money laundering and counter-terrorist financing.

The Issuer has a duty of ongoing vigilance towards its clientele throughout the contractual relationship. As such, it collects any relevant information on the Client’s situation and any probative document enabling the Client’s identity to be verified. In the absence of such information, the relationship may be terminated. Due to its legal and regulatory obligations in relation to anti-money laundering and counter-terrorist financing, including international financial sanctions, the Issuer may have to take any measures — such as an asset freeze — which will have the consequence of blocking the card and/or terminating the Framework Contract.

In the event of subscription by a natural person or by a legal entity whose beneficial owner meets the definition of politically exposed person referred to in Articles L.561-10-2° and R.561-18 of the French Monetary and Financial Code, in addition to the aforementioned obligations, the Issuer is also required to investigate the origin of the assets and funds involved in the business relationship. For this purpose, the Client undertakes to provide the Issuer, at its first request, with this information. If the Client does not provide the elements requested by the Issuer under its regulatory obligations, the relationship may be terminated.

ARTICLE 12 — INTERNATIONAL ECONOMIC SANCTIONS

All activities carried out under this Framework Contract must be performed in accordance with the laws or regulations on export controls and international economic sanctions applicable to the Parties in performing the Framework Contract.

Neither Party shall be required to perform the obligations required by this Framework Contract if to do so would result in a breach of, or be incompatible with, the laws and regulations on export controls and international economic sanctions applicable to it, or would expose that Party to sanctions as provided by such laws and regulations.

Where the performance by a Party of any of its obligations would result in a breach of or be incompatible with the laws and regulations on export controls and international economic sanctions applicable to it, or would expose that Party to sanctions as provided by such laws and regulations, that Party (the "Affected Party") shall, as soon as possible, give written notice to the other Party of its inability to perform any of its obligations. Once such notice has been given, the Affected Party shall have the right (i) to suspend performance of the obligation concerned under this article until the Affected Party can lawfully perform that obligation; and/or (ii) to terminate the Framework Contract if the Affected Party cannot lawfully perform that obligation.

ARTICLE 13 — ANTI-CORRUPTION

During the performance of the Framework Contract, the Parties undertake to comply strictly with the laws in force in France and abroad prohibiting the corruption of public officials and private persons, influence peddling, and/or money laundering.

In this context, the Parties undertake, in particular, to implement and apply all necessary and reasonable policies and measures to prevent corruption, in compliance with the regulations applicable to them. The Parties undertake to impose on members of their personnel and contractors the obligations set out in this clause.

If the Parties fail to comply with any of the commitments set out in this clause, they may, notwithstanding any contrary contractual stipulations, terminate the Framework Contract immediately and as of right, without notice or compensation of any kind whatsoever on their part, and without prejudice to any other right and remedy available to them as a result of the breach noted.

ARTICLE 14 — COMMUNICATION — INFORMATION — EVIDENCE

Communication between the Company, in its own name or in the name and on behalf of the Issuer, and the Client shall take place in French or English and by electronic means. Accordingly, the parties agree to establish a process for the dematerialisation of documents pursuant to which they shall exchange in order to facilitate their relations, in particular the transmission of documents by electronic means.

The Client thus expressly agrees to receive in dematerialised form, in particular via its Client Portal, any documents, any pre-contractual information and more generally any correspondence related to the management of the Cards, in particular statements of operations, supporting documents or notifications of operations.

The Issuer, the Company and the Client irrevocably agree, in accordance with Article 1368 of the French Civil Code, that, unless otherwise provided by law, the Issuer’s or the Company’s copy of any instrument, statement of operations or receipt may consist of an electronic document, even if the Client’s copy is established in paper format. The electronic copy produced by the Issuer or the Company shall have the same probative force as the original signed copy of the Client. The Client may only contest the Issuer's or Company's copy by providing evidence to the contrary, either by means of the original copy intended for it if a synallagmatic agreement is involved, or the duplicate delivered if a unilateral instrument is involved.

Computer, telephone, telematic, video, e-mail or electronic recordings, faxes or any other commonly accepted means of evidence, in the possession of the Issuer or the Company, or their reproduction on any other medium, shall be proof of the operations carried out between the Client and the Issuer or the Company, the Client being entitled to provide evidence to the contrary. The Issuer and the Company shall be entitled, in the same way as the Client, to provide evidence by any means of any legal act or fact, even beyond the statutory threshold referred to in Article 1359 of the French Civil Code; they may in particular prove any act or fact by means of their recordings made in strict compliance with the law. The Client agrees that the Issuer or the Company may validly correspond with it via the aforementioned means of communication.

ARTICLE 15 — CONFIDENTIALITY

The Issuer and the Company are bound by confidentiality regarding the information exchanged. However, such information may be shared for the benefit of certain third parties in accordance with law and international conventions to satisfy legal or regulatory obligations and in particular for the benefit of the tax or customs authorities, the Bank of France, supervisory authorities and judicial authorities. Furthermore, in accordance with Article L.511-33 of the French Monetary and Financial Code (or any other legislation), the Issuer is authorised to share confidential information strictly within the framework of the aforementioned texts. The Client and the Cardholder authorise the Issuer and the Company to communicate the information collected under this agreement to establishments and companies that are members of the group to which the Issuer belongs, as well as to its partners, guarantors, brokers and insurers, service providers, within the limits necessary for the performance of the purposes of the Framework Contract.

ARTICLE 16 — AMENDMENT OF THE FRAMEWORK CONTRACT

Any amendment of the Framework Contract shall be communicated in writing to the Client on paper or another durable medium with reasonable prior notice before the envisaged date of application. Such amendment shall be deemed accepted by the Client in the absence of written objection on its part before the expiry of such period. If the Client refuses the proposed amendment, it may terminate the Framework Contract without charge before the date of entry into force of the amendment in question. Any legal or regulatory measure having the effect of modifying all or part of the Framework Contract shall take effect as of its entry into force. Save for regulatory requirements, the amendments shall not have the effect of calling into question the specific arrangements agreed between the Parties under the Framework Contract.

ARTICLE 17 — TERM AND TERMINATION OF THE FRAMEWORK CONTRACT

The Framework Contract is concluded for a term of five (5) years from the date of signature of the Framework Contract, subject to acceptance by the Issuer, issuance of the first Card constituting acceptance. Unless otherwise notified by the Client, the Framework Contract shall automatically renew for successive periods of one (1) year.

The Framework Contract may be terminated on each anniversary date of the Framework Contract, in writing, by registered letter with acknowledgement of receipt sent by the Company or by the Client. Termination of the Framework Contract at the initiative of the Company takes effect three (3) months after the date of sending its notification to the Client by registered letter with acknowledgement of receipt, the postmark being authoritative.

Termination of the Framework Contract at the initiative of the Client takes effect thirty (30) days after the date of sending its notification to the Company by registered letter with acknowledgement of receipt, the postmark being authoritative. No further Card may be ordered or renewed during the notice period.

The parties undertake to comply with all contractual obligations incumbent upon them under the Framework Contract until termination of the Framework Contract becomes effective.

As from termination of the Framework Contract, the Client is no longer entitled to use the Card, and the Issuer and/or the Company may take any steps necessary to that end.

ARTICLE 18 — FORCE MAJEURE

18.1 The Parties cannot be held liable for damages caused by delays or failures in the performance of their obligations due to a force majeure event. The following events shall in particular be regarded as force majeure events: natural disasters, fires, strikes, riots, wars or terrorist attacks, mandatory requirements of national or international public authorities related in particular to epidemics, and more generally any event beyond the control of a Party, which could not reasonably be foreseen at the time of acceptance of the General Terms, whose effects cannot be avoided by appropriate measures, and which prevents performance of its obligation by the Party concerned.

18.2 The Party concerned shall, as soon as reasonably possible after the onset of the force majeure event, inform the other Party in writing of the existence of such event, of its effective date, its probable or potential duration, and the impact of the force majeure event on its ability to perform its obligations. In this regard, the Party concerned shall use all reasonable efforts to mitigate the impact of the force majeure event on the performance of its obligations.

18.3 Should a force majeure event consisting of mandatory requirements of national or international public authorities of a temporary nature occur, the Company's obligations shall be suspended for the duration of such requirements (and any extensions thereof). Should force majeure events of another nature occur, the Company's obligations shall be suspended for a maximum period of three (3) months from the occurrence of the event, the Client and the Company during that period shall endeavour, if necessary, to agree on the terms for continuing their contractual relationship despite the occurrence of such event.

18.4 At the end of the period referred to in Article 18.3, if the Party concerned is still unable to perform any of its obligations under these General Terms due to the force majeure event, the Company or the Client may terminate the contract as of right. The party intending to invoke this provision shall notify its decision to the other party by registered letter with acknowledgement of receipt. Termination shall then take effect within thirty (30) days of receipt of such notification by the other Party.

ARTICLE 19 — APPLICABLE LAW — JURISDICTION

The law applicable to the negotiation, conclusion, validity, interpretation and performance of the Framework Contract is French law. Any dispute of any nature relating to the Framework Contract shall be subject to the exclusive jurisdiction of the courts within whose jurisdiction the registered office of the defendant is located.

For any mediation request, the Parties must be able to demonstrate having first attempted to resolve their dispute between themselves by means of a written complaint.

ARTICLE 20 — INSURANCE

The Company declares having taken out, and undertakes to maintain, sufficient insurance cover with a reputable insurance company for all damaging consequences of the acts for which it may be held liable by virtue of the performance of the Framework Contract.

The Company’s insurance certificate will be provided to the Client upon simple written request.

ARTICLE 21 — PERSONNEL

The Company undertakes to comply with the provisions of Articles L.8211-1 et seq. of the French Labour Code relating to combating illegal work.

In addition, the Company undertakes (i) to comply with the provisions of Articles L.8221-3 and L.8221-5 of the French Labour Code on the prohibition of concealed work and (ii) pursuant to Articles L.8222-1 and L.8222-4 of the French Labour Code, to provide the Client with the documents referred to in Article D.8222-5 of the French Labour Code if it is established in France, or in Article D.8222-7 of the French Labour Code if it is established or domiciled abroad, on the date of conclusion of this Framework Contract and every six (6) months during its performance.

The Company undertakes to deliver all of these documents, via the dematerialised platform indicated by the Client, every six (6) months until the expiry of the Framework Contract. For information, it is specified to the Company that, as part of its referencing process, the Client has chosen to be assisted by the company PROVIGIS, a collaborative platform specialised in the matter.

The Company also undertakes not to propose to the Client, nor to use, any subcontractor not complying with these obligations.

The Company irrevocably undertakes vis-à-vis the Client to indemnify the latter against all consequences related to the breach of the obligations set out in this article.

By signing the Framework Contract, the Company certifies on its honour (i) that it has made all mandatory tax declarations with the tax administration as of the date hereof, and (ii) that the work is carried out with employees regularly employed in accordance with Articles L.1221-10 et seq., L.3243-1, L.3243-2, L.3243-4 and R.3243-1 et seq., and that, in the event of employment of foreign national employees, they are in a legal situation authorising them to carry out an activity in France. If it is established or domiciled abroad, the Company certifies on its honour having provided its employees with pay slips containing the information required by Article R.3243-1 of the French Labour Code or equivalent documents.

ARTICLE 22 — TERMINATION CLAUSE

The Framework Contract may be terminated as of right in the event of a breach by one of the Parties of its obligations under the Framework Contract which has not been remedied within a period of SIXTY (60) calendar days from receipt of a formal notice requiring such breach to be remedied and which has remained without effect; the Framework Contract may then be terminated as of right by the other party, without prejudice to any damages to which it may be entitled as a result of such breach and any penalties which may be due to it.

Termination of the Framework Contract shall be effective as of the first presentation, to the defaulting party, of a registered letter with acknowledgement of receipt notifying the termination, without it being necessary to carry out any other judicial or extrajudicial formality.

ARTICLE 23 — GENERAL PROVISIONS

QUALIFICATIONS — CERTIFICATIONS

The Company warrants that it holds all legal and regulatory authorisations, and the rights enabling it to provide the services forming the subject matter of the Framework Contract.

CAPACITY

Each party declares that it is duly authorised to enter into this Framework Contract and to perform its obligations under the Framework Contract.

The Parties declare that the provisions of the Framework Contract have been, in compliance with the mandatory provisions of Article 1104 of the French Civil Code, negotiated in good faith, and that, pursuant to those of Article 1112-1 of the same Code, all information of determining importance to the consent of the other has been disclosed.

INDEPENDENCE

No provision of this Framework Contract may be interpreted as creating or implying a relationship of joint venture, partnership, principal-agent or subordination between the parties. Save where otherwise expressly provided in this Framework Contract, neither party has the power or authority to bind the other party, nor shall it purport to have any such power or authority.

SEVERABILITY

If a provision (or part of a provision) of this Framework Contract is held by a competent court to be invalid, unenforceable or illegal, the other provisions shall remain in force. If an invalid, unenforceable or illegal provision would be valid, enforceable or legal if some part of it were deleted, the provision shall apply with any modifications necessary to give effect to the common commercial intention of the parties.

WAIVER

No failure or delay by a party in exercising a right or remedy under this Framework Contract or by law shall constitute a waiver of that right or remedy or of any other right or remedy and shall not prevent or restrict the exercise of that right or remedy or of any other right or remedy. No exercise or partial exercise of any right or remedy shall prevent or restrict the further exercise of that right or remedy or of any other right or remedy.

ASSIGNMENT

This Framework Contract binds the Parties hereto and their respective successors and assigns, and shall inure to the benefit of said Parties and their respective successors and assigns. The Company may not assign this

Framework Contract or any of its rights or obligations hereunder without having first obtained the written consent of the Client.

SUBCONTRACTING

The Company undertakes to select its subcontractors in accordance with high criteria of reliability, security and sustainability, and to define their obligations so as to be able to ensure strict compliance with its own obligations under the Framework Contract, in particular those relating to confidentiality, intellectual property and the status of personnel. Total subcontracting is prohibited.

The use of subcontractors by the Company shall in no way reduce its liability vis-à-vis the Client under the Framework Contract, the Company remaining guarantor vis-à-vis the Client of the proper performance of the Framework Contract and remaining its exclusive point of contact.

NOTICES

To be valid, any notice under the Framework Contract must be made to the addresses appearing below, or to any other address notified by the Parties in accordance with this article. Notices are made by hand delivery against receipt or by registered letter with acknowledgement of receipt.

Notices shall be deemed to have been given on the following date: (i) when delivered by hand, the date indicated on the receipt, (ii) when made by registered letter with acknowledgement of receipt, the date indicated on the acknowledgement of receipt or, failing receipt, the date of first presentation.

- **For GREENWAY:** Greenway — 5 RUE PLEYEL, 93200 SAINT-DENIS — support@greenway.care | invoice@greenway.care

ELECTRONIC SIGNATURE

The Parties agree that the Framework Contract is concluded in the form of an electronic writing, in accordance with the provisions of Article 1366 of the French Civil Code, and signed electronically by means of a reliable identification process implemented by DocuSign ensuring the link between each signature and this Framework Contract, in accordance with the provisions of Article 1367 of the French Civil Code.

The Parties acknowledge that the Framework Contract has the same probative force as a written document on paper in accordance with Article 1366 of the French Civil Code and that it may validly be relied upon against them.

The Parties attribute to this electronic signature the same value as their handwritten signature and, in order to confer certain date on that attributed to the signature of the Framework Contract by the DocuSign service (www.docusign.com).

Each party undertakes to take all appropriate measures to ensure that the electronic signing of this document is carried out by its duly authorised representative for the purposes of this document.

The Parties acknowledge that (i) the requirement for multiple originals is deemed satisfied as long as the Framework Contract signed electronically is established and retained in accordance with Articles 1366 and 1367 of the French Civil Code, and (ii) this process allows each Party to have a copy on a durable medium or to have access thereto, in accordance with the provisions of Article 1375 of the French Civil Code.

The Parties agree to designate Puteaux (France) as the place of signature of the Framework Contract.

ANNEX 1 — FINANCIAL TERMS

ARTICLE 1 — PRICING

The subscribed Services take effect on the date of signature of the Framework Contract or of the amendment by the Parties. The Financial Terms applied are either the public Terms (https://www.greenway.care/fr/tarifs) or those negotiated via a Quote and overriding the public pricing for the specific items thereof.

Should the Company develop new categories of products and services accessible with the Card, the Client agrees that the Company shall charge service fees on such new services if the Client uses them. The Client acknowledges that any consumption of such services by means of the Card constitutes unreserved acceptance of the conditions, in particular pricing conditions, applicable to such new Services.

ARTICLE 2 — PAYMENT AND INVOICING TERMS

2.1 The Services are invoiced monthly in accordance with the price list above. The termination of a Service during an ongoing period shall not give rise to a refund for the period during which the Licence / Licence Subscription has been suspended by the Company.

2.2 Payment of invoices is made by bank direct debit on the Company's bank account.

2.3 Pursuant to the provisions of Articles L.441-10 to L.441-16 of the French Commercial Code on payment terms between undertakings, the Company's invoices are payable within 7 days of the date of issuance of the invoice without any discount for early payment. No cheque, bill of exchange or other instrument shall be deemed to constitute valid payment until the Company has collected all sums due in full.

ARTICLE 3 — LATE PAYMENT

Any late payment shall entail for the Client, as of right and without the need for prior formal notice, a penalty rate equal to three times the statutory interest rate after a prior reminder from GREENWAY. Such interest shall accrue from the due date of the invoice until the date of full payment of the invoice. An additional flat-rate indemnity of forty euros (€40) for recovery costs shall also be due. Furthermore, the Services may be suspended until full payment of the sums due after formal notice sent electronically.

ARTICLE 4 — ANNUAL REVIEW OF PRICES

The prices and financial terms of this Contract may be reviewed once a year, on the anniversary date of its signature. The revision is made automatically according to the variation of the revised SYNTEC index (published by the SYNTEC Federation).

ANNEX 2 — SERVICES PROVIDED

ARTICLE 1 — THE CLIENT PORTAL

Upon subscription to the Framework Contract, and subject to the prior communication to the Company by the Client of the email address and personal information of the Principal User or of the Manager designated in the Framework Contract (surname, first name and landline phone number), the latter shall receive in return login credentials enabling access to the Client Portal. The Client Portal is secure and encrypted and is therefore accessible only after entering a username provided by the Company and a password chosen by the Client upon its first connection to the Client Portal.

The Client Portal enables the Client to access the detailed information on its Card fleet and to configure the use parameters thereof.

The basic functionalities of the Client Portal, described below, are accessible to all Clients who have entered into the Framework Contract:

- **Card Management:** The Client may order, configure, delete or suspend its Cards. The Card configuration consists in authorising expense categories according to the profile of the Cardholders and the company's mobility policy, defining payment limits (frequency, amount) and carrying out temporal (authorised hours/days) and geographical controls. The geographical and temporal controls shall not apply to remote sales (VAD). The Client may adjust these configurations in real time, in particular for an exceptional mission.
- **Cardholder Management:** The Client may request the provision of a Mobile Application to the Cardholders as specified in the article below, by completing a Cardholder record containing their personal information. A login ID is then sent to the Cardholder. The Client may modify or delete this Cardholder record at any time, the deletion making it impossible for the Cardholder to use the Mobile Application.
- Assistance with the control of mobility expenses (recoverable VAT amount).
- Management of invoices and debit notes (expense notes).

The Company reserves the right to suspend access to the Client Portal in the event of fraudulent use or attempted fraudulent use of such access.

ARTICLE 2 — PAYMENT CARD

The Card is a payment instrument enabling the Cardholder, within the context of their professional activity, to carry out payment operations for the purpose of settling purchases of goods and services related to professional expenses.

The Cardholder may be the Client itself or a collaborator of the Client expressly designated by the Client. The expenses settled with the Card as well as the fees relating to the use of the service shall be paid by the Client in accordance with the terms and pricing conditions agreed between the Client and the Company in the Framework Contract.

The Company shall establish, at a frequency agreed with the Client and at most within a period not exceeding one (1) month, an invoice statement summarising the payment operations carried out with the Card, as well as any fees and commissions.

Under the legislation on anti-money laundering and counter-terrorist financing, the Client and/or Cardholder undertake to use the Card only for the settlement of their own professional expenses and to respond to any request relating to the legal and regulatory obligations of the Issuer in relation to anti-money laundering and counter-terrorist financing, including international financial sanctions, in this Agreement.

The Card is a nominative payment instrument for the exclusive use of its Cardholder, enabling it to carry out payment operations and having as its sole purposes to:

- settle purchases of products and services with Acceptors, in person or remotely;
- authorise an Acceptor to proceed with an information request made by the EPT or payment machine in connection with:
    - a payment operation for the purpose of renting products or services by the Cardholder,
    - or a request by the Acceptor for one or more payment operations by Card planned with the Cardholder’s consent.
- the payment operations listed above are possible only within the limits of the ceilings set by the client and after validation of the payment by PIN code, contactless or remote validation.

The Client undertakes to inform the Cardholders of the Conditions and limits of use of the Card, before delivering their Card to them. The Issuer makes available to the Cardholder a Card featuring "contactless" technology, the conditions of operation of which are governed by this article.

The Client undertakes to take regular cognisance of the security information communicated to it by the Issuer, the Company or on the Client Portal. The Client selects, in its Client Portal, the categories of products and services for which the Card may be used by the Cardholder and undertakes to inform the Cardholder accordingly. The Client nevertheless undertakes to pay all amounts resulting from transactions carried out in connection with non-compliant use of the Card by its Cardholder.

The return of goods or services paid for by Card may be the subject of a refund request with the Acceptor only if a transaction has previously been debited for a greater or equal amount. If an agreement is reached between the Cardholder and the Acceptor, the latter may operate the EPT to initiate the refund transaction with the same Card as that used for the initial transaction. The refund is then stored as a "Credit to spend" on the card. Where the Client benefits from a Deferred Payment granted by the Company, such Credit to spend shall offset the next expenses made by the Cardholder with its Card. No refund shall be made to the Client's bank account.

ANNEX 3 — INVOICE TEMPLATE

Below is an example of the document that you will receive at the beginning of each month. It comprises 3 parts:

1. A summary page.
2. An invoice page comprising the subscriptions and other fees.
3. The disbursement note, setting out all consumption.

ANNEX 4 — ANNEX ON OBLIGATIONS REGARDING THE PROCESSING OF PERSONAL DATA

By signing this Annex, the Parties agree to comply with all applicable laws and regulations relating to the processing of personal data and, in particular, with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "the European Regulation on Data Protection" or "GDPR") and French Law No. 78-17 of 6 January 1978 on Information Technology, Files and Liberties, as amended (hereinafter the "French Data Protection Act").

The Client warrants having been authorised by the Principal User and the Manager to communicate to the Company their personal data necessary for the purposes of using the Client Portal. Similarly, the Client warrants having been authorised by the Cardholders to communicate to the Company their personal data necessary for the purposes of using the Mobile Application, and having informed them that their data would also be transmitted by the Company to the Issuer. The personal data concerned are the following: surname, first name, date of birth, professional mobile phone and email, professional address.

These personal data are necessary to use the Client Portal and the Mobile Application. The Client undertakes to inform the Company immediately of any modification of the Cardholder’s personal data.

The Client shall generally ensure compliance with the legal and regulatory provisions on the protection of privacy and personal data of the Principal User, the Manager and the Cardholder.

The Client also undertakes to inform them that:

- for the Client, as well as the Principal User and the Manager: their data are collected and processed by the Company as controller for the performance of the Framework Contract and for follow-up of the commercial relationship with the Client;
- their data are collected and processed by the Issuer, as controller, for the issuance of the Card and management of the operations carried out;
- their personal data are communicated to the Issuer by the Company, and to the Company by the Issuer, for the purposes of the Framework Contract. Furthermore, personal data may be communicated to the companies of the groups to which the Company and the Issuer respectively belong, as well as to partners, service providers or subcontractors involved in the performance of the Framework Contract;
- the Client, the Manager and the Principal User may exercise their rights of access, rectification, erasure, restriction, data portability and objection, with the Company by sending a postal letter to the Company or by email to the following address: rgpd@greenway.care;
- the Cardholder may exercise their rights of access, rectification, erasure, restriction, data portability and objection directly with the Client. The Company shall transfer to the Client any Cardholder request addressed directly to it, in order for the Client to give effect to it. The Company shall assist the Client, upon request and to the extent possible.

It is specified that the Company and the Issuer shall inform each other of the requests to exercise rights made under the Framework Contract, where necessary for the processing thereof.

The personal data protection policies of the Issuer and of the Company are accessible on their respective websites.

ARTICLE 1 — DEFINITIONS

Term	Definition
"Contract"	designates these General Terms and any other contractual document applicable depending on the method of conclusion of the contract determined between the Parties.
"Processing", "Controller", "Joint Controller", "Processor", "Sub-processor", "Personal Data":	these terms have the same meaning as the definition given to them in the GDPR, insofar as they apply to the Contract.
"Services":	designates the services provided by the Company to the Client and described in the Contract.
"User Data":	designates the Personal Data (surnames, first names, roles, employer, phone number and email address where applicable, professional expenses) of the Users of the Services (including the Cardholder), processed by the Company during the performance of the Contract in the name and on behalf of, and under the detailed instructions of, the Client.
"Company Contact Data":	designates the Personal Data relating to the Company's personnel involved in the performance of the Contract and communicated to the Client on that basis.
"Client Contact Data":	designates the Personal Data relating to the Client's personnel, in particular the Client Manager, involved in the performance of the Contract and communicated to the Company on that basis.

All terms used in this Annex on the processing of Personal Data appearing in capital letters and not defined below are defined in the Contract.

ARTICLE 2 — CONTEXT

Within the context of the Contract, the Parties will be required to process Personal Data and by this Annex intend to define the conditions and modalities of Processing of such Personal Data.

ARTICLE 3 — PURPOSE

This Annex on the processing of Personal Data (hereinafter the "Agreement") aims to define the conditions under which the Parties undertake to carry out Personal Data Processing operations for the purposes of performing the Contract.

ARTICLE 4 — TERM

The Agreement enters into force on the date of entry into force of the Contract and shall remain in force throughout the term of the Contract and for as long as the Parties have access to any Personal Data communicated by the other Party under the Contract.

Expiry or termination of the Contract, for any reason whatsoever, shall not affect the validity of this Agreement.

ARTICLE 5 — OBLIGATIONS OF THE PARTIES

Performance of the Contract involves the following Personal Data Processing operations, the respective purposes of which are specified below:

- The Processing by the Company of User Data, in the name and on behalf of, and under the detailed instructions of, the Client, for the purposes of performing the Contract;
- The Processing by the Company of Client Contact Data for the purposes of performing the Contract;
- The Processing of the Company's Contact Data for the purposes of performing the Contract.

5.1 Processing of User Data

5.1.1 Obligations of the Company

The Company collects the User Data solely for the purposes of performing the Contract. When it collects the User Data under the Contract, and when it subsequently processes them, the Company acts as the Client's Processor. The Client retains the status of Controller, insofar as it determines the purposes and means of such Processing, i.e., the objective and manner of carrying it out.

The Company undertakes to process the personal data solely for the purpose that is the subject of the subprocessing and in accordance with the documented instructions of the Client.

The Company undertakes to implement all reasonably necessary and appropriate technical and organisational measures to protect the Personal Data it processes under the Contract against any unauthorised or accidental access, modification, transmission, communication, deletion or destruction.

The Company also ensures that all persons authorised to process the personal data for the Client commit to respecting confidentiality or are subject to an appropriate statutory confidentiality obligation and receive the necessary training regarding the protection of personal data. The Company undertakes to take into account, in its tools, products, applications and services, the principles of data protection by design and by default. The Company, as Processor, implements the necessary means to enable the Controller to discharge its obligation to give effect to the requests of the data subjects to exercise their rights: right of access, rectification, erasure and objection, right to restriction of processing, right to data portability, right not to be subject to automated individual decision-making.

Where data subjects submit requests to exercise their rights to the Company, the Company must address such requests upon receipt (without exceeding a period of 72 hours) by email sent to the Client's DPO.

The Company undertakes to modify or delete, at the Client's request, any personal data appearing in its information system, in particular in the event of the exercise by a person of their rights of access, rectification and deletion, so that the data held by the Company concerning such person are and remain accurate and lawful.

The Company notifies the Client of any personal data breach within a maximum of 24 hours after becoming aware of it and by email. This notification shall be accompanied by any useful documentation to enable the Client, if necessary, to notify this breach to the competent supervisory authority.

The notification shall contain at least:

- a description of the nature of the personal data breach including, if possible, the categories and approximate number of persons affected by the breach and the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or of another contact point where further information can be obtained;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken or envisaged to address the personal data breach, including, where applicable, measures to mitigate any possible adverse effects.

If, and insofar as, it is not possible to provide all this information at the same time, the information may be communicated in stages without undue delay.

Where the breach is likely to result in a high risk to the rights and freedoms of a natural person, only the Client may communicate to the data subject, in clear and plain language, the nature of the personal data breach.

In the event of a personal data breach, the notification to the national supervisory authority, as soon as possible and if possible, no later than 72 hours after becoming aware of it, shall be carried out by the Client.

The Company assists, at its expense, the Client in complying with its obligations. The Company assists the Client in particular for the performance of data protection impact assessments and for the carrying-out of prior consultation of the supervisory authority.

The Company immediately informs the Client of any legally binding request for the communication of personal data or for information regarding the Processing(s) carried out under the Contract by a law enforcement body, unless such notification is prohibited by law, in which case notification must be made within a maximum of forty-eight (48) hours after the lifting of the prohibition.

The Company makes available to the Client the documentation and information necessary to demonstrate compliance with all of its obligations and to enable the carrying out of audits, including inspections, by the Client or by another auditor mandated by it, and contributes to these audits. It is specified that, for audits, the auditor shall not be a competitor of the Company.

5.1.2 Obligations of the Client

The Client acts as Controller. As such, the Client warrants to the Company that the User Data are collected and processed lawfully and that the data subjects have been informed of such Processing and of their resulting rights. Accordingly, the Client shall indemnify the Company against any action by third parties based on a regulatory breach of the Controller's obligations.

In the event of a complaint or exercise of rights by a data subject based on a Processing carried out by the Company on behalf of the Client, the Client shall be solely responsible for responding to it, the Company undertaking to cooperate with the Client to this end, at the Client's request.

5.2 Processing of Contact Data

For the purposes of performing the Contract, each of the Parties shall communicate its Contact Data to the other Party. Each Party is Controller of the processing of the other Party's Contact Data.

Such Contact Data shall be processed by the recipient Party solely for the purposes of managing the contractual relationship arising from the Contract. They shall be transmitted only to the authorised personnel and authorised Suppliers of each of the Parties involved in the Contract.

These Contact Data may be retained by the recipient Party for a maximum period of one year from the end of the Contract.

Each of the Parties undertakes to inform the persons concerned by these Contact Data of the fact that these Data will be communicated to the other Party for the purposes of the Contract and to inform them of their rights: right of access, objection, rectification and erasure of the personal data concerning them, as well as the right to data portability, the right to define directives relating to the fate of their personal data after their death and to request restriction of the processing concerning them, the right to lodge a complaint with the CNIL.

Data subjects may exercise their rights with the DPO of the Party that communicated the Contact Data to the other Party.

In the event of the exercise of rights or a complaint by a data subject with the recipient Party, the latter undertakes to immediately inform the communicating Party so that the latter can provide an appropriate response.

In the event of a breach of Contact Data with the recipient Party, the latter undertakes to immediately inform the communicating Party, specifying the names of the persons concerned and the nature of the breach, and the Parties shall cooperate in order to put an end to it as soon as possible.

ARTICLE 6 — LIABILITY

Non-compliance with the provisions of this Annex constitutes a serious breach of the Parties' commitments and may lead to termination of the Contract for fault of one of the Parties without prejudice to any damages.

Notwithstanding any provision of the Contract to the contrary, given the critical and strategic nature for the Client of ensuring a processing of personal data in compliance with applicable regulations and in particular with the GDPR, it is expressly agreed between the Parties that the liability incurred in the event of breach by the Company of the provisions of this Annex shall not be capped.

ARTICLE 7 — SUBCONTRACTING

It is noted that, as at the date of signature, the Company has entered into agreements with the following Sub-processors to carry out the processing of Personal Data, which the Client expressly and specifically acknowledges and accepts.

Name	Head office	Purpose of processing	Data concerned	Country of data storage
AWS App/Data	USA	Storage	Client	European Union
Hubspot	USA	Communication	Client	European Union
Sinch	USA	Communication	Client	European Union
Twilio	USA	Administrative	Client	European Union
Zapier	USA	Organisation	Client	European Union
Slack	USA	Communication	Client	European Union
Google	USA	Organisation	Client	European Union

Name	Head office	Purpose of processing	Data concerned	Country of data storage
Docusign	USA	Retention	Client	European Union
LinkedIn	USA	Communication	Client	European Union
Clickup	USA	Administration	Client	European Union
Stripe	USA	All	Client	European Union
Enfuce	Finland	Administrative	Client	European Union
Chorus	France	Recording	Client	European Union
Pennylane	France	Administrative	Client	European Union
Attio	USA	Communication	Client	European Union

For any addition of a new subsequent subcontractor, the Company must obtain the prior written consent of the Client.

ARTICLE 8 — SECURITY

The Parties declare that they maintain in writing a register of all categories of processing activities carried out.

Each Party undertakes to:

- have appropriate measures in place to ensure the continuity, integrity, availability and resilience of its systems and Processing services;
- have means enabling the availability of Personal Data and access to them to be restored within appropriate time frames in the event of a physical or technical incident;
- establish a procedure for regularly testing, analysing and evaluating the effectiveness of the technical and organisational measures to ensure the security of the Processing and to provide evidence thereof to the other Party or to the supervisory authorities on first request;
- comply with the commitments provided for in this Annex and ensure that its permanent or temporary personnel comply with its terms;
- maintain an up-to-date register of processing activities whenever it carries out an operation or set of operations applied to personal data or sets of personal data. This register of processing activities shall be consultable by each of the Parties;
- cooperate with the supervisory authority at its request.

The Company applies the technical and organisational security and confidentiality measures aimed at preventing the destruction, loss, alteration, communication or unauthorised access, whether accidental or unlawful, of/to the Personal Data, in accordance with Article 32 of the GDPR.

The Company is able to assess the relevance of the choice of its measures and may, at any time, justify them.

The Company shall not significantly reduce the general security during the performance of the Contract without obtaining the Client’s prior written consent.

These security obligations are essential obligations without which the Client would not have contracted with the Company.

ARTICLE 9 — DATA PROTECTION OFFICER

The Data Protection Officer (DPO) of the Company may be reached at the following contact address: dpo@greenway.care.

ARTICLE 10 — FATE OF THE DATA

Upon completion of the services relating to the processing of such data, the Company undertakes, in accordance with the Client’s instructions, to return all personal data for which the Client is controller.

The return must be accompanied by the destruction of all existing copies in the processor’s information systems. Once destroyed, the processor must provide written evidence of the destruction.

ANNEX 5 — MANDATE FOR THE RETRIEVAL OF SUPPORTING DOCUMENTS / PURCHASE INVOICES

ARTICLE 1 — PURPOSE OF THE MANDATE

By this instrument, the Client grants power and mandate to the Company GREENWAY (hereinafter the "Agent") to retrieve, in its name and on its behalf, the supporting documents and purchase invoices corresponding to purchases made using a Greenway payment card (hereinafter the "Mandate").

Supporting documents and purchase invoices mean the original or a duplicate enforceable against the tax and social administration, including simplified invoices and restaurant receipts for operations of an amount less than €150 excluding tax, in accordance with Article 242 nonies A of Annex II to the French General Tax Code.

ARTICLE 2 — LEGAL BASIS

This Mandate is based on the provisions of Articles 1984 et seq. of the French Civil Code relating to the contract of mandate.

The supporting documents and purchase invoices concern purchases made from the various Suppliers / Merchants, physical and online, from the date of signature of this Framework Contract and relating to all purchases made with a Greenway payment card.

The Suppliers' invoicing obligation results from the provisions of Articles L.441-9 et seq. of the French Commercial Code and Article 289 of the French General Tax Code.

ARTICLE 3 — SCOPE AND MODALITIES OF PERFORMANCE OF THE MANDATE

3.1 In the course of performing the Mandate, the Agent carries out the following steps in the name and on behalf of the Client:

- the automated or manual retrieval of the invoices made available by the Suppliers via digital interfaces (API, supplier portals, online client areas);
- the setting up and management of a dedicated email address to which the Suppliers or the Client forward or redirect the invoices;
- the sending of requests for the transmission of invoices or duplicates to the Suppliers, by electronic or postal means;
- the reconciliation of the supporting documents and purchase invoices with the corresponding transactions, subject to receiving sufficient information from the Supplier to identify it.

3.2 The Agent retains the supporting documents and invoices collected via its Application and undertakes not to disclose them to unauthorised third parties.

3.3 The Agent may, in the performance of the Mandate, communicate to the Supplier an extract of this Mandate or a power of attorney signed by the Client, in order to justify its capacity as agent. Such extract or power of attorney shall not contain any confidential commercial or financial information relating to the Client.

ARTICLE 4 — NATURE OF THE AGENT'S OBLIGATION

4.1 The Agent undertakes to perform the Mandate with diligence and in accordance with the rules of the art. The Agent's obligation under this Mandate constitutes an obligation of means and not of result. The Agent undertakes to use its best efforts to obtain the supporting documents and invoices in the name and on behalf of the Client, but does not guarantee the actual obtaining of each invoice or supporting document.

4.2 In particular, the Agent shall not be held liable in the following cases:

- refusal or default of a Supplier to transmit the invoice or duplicate despite the Agent's reminders;
- inability to identify the Supplier from the data of the transaction;
- absence of an invoice or supporting document issued by the Supplier (cases of transactions for which no invoice is legally required or has been generated by the Supplier);
- breach by the Client of its cooperation obligations set out in Article 6 below.

4.3 In any event, the Agent's liability under this Mandate is limited to the amount of the service fees received by the Agent under the Framework Contract during the twelve (12) months preceding the event giving rise to the claim.

ARTICLE 5 — OBLIGATIONS OF THE SUPPLIERS

5.1 The Supplier is legally required to deliver to the Client, and therefore to the Agent pursuant to this Mandate, a duplicate of the supporting documents and invoices of the purchases made, in accordance with the provisions of Articles L.441-9 of the French Commercial Code and 289 of the French General Tax Code.

5.2 As soon as the transaction takes place between two professionals, the issuance of an invoice in duplicate is mandatory. This invoice must be delivered either at the time of delivery of the goods in contracts for the sale of goods, or upon completion of the provision of services.

5.3 In the event of persistent refusal of a Supplier to transmit the invoices despite the Agent's reminders, the Agent shall inform the Client thereof as soon as possible so that the Client may, if it so wishes, directly exercise its rights against the Supplier or mandate the Agent for any additional step.

ARTICLE 6 — COOPERATION OBLIGATIONS OF THE CLIENT

6.1 The Client undertakes to enable the Agent to perform this Mandate by providing it with any necessary cooperation and by communicating to it in good time the information and documents required. To this end, the Client undertakes in particular to:

- forward to the Agent, as soon as possible, any invoice or supporting document received directly from a Supplier that should have been addressed to the Agent;
- inform the Cardholders of the obligation to collect and forward to the Agent the receipts, till tickets and supporting documents given during purchases at points of sale;
- inform the Agent of any change in its relations with a Supplier likely to affect the performance of the Mandate.

6.2 Breach by the Client of its cooperation obligations shall not engage the Agent's liability for any delay or impossibility in obtaining the supporting documents and invoices resulting therefrom.

ARTICLE 7 — ELECTRONIC INVOICING

7.1 In the context of the electronic invoicing reform in France, and in accordance with the provisions of Article 289 bis of the French General Tax Code and Ordinance No. 2021-1190 of 15 September 2021 on the generalisation of electronic invoicing in transactions between persons liable to VAT, the Client expressly authorises the Agent to intervene with the Suppliers to organise the transmission of electronic invoices in the context of this Mandate.

7.2 On this basis, the Agent is authorised to contact the Suppliers in order to request them to transmit the electronic invoices relating to purchases made using the Card via the Supplier's Partner Dematerialisation Platform (PDP) or, where applicable, via the Public Invoicing Portal (PPF), to the Client or to any receiving address designated by the Agent in the name and on behalf of the Client.

7.3 The Agent may for this purpose communicate to the Suppliers the information necessary for the routing of the electronic invoices, notably the receiving details (dedicated email address, recipient identifier on the PPF, or any other technical entry point designated by the Agent), as well as the accepted invoice formats (Factur-X, UBL, CII or any other format compliant with the applicable regulations).

7.4 The Supplier remains solely responsible for the issuance and transmission of the electronic invoice via its own PDP or via the PPF, in accordance with its legal and regulatory obligations. The Agent does not provide a dematerialisation platform service and is not responsible for technical failures or delays attributable to the Supplier's PDP or to the PPF.

7.5 The Client authorises the Agent to receive, retain and process the electronic invoices transmitted by the Suppliers, in compliance with the applicable legal and regulatory requirements regarding integrity, authenticity of origin and legibility of the invoices, in accordance with Articles 289 V and 289 VII of the French General Tax Code.

7.6 The Client undertakes to cooperate with the Agent to facilitate the setting up of the routing of electronic invoices, notably by communicating its SIREN number, its intra-Community VAT number and any other information necessary for identifying the invoice recipient in the Suppliers' electronic invoicing systems.

ARTICLE 8 — EXECUTION REPORT

8.1 The Agent makes available to the Client, via the Client Portal, a follow-up of the performance of the Mandate including a status of the invoices collected, of the requests in progress and of any refusals or defaults of Suppliers.

8.2 The Client may at any time consult this status on the Client Portal. A summary report may be communicated to the Client on request.

ARTICLE 9 — TERM AND TERMINATION

This Mandate takes effect on the date of signature of the Framework Contract and remains in force throughout the duration thereof. It terminates as of right upon termination or expiry of the Framework Contract. The Client may also revoke this Mandate at any time by written notice addressed to the Agent, the revocation taking effect within thirty (30) days following receipt of the notice.

ANNEX 6 — DATA MANDATE FOR CONNECTED VEHICLES

ARTICLE 1 — PURPOSE OF THE MANDATE

By this instrument, the Client grants power and mandate to the Company to retrieve, in its name and on its behalf, from the suppliers of connected vehicles, the data relating to the Client's vehicles identified by their Vehicle Identification Number (VIN). This data includes, without limitation, the vehicle's location, fuel tank level or electric charge level, repair history, as well as any other relevant information available via the suppliers' connected systems.

ARTICLE 2 — LEGAL BASIS

This mandate authorises the Company to access the data of the Client's connected vehicles with the suppliers, from the date of signature of this contract. This data concerns exclusively vehicles registered under the Client's name and identified by their VIN, in accordance with the Company's general terms and conditions of service and the applicable regulations on data protection.

ARTICLE 3 — OBLIGATIONS OF THE SUPPLIERS

The suppliers of connected vehicles are required to provide the Company, as the Client's agent, with access to the data of the vehicles identified by their VIN, insofar as such data is available and in accordance with the existing agreements between the Client and the suppliers. Such access may include, without limitation, API interfaces or other technical systems (through partners) enabling the collection of the data referred to in Article 1.

ARTICLE 4 — UNDERTAKING OF GREENWAY

The Company undertakes to collect, process and retain the data of the connected vehicles via its Application, in compliance with the regulations in force, in particular with regard to the protection of personal data (GDPR). The Company undertakes not to disclose this information to third parties, except with the express authorisation of the Client or in the event of a legal obligation. The data collected shall be used exclusively to provide the services agreed with the Client, such as location tracking, management of fuel or electric charge, and tracking of repairs.

ARTICLE 5 — TERM AND TERMINATION

This mandate takes effect on the date of signature of the contract and remains in force until its termination by either party, in accordance with the Company's general terms and conditions of service. In the event of termination, the Company shall immediately cease to collect the vehicle data from the suppliers, except as otherwise provided by law.

ANNEX 7 — SERVICE LEVEL AGREEMENT (SLA) ON THE AVAILABILITY OF THE PLATFORM

ARTICLE 1 — DEFINITIONS

For the purposes of this Annex, the following terms and expressions shall have the meaning set out below, unless the context otherwise requires:

- **Platform:** Designates the Client Portal and the Mobile Application made available by the Company, as described in Annex 2 of the General Terms.
- **Availability:** The percentage of time during which the Platform is accessible and operational for Users and the Client, calculated on a monthly basis.
- **Downtime:** Any period during which the Platform is not accessible or does not function correctly due to a failure attributable to the Company.
- **Anomaly:** Malfunction or non-compliant behaviour of the Platform in relation to its functional or technical specifications, reported by the Client or detected by the Company.
- **Severity Level:** Classification of an Anomaly according to its impact on the features and availability of the Platform:
    - Severity 1 (Critical): Total service interruption or major unavailability preventing any use of the Platform.
    - Severity 2 (Major): Significant malfunction affecting one or more essential features without total interruption of the service.
    - Severity 3 (Minor): Limited malfunction or cosmetic anomaly not hindering general use of the Platform.
- **Resolution Time:** Time elapsed between the Company's qualification of an Anomaly and the making available of a corrective solution, workaround or definitive fix.
- **Scheduled Maintenance Window:** Periods predefined and announced in advance by the Company to carry out updates, corrections or improvements to the Platform.
- **Force Majeure:** Events as defined in Article 18 of the General Terms.
- **Service Credit:** Refund or reduction granted to the Client in the event of non-compliance with the Availability commitments.

ARTICLE 2 — PURPOSE

The purpose of this Annex is to define the Company's commitments regarding the Availability of the Platform, the calculation methods, the exclusions, as well as the consequences in the event of non-compliance with these commitments. It supplements the General Terms and forms an integral part of the Accession Agreement. Included in the Company's liability is that of the Issuer.

ARTICLE 3 — AVAILABILITY COMMITMENTS

3.1 The Company undertakes to ensure an Availability of the Platform of at least 99.5% on a monthly basis, measured 24 hours a day, 7 days a week.

3.2 Availability is calculated according to the following formula:

Availability (%) = [(Total Time of the Month − Downtime) / Total Time of the Month] × 100

- Total Time of the Month: Total number of minutes in the calendar month.
- Downtime: Sum of minutes of unavailability attributable to the Company.

3.3 The Company sets up a continuous monitoring system to monitor the Availability of the Platform. Availability reports will be made available to the Client on the Client Portal, on request or monthly.

3.4 In addition to Availability monitoring, the Company ensures follow-up of Anomalies affecting the Platform, according to their Severity level and the resolution times set out in Article 7. The availability reports will include a monthly indicator of the number and severity of Anomalies observed.

ARTICLE 4 — EXCLUSIONS

The following periods are not taken into account in calculating Downtime:

4.1 Scheduled Maintenance Windows, announced to the Client at least 48 hours in advance via the Client Portal or by email. These periods shall not exceed 4 hours per month and shall be scheduled outside peak hours (generally between 10 p.m. and 6 a.m. CET).

4.2 Unavailability caused by Force Majeure events.

4.3 Unavailability due to actions or omissions of the Client or of the Users, such as erroneous configurations, misuse or internet connection problems on the Client’s side.

4.4 Unavailability resulting from failures of third parties not controlled by the Company, such as hosting providers or payment networks (Mastercard/Visa).

4.5 Temporary interruptions necessary for security, regulatory compliance or anti-fraud reasons, in accordance with Articles 10, 11 and 12 of the General Terms.

4.6 Anomalies resulting from improper use of the Platform, incorrect configuration or a non-compliant environment of the Client are not considered attributable to the Company.

ARTICLE 5 — CONSEQUENCES OF NON-COMPLIANCE

5.1 In the event of non-compliance with the Availability commitment, the Client shall be entitled to a Service Credit calculated as follows:

Monthly Availability	Service Credit (percentage of the monthly subscription and service fees)
Between 99.0% and 99.5%	5%
Between 98.0% and 99.0%	10%
Between 90.0% and 98.0%	20%
Less than 90.0%	50%

5.2 The Service Credit shall be applied on the next invoice or refunded to the Client within 30 days of the claim. The maximum amount of Service Credits per year shall not exceed 100% of the annual subscription paid by the Client.

5.3 To benefit from a Service Credit, the Client must submit a written request (via the Client Portal or email) within 30 days of the end of the month concerned, providing reasonable evidence of the unavailability.

5.4 Service Credits constitute the Client's sole and exclusive remedy in the event of non-compliance with the Availability commitments. They do not exclude the other remedies provided for in the General Terms in the event of gross misconduct by the Company.

5.5 In the event of repeated non-compliance with the resolution times defined in Article 7 for Severity 1 or 2 Anomalies, the Client may benefit, on request, from an additional Service Credit of 5% per incident not resolved within the contractual deadlines.

ARTICLE 6 — COMPLAINTS AND FOLLOW-UP

7.1 Complaints relating to Availability or Anomalies shall be handled in accordance with Article 7 of the General Terms.

7.2 The Company provides priority technical support in the event of a Severity 1 Anomaly, with regular communication to the Client until full resolution.

7.3 The follow-up of Anomalies, processing times and performance indicators is accessible via the Client Portal.

ARTICLE 7 — ANOMALY MANAGEMENT AND RESOLUTION COMMITMENTS

7.1 Reporting of Anomalies

Anomalies may be reported by the Client via the Client Portal, email or any other channel provided for this purpose. The Company acknowledges receipt and assigns a Severity level after initial diagnosis.

7.2 Resolution Time Commitments

The resolution times are measured in business hours (Monday to Friday, 9:00 a.m. to 6:00 p.m. CET), unless otherwise stated.

Severity Level	Description	Response Time	Target Resolution Time
1 — Critical	Total unavailability or complete blocking of operations	1 hour	8 hours
2 — Major	Main features impacted without total interruption	4 hours	2 business days
3 — Minor	Non-blocking or cosmetic anomalies	1 business day	5 business days

7.3 Corrective Measures

The Company may deploy a temporary workaround to restore the service pending a definitive fix. In such case, the resolution time remains suspended until the permanent fix is deployed to production.

7.4 Follow-up and Incident Report

A monthly report detailing the number of Anomalies by Severity, their processing times and any discrepancies with respect to the commitments shall be communicated to the Client on request.

7.5 Exclusions

The following are not considered Anomalies attributable to the Company:

- errors originating from third-party integrations;
- requests for changes or customisations;
- malfunctions not reproducible in a standard environment.

ANNEX 8 — BUSINESS CONTINUITY PLAN (BCP) AND DISASTER RECOVERY PLAN (DRP)

ARTICLE 1 — DEFINITIONS

For the purposes of this Annex, the following terms and expressions shall have the meaning set out below, unless the context otherwise requires:

- **Business Continuity Plan (BCP):** All measures and procedures put in place by the Company to ensure the continuity of essential Services in the event of a major incident affecting its operations, in order to minimise interruptions for the Client.
- **Disaster Recovery Plan (DRP):** All technical and organisational measures and procedures aimed at restoring the Company's systems, data and infrastructures after a disaster, within predefined time frames.
- **Major Incident:** Any unforeseen event, such as a computer outage, cyberattack, natural disaster, pandemic or any other event likely to significantly disrupt the Services, excluding Force Majeure events as defined in Article 18 of the General Terms.
- **Recovery Time Objective (RTO):** Maximum acceptable time to restore the Services after a Major Incident.
- **Recovery Point Objective (RPO):** Maximum acceptable quantity of data lost in the event of a Major Incident, measured in time (e.g., the latest available backup).
- **Platform:** Designates the Client Portal and the Mobile Application, as defined in Annex 2 and Annex 6 of the General Terms.
- **Service Credit:** Refund or reduction granted to the Client in the event of non-compliance with the BCP or DRP commitments, calculated in a manner similar to the provisions of Annex 6.

ARTICLE 2 — PURPOSE

The purpose of this Annex is to define the Company's commitments with regard to business continuity and recovery, in order to ensure the reliability and resilience of the Services provided to the Client. It supplements the General Terms and Annex 6 on the Service Level Agreement (SLA) on the Availability of the Platform, and forms an integral part of the Accession Agreement. The BCP and DRP aim to protect the Client's interests by minimising the impacts of a Major Incident on access to the Cards, the Client Portal, the Mobile Application and the other Services.

ARTICLE 3 — COMMITMENTS OF THE COMPANY

3.1 Implementation of the BCP and DRP

The Company undertakes to maintain an up-to-date BCP and DRP, tested at least once a year and adapted to changes in the Services. These plans include:

- Identification of potential risks and critical assets (such as servers, databases, payment systems and personal data processed in accordance with Annex 4).

- Procedures for detecting, notifying and managing incidents.
- Redundancy measures (e.g., automated backups, geographically distant backup sites and partnerships with reliable third-party suppliers).
- A dedicated crisis management team, including a BCP/DRP coordinator.

3.2 Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

- For critical Services (issuance and use of Cards, access to the Client Portal and the Mobile Application): maximum RTO of 4 hours and maximum RPO of 1 hour.
- For secondary Services (invoice management, assistance with expense control): maximum RTO of 24 hours and maximum RPO of 24 hours. The Company undertakes to comply with these objectives in the event of a Major Incident, subject to the exclusions set out in Article 4.

3.3 Notification and Communication

In the event of a Major Incident, the Company shall inform the Client as soon as possible, and at the latest within 2 hours following detection, via email, the Client Portal or any other agreed means. This notification shall include:

- The nature of the incident.
- The estimated impact on the Services.
- The measures taken for recovery.
- An estimate of the resolution time. The Company shall provide regular updates (at least every 4 hours) until full resolution.

3.4 Tests and Improvements

The Company shall carry out annual tests of the BCP and DRP, including incident simulations. The results of these tests shall be documented and available upon request by the Client, subject to confidentiality. Any necessary improvement shall be implemented within 3 months following the tests.

ARTICLE 4 — EXCLUSIONS

The BCP and DRP commitments shall not apply in the following cases:

4.1 Force Majeure events as defined in Article 18 of the General Terms.

4.2 Incidents caused by actions or omissions of the Client, Users or Cardholders (e.g., fraudulent use or use of the Card or Platform that does not comply).

4.3 Unavailability due to third parties not controlled by the Company (e.g., outages at the Issuer, Mastercard/Visa, or hosting providers).

4.4 Scheduled Maintenance Windows, announced in accordance with Annex 6.

4.5 Incidents resulting from international economic sanctions, from anti-fraud, anti-money laundering or anti-corruption measures, as set out in Articles 10 to 13 of the General Terms.

ARTICLE 5 — CONSEQUENCES OF NON-COMPLIANCE

5.1 In the event of non-compliance with the RTO or RPO attributable to the Company, the Client shall be entitled to a Service Credit calculated as follows:

- If the RTO or RPO is exceeded by less than 50%: Credit equivalent to 8% of the monthly subscription.
- If the RTO or RPO is exceeded by 50% to 100%: Credit equivalent to 19% of the monthly subscription.
- If the RTO or RPO is exceeded by more than 100%: Credit equivalent to 35% of the monthly subscription.

The maximum amount of Service Credits per year shall not exceed 40% of the annual subscription paid by the Client.

5.2 The Service Credit shall be applied on the next invoice or refunded within 30 days of the claim. To benefit from it, the Client must submit a written request (via the Client Service or email to support@greenway.care) within 30 days following the resolution of the incident, providing reasonable evidence.

5.3 Service Credits constitute the Client's sole and exclusive remedy in the event of non-compliance with the BCP or DRP commitments, without prejudice to the other remedies provided for in the General Terms in the event of gross misconduct by the Company.

ARTICLE 6 — COMPLAINTS AND FOLLOW-UP

Complaints relating to the BCP or DRP shall be handled in accordance with Article 7 of the General Terms. The Company shall provide priority technical support in the event of a Major Incident.

ARTICLE 7 — DATA RECOVERY AT THE END OF THE CONTRACT

In the event of termination or expiry of the Framework Contract, the Company undertakes to assist the Client in recovering its data stored on the Platform, in order to ensure a smooth transition and to minimise any business interruption related to the end of the contract. Such recovery is part of the continuity and recovery commitments described in this Annex, and is subject to the provisions on personal data protection set out in Annex 4.

7.1 Recovery Modalities

The Company shall provide the Client, upon written request (via the Client Service or email to support@greenway.care), a full export of the Client's data in a standard and machine-readable format (e.g., CSV, JSON or XML), including, in particular, the data relating to the Cards, transactions, invoices and customised configurations. This export shall be made available within a maximum period of 30 calendar days following receipt of the request, subject to the Client having paid all sums due under the Contract.

7.2 Temporary Access and Assistance

If necessary, the Company shall grant the Client temporary and secure access to the Platform for a maximum period of 15 days following the end of the Contract, exclusively for the purposes of data extraction. Reasonable technical assistance shall be provided by the Company to facilitate this operation, at no additional cost, except for any costs related to specific or excessive requests.

7.3 Deletion of Data

Once the data recovery has been confirmed in writing by the Client, the Company shall proceed with the secure and irreversible deletion of such data from its systems, in accordance with the requirements of the

General Data Protection Regulation (GDPR) and good security practices. A certificate of deletion shall be provided to the Client on request.

7.4 Exclusions and Limitations

This recovery obligation shall not apply to data lost or corrupted as a result of actions or omissions of the Client prior to the end of the Contract, nor to data subject to legal retention obligations (e.g., in anti-money laundering or anti-fraud matters). In the event of non-payment of the sums due, the Company reserves the right to suspend access to the data pending full payment.

7.5 Consequences of Non-Compliance

In the event of non-compliance attributable to the Company with the data recovery commitments (e.g., exceeding the export deadline without justification), the Client shall be entitled to a Service Credit equivalent to 10% of the last annual subscription, applied or refunded within 30 days following the claim. This credit constitutes the Client's exclusive remedy for this reason, without prejudice to the other provisions of the General Terms.

ANNEX 9 — CYBERSECURITY MEASURES

ARTICLE 1 — DEFINITIONS

For the purposes of this Annex, the following terms and expressions shall have the meaning set out below, unless the context otherwise requires:

- **Cybersecurity:** All technical, organisational and procedural measures put in place to protect information systems, data and Services against threats, attacks or IT incidents.
- **Security Incident:** Any event likely to compromise the confidentiality, integrity or availability of the data or Services, such as a cyberattack, data leak, malicious failure or security breach.
- **Platform:** Designates the Client Portal and the Mobile Application, as defined in Annex 2 of the General Terms.
- **Hosting Provider:** Bearstech, a cooperative engineering company specialised in hosting, managed services, DevOps and Cloud services, based in Paris, France, and hosting the Company's servers exclusively in France.
- **GDPR:** Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

ARTICLE 2 — PURPOSE

The purpose of this Annex is to define the Company's commitments with regard to cybersecurity, in order to ensure the protection of the data of the Client, Users and Cardholders, as well as the resilience of the Services against cyber risks. It supplements the provisions on the protection of personal data (Annex 4), on the Business Continuity Plan (BCP) and the Disaster Recovery Plan (DRP) (Annex 7), and forms an integral part of the Framework Contract. The measures described aim to comply with applicable regulatory standards, in particular the GDPR, and to minimise the potential impacts of a Security Incident.

ARTICLE 3 — COMMITMENTS OF THE COMPANY

3.1 Infrastructure and Hosting

The Company's servers and IT infrastructures are hosted exclusively by the Hosting Provider, Bearstech, in France. This location ensures compliance with European requirements regarding data sovereignty and protection against unauthorised extra-EU transfers. Bearstech provides secure hosting services, including geographic redundancy measures within French territory, data encryption protocols in transit and at rest (TLS 1.3 minimum for communications, AES-256 for storage), and continuous monitoring of the infrastructures.

3.2 Technical Security Measures

The Company implements the following measures to ensure the cybersecurity of the Services:

- **Encryption:** All sensitive data (including personal data and payment information) are encrypted in transit and at rest. Communications with the Platform use secure protocols (HTTPS with SSL/TLS certificates).

- **Access Controls:** Restricted access based on the principle of least privilege (RBAC — Role-Based Access Control). Mandatory multi-factor authentication (MFA) for Managers, Principal Users and the Company's personnel. Passwords are hashed and salted.
- **Firewall and Intrusion Detection:** Deployment of advanced firewalls (WAF — Web Application Firewall) and intrusion detection and prevention systems (IDS/IPS) to block common attacks (DDoS, SQL injection, XSS, etc.).
- **Backups and Redundancy:** Daily automated backups of the data, retained for at least 30 days, with regular restoration testing. Redundant infrastructures to avoid single points of failure.
- **Updates and Patches:** Systematic application of security updates for all software and systems, with a maximum deadline of 7 days for critical patches.

3.3 Organisational Measures

- **Audits and Tests:** The Company carries out annual internal security audits and external penetration tests (pentests) at least once a year, performed by certified third parties. The results are analysed and vulnerabilities corrected within a maximum period of 30 days for critical risks.
- **Training:** The Company's personnel receive annual training on cybersecurity best practices, incident management and GDPR compliance.
- **Compliance:** Compliance with ISO 27001 server standards (or equivalent) for information security management. Collaboration with the Issuer to align the measures with PCI-DSS requirements for payment data.

3.4 Security Incident Management

In the event of a Security Incident:

- **Detection and Notification:** The Company has a 24/7 monitoring system to detect incidents in real time. The Client is informed within 24 hours following detection of an incident affecting its data, primarily via email or the Client Portal, with details on the nature, impact and corrective measures.
- **Response and Remediation:** Immediate activation of an Incident Response Team (IRT). The compromised data are isolated, and a post-incident analysis is carried out to prevent recurrences. Upon the Client's first request, a report shall be provided on the incident, its nature and the impacts concerning the Client.
- **Regulatory Notification:** In the event of a personal data breach, notification to the CNIL within 72 hours, in accordance with the GDPR, and to the Client if a high risk is identified.

ARTICLE 4 — EXCLUSIONS

The cybersecurity commitments shall not apply to incidents resulting from:

4.1 Actions or omissions of the Client, Users or Cardholders (e.g., password sharing, use of the Card or Platform that does not comply).

4.2 Force Majeure events (Article 18 of the General Terms).

4.3 Failures of third parties not controlled by the Company or the host (e.g., at the Issuer or the Mastercard/Visa networks).

4.4 Sanctions or legal obligations related to anti-fraud, anti-money laundering or anti-corruption (Articles 10 to 13 of the General Terms).

ARTICLE 5 — CONSEQUENCES OF NON-COMPLIANCE

5.1 In the event of a breach attributable to the Company resulting in a major Security Incident, the Client shall be entitled to a Service Credit applied on the next invoice equivalent to:

- 5% of the annual subscription, in the event of a data breach affecting more than 10% of the Client's Users.
- 25% of the annual subscription, in the event of a data breach affecting more than 5% of the Client's Users.
- 10% of the annual subscription, in the event of a data breach affecting more than 1% of the Client's Users.

5.2 The maximum amount of Service Credits per year shall not exceed 50% of the annual subscription. The request must be submitted in writing within 30 days following the incident.

5.3 These credits constitute the Client's exclusive remedy, without prejudice to the remedies for gross misconduct provided for in the General Terms.

ARTICLE 6 — TERM AND MODIFICATION

This Annex enters into force on the date of signature of the Framework Contract and follows the term thereof (Article 17 of the General Terms). Any modification shall be notified to the Client in accordance with Article 16 of the General Terms.

ARTICLE 7 — COMPLAINTS AND FOLLOW-UP

Complaints relating to cybersecurity shall be handled via the Client Service (Article 7 of the General Terms). The Company provides priority support in the event of a suspected incident.

ANNEX 10 — ENFUCE: CARD TERMS AND CONDITIONS

This agreement ("Conditions") sets out the terms for use of the card issued by Enfuce License Services Ltd and constitutes a binding agreement between you and us. The terms "you" and "your" refer to the account holder, as defined below.

The Card is issued by Enfuce License Services Ltd ("Enfuce", "we", "our" or "us"). We are authorised and supervised by the Finnish Financial Supervisory Authority as an electronic money institution and are authorised to issue card payment instruments connected to the Card Scheme network (as defined below).

The Card is provided to you in collaboration with Greenway SAS (see below for details) which is referred to in these Conditions as "Greenway". Greenway's role is explained in more detail in Article 3.

These conditions apply to the following card programme ("Card Programme"):

DESCRIPTION OF THE CARD PROGRAMME

Type of card:	**Commercial — Physical, virtual and wallet (e.g., digital wallet card)**
Type of funding:	Deferred debit. The Card operates on a deferred debit basis: Transactions carried out by means of the Card are settled by the Account Holder at the end of the deferral period agreed in the Framework Contract concluded with Greenway, the duration of which does not exceed sixty (60) days from the date of invoicing. This deferred payment facility, non-onerous, is granted by Greenway as an accessory commercial arrangement to the Services, in accordance with Article L.511-7, I, 1° of the French Monetary and Financial Code. Enfuce is not a party to the deferred payment and does not grant any credit to the Account Holder. The commercial receivables resulting from the deferred payment may be assigned by Greenway to Aria in accordance with Annex 11.
Card scheme:	Mastercard Card
Currency:	EUR
Issuer:	Enfuce License Services Ltd, a company incorporated under Finnish law with its address at Metsänneidonkuja 12, 02130 Espoo, Finland, email issuing.support@enfuce.com. Enfuce is registered in the Finnish trade register under number 2992502-3 and is authorised as an electronic money and payment institution. Enfuce is supervised by the Finnish Financial Supervisory Authority, Snellmaninkatu 6, 00101 Helsinki, tel. +358 9 183 51, finanssivalvonta(at)finanssivalvonta.fi.
Greenway:	Greenway SAS, business identity code 978 860 062, a company incorporated under French law with its registered office at 5 rue Pleyel, 93200 Saint-Denis, France. Email: hello@greenway.care
Deferred payment:	Granted by Greenway SAS under the conditions of the Framework Contract.
Assignee of receivables:	ARIA, SAS registered with the RCS of Bobigny under number 839 836 608, 5 Rue Pleyel, 93200 Saint-Denis. Receivables resulting from the use of the deferred payment may be assigned to Aria in accordance with Annex 11.
User Interface:	Website www.greenway.care and mobile application. The user interface allows: · ordering and administration of cards; · activation, consultation of transactions, consultation of the available balance, blocking and unblocking of cards and enquiries to the customer service regarding the use of the cards and/or the available balance.

Type of card:	Commercial — Physical, virtual and wallet (e.g., digital wallet card)
Unused card limit:	A card may be blocked or terminated if it remains inactive, i.e., unused for a period of twelve (12) consecutive months.
Transaction limits:	As set out in the annex.
Use of the card:	Mobile/e-commerce: Yes; ATM withdrawals: Yes; Balance transfers: No; Territory of use: Worldwide. Use restriction: Please also see the restricted high-risk merchant categories in the annex.

You must accept and comply with these conditions in order to use the card. You will be asked to confirm your acceptance of these conditions when you apply for a card. If you do not accept these conditions, we will not be able to process your card application and/or activate a card. The conditions in force at the time of your application will be displayed on the user interface.

These conditions constitute a legally binding agreement between you and us. By confirming your agreement to these conditions on behalf of the legal entity or organisation you represent, i.e., the account holder, you confirm that you have the authority necessary to enter into a legally binding agreement. Please note that Greenway is not a party to this agreement and your relationship with Greenway is governed by a separate agreement, referred to in these Conditions as the Greenway Agreement.

ARTICLE 1 — DEFINITIONS AND INTERPRETATION

1.1 The defined terms have the meaning set out below, unless they are defined elsewhere in these conditions:

"Account Holder": you, the entity or organisation to which the cards are issued, which owns the funds available on the cards and which is authorised to allow card users to use the cards.

"Applicable Law": all applicable laws, including statutes, statutory instruments, regulations, court decisions and judgments, all requirements, guidance or codes of practice stipulated by an applicable regulatory authority, and including any applicable rule or requirement of a card scheme related to the issuance, sale, authorisation or use of the card.

"ATM": automated teller machine where card users can withdraw cash, if this feature is activated for the cards (as set out in the Card Programme description above).

"Available Balance" means, for each Card, the maximum amount that the Account Holder may spend, within the limits of the ceilings and settings defined in the Framework Contract and on the User Interface.

"Business Day" means Monday to Friday, 9 a.m. to 5 p.m. CET, excluding bank, national and public holidays in Finland.

"Card" means each of the types of payment instruments specified in the Card Programme description above, such as physical cards, virtual cards or tokenised cards (electronic wallet), that we issue to you in the denomination currency. References to a card include all security details relating to that card.

"Card Scheme": the payment network to which the cards are connected, as specified in the Card Programme description.

"Card User": a person to whom a card is provided and who is validly authorised by you to use the funds on the card on your behalf.

"Customer Services" means the assistance provided by Greenway in relation to the Card and the Card Programme, the details of which are described in the Annex to these Conditions.

"Denomination Currency": the currency specified in the Card Programme description.

"Personal Data": all personal identity data relating to a card application and to use of the card, including (but not limited to) the following data concerning card users: name, date of birth, home address, email address and phone number (landline and/or mobile), and may include security data. Full details of the personal data we process are set out in our privacy policy (https://enfuce.com/privacy-and-data-protection/).

"PIN" or "PIN Code": the personal identification number used to authorise transactions carried out using the card.

"POS" means a point-of-sale terminal.

"Greenway Agreement": any agreement between you and Greenway relating to the Card Programme, including the User Interface terms of use and the terms applicable to any additional services provided to you by Greenway.

"Regulatory Authority" means, depending on the context, any card scheme and/or any regulatory authority or agency having jurisdiction over us or Greenway with regard to the issuance, marketing, sale, authorisation or use of the cards or the services provided under these Conditions, including, without limitation, the Finnish Financial Supervisory Authority.

"Security Details": certain information relating to a card and its use, e.g., card users' personal details or passwords, the PIN of the card, the card number (including the three-digit CVV number), its expiry date or the password associated with your account and/or any card user account on the user interface.

"Transaction": the use of a card to (i) make a payment or purchase of goods or services from a merchant on the Internet, by phone or by mail or (ii) withdraw cash from an ATM or from a bank, where authorised.

"User Interface" means the website, sub-sites or mobile applications provided to you by Greenway in accordance with and subject to the Greenway Agreement, where you and the Card Users may carry out certain operations in connection with the Cards, as specified in the Card Programme Description. The "User Interface" includes all sub-sites accessible only to your authorised administrative users authorised to order and manage the cards, as well as the card user interfaces.

ARTICLE 2 — ELIGIBILITY AND OTHER CHECKS

2.1 A card application may be subject to certain eligibility and other checks carried out by Greenway on our behalf, for example to verify the details of the account holder’s organisation and/or whether the proposed card user meets the card eligibility criteria agreed between you and Greenway. We reserve the right to carry out eligibility and other relevant checks on any Card User. You agree to provide all information and documents requested by Greenway. Please note that Greenway may use third parties to verify certain information, e.g., credit reference agencies.

2.2 All information you provide must be accurate and truthful to the best of your knowledge. You must promptly inform customer services of any change in the information you have provided or, if this feature is available, update your information in the user interface. You must notify any changes in this information, any sanctions likely to affect you or any card user, or if the use of a card may become illegal for any other reason.

2.3 We (and Greenway on our behalf) reserve the right to carry out additional checks (including in respect of card users) after the issuance and/or activation of a card, for example before processing a transaction.

2.4 If you do not provide the information or documents requested by Greenway or by us, we may be unable to issue the Card(s) and/or process the Transactions, or even suspend all or part of the Cards and ultimately terminate this agreement with you.

2.5 It is your responsibility, and you continuously warrant and represent to us, that you have provided the appropriate notices and, where applicable laws require, that you have obtained all necessary consents from the card users in order to transmit to us any information concerning such users.

2.6 All card applications and activations are at our discretion and we may refuse to accept your application.

ARTICLE 3 — OUR ROLE AND GREENWAY'S ROLE

3.1 We are the issuer of the card and we process all transactions made with the card.

3.2 The card programme is provided to you in collaboration with Greenway, which provides you with the user interface, accepts and processes card applications on our behalf, provides customer services and carries out certain activities relating to the administration and management of the card programme on our behalf.

3.3 Greenway directly grants the Account Holder a Deferred Payment facility for the settlement of Transactions carried out by means of the Card, as an accessory commercial arrangement to the Services provided under the Framework Contract, in accordance with Article L.511-7, I, 1° of the French Monetary and Financial Code. Enfuce is not a party to this deferred payment relationship and does not grant any credit to the Account Holder. The commercial receivables resulting from the deferred payment may be assigned by Greenway to an assignee (Aria) in accordance with the Framework Contract.

3.4 Greenway is your primary point of contact and if you or any Card User has any questions or issues relating to the use of the Cards, you and the Card Users must contact Greenway via customer services.

3.5 Greenway is authorised to collect and transmit to us all information, communications and instructions submitted by you or by any Card User, such as the card application or requests made via customer services.

3.6 We may exercise our rights under these Conditions through Greenway and, to that limited extent, references to "we", "us" or "our" shall be construed as references to Greenway.

ARTICLE 4 — GENERAL INFORMATION ABOUT THE CARD

4.1 The card is a payment instrument, allowing immediate payment, which can be used to pay for goods and services at locations that accept cards marked with the card scheme.

4.2 The card remains our property and must be returned to us or destroyed at our request.

4.3 Use of the card is personal to the card user. Card Users may not assign their rights to use their cards to anyone else and are strictly prohibited from allowing a third party to use their cards.

4.4 No interest is payable on the card's available balance and no funds loaded onto the card constitute a deposit with us.

4.5 Transactions carried out using the Cards are settled by the Account Holder at the end of the deferral period agreed with Greenway under the Framework Contract. Enfuce is not involved in the deferred payment relationship between the Account Holder and Greenway, and does not grant credit to the Account Holder.

4.6 Information relating to the available balance, transactions and card funding methods is set out in the user interface and the Greenway Agreement.

ARTICLE 5 — ACTIVATION AND USE OF THE CARD

5.1 A physical card must be activated by the card user within the notified deadline. An activation procedure will be provided with the card.

5.2 Each card expires on the date indicated on the card and cannot be used after its expiry.

5.3 A card may only be used if it has a sufficient available balance to carry out a transaction and pay the associated fees. If the available balance is insufficient to pay for a transaction (including applicable fees), the transaction will be declined. The amount of each transaction and the associated fees will be deducted from the available balance.

5.4 The Account Holder settles the Transactions carried out by means of the Card in accordance with the terms set out in the Framework Contract concluded with Greenway. No interest is charged by Greenway or Enfuce in respect of the deferred payment granted to the Account Holder. The service fees due by the Account Holder are exclusively those defined in Annex 1 of the Framework Contract, on a flat-rate basis. Settlement takes place at the latest at the end of the deferral period agreed, which does not exceed sixty (60) days from the date of invoicing.

5.5 The fees specified in the price list shall be deducted from the available balance. If, for any reason, we are unable to charge your cards with the fees or other amounts owed to us, you agree to make payment as soon as possible upon receipt of a request for payment from us or from Greenway.

5.6 The programme description and the provisions of the annex set out the restrictions and limits that apply to the use of the cards.

5.7 You agree to accept a credit on a card (i.e., an increase in the available balance) if you or any card user are entitled to a refund for any reason.

5.8 We are not required to guarantee that all merchants, points of sale and ATMs will accept the card (whether it is a physical card or a token via a digital wallet).

5.9 If (in exceptional circumstances or by mistake) we carry out a transaction while the available balance is insufficient, we will deduct such amounts from any subsequent reload or other payment increasing the available balance or, if the available balance is not sufficient, we may ask you to reimburse such amounts.

5.10 Some merchants may generate a pre-authorisation to reserve an amount that may be greater than the resulting payment transaction. This is the case, for example, when the card is used to book a hotel or a rental car and the final amount of the bill is not known. In this case, if the available balance is not sufficient, the pre-authorisation request may be declined. For such services, card users must ensure that their card has a sufficient available balance to cover the amount required by the pre-authorisation.

5.11 We do not recommend using the card as a guarantee for future payment, for example as a deposit, because in such situations merchants may estimate the final bill and that estimated amount will be temporarily unavailable to be spent with the card.

5.12 If a merchant agrees to refund a card (if the card was used to make the transaction), the merchant may process the refund through a point of sale. Amounts credited to the card for refunds made by merchants increase the card's available balance when we receive confirmation from the card scheme that the merchant refund has been processed. If the amount credited to the card is greater than the refund amount, the excess amount may be deducted from your available balance and returned to the merchant. Loading fees may apply to refunds made through a point of sale, if such fees are specified in the price list.

5.13 You must ensure that transactions carried out by card users do not breach any applicable law and that they comply at all times with all applicable laws relating to the use of the cards.

5.14 The ability of your users to use or access the card may occasionally be interrupted, for example if we need to carry out maintenance on our systems or if the card scheme encounters problems in processing transactions. You or the card users should inform customer services of any problems encountered when using the card or report the problem via the user interface, and we will do our best to resolve these issues as soon as possible.

5.15 You or the card users may request the blocking or unblocking of the card by contacting customer services or using the user interface. Blocking a card does not satisfy the card users' obligation to notify us of the suspected or actual loss, theft, misuse or fraudulent use of the card or the security details. Please see clause 5 for further details on what to do in such circumstances.

5.16 You are responsible for any use of the cards and for all acts and omissions of the card users. You warrant, represent and undertake that all card users shall be informed of the content of these conditions and understand the obligations related to the use of the cards.

ARTICLE 6 — DIGITAL WALLETS

6.1 This clause 6 applies if a digital wallet (e.g., Apple Pay and Google Pay) is activated for the cards as part of the card programme.

6.2 The use of a digital wallet is subject to the terms and conditions of the digital wallet provider, which will be provided to card users when they activate a digital wallet on their device. We are not responsible for the terms of use of digital wallets.

6.3 To use a card in a digital wallet or to remove it from the digital wallet, card users must follow the wallet provider's instructions. Some digital wallet providers may restrict the use of certain cards or limit the number of cards added. Please note that the wallet functionality is not our responsibility and any questions relating to the use of wallets must be addressed to the relevant wallet provider.

6.4 Card transactions using a digital wallet can be carried out with merchants that accept the digital wallet in question.

6.5 In the event of loss or theft of the device on which a digital wallet storing a card is activated, card users must notify us immediately and treat the incident as if it were a loss or theft of the card. Before selling or disposing of the device, the card must be removed from the wallet.

6.6 Card users should be alert to any message informing them that a card has been added to a digital wallet and immediately inform customer services if they suspect fraud.

6.7 The use of a card in a digital wallet may be suspended by us in certain exceptional situations, in order to protect the security of the card. If a card expires or is terminated, users will no longer be able to use their cards in the wallet.

ARTICLE 7 — CARD SECURITY

7.1 Card users must sign the back of physical cards as soon as they receive them.

7.2 Card users must treat the card like cash. If a third party gains access to a card and/or the security details, you may lose some or all of the money you hold on the card, in the same way as if you lost cash.

7.3 The card and its security details (including the PIN) must be kept securely by taking appropriate measures, including, but not limited to, the following:

- never allowing anyone else to use the card and never disclosing the PIN or other security details to anyone;
- not carrying the PIN with the card or recording it in a place where it can be viewed by others;
- not interfering with the magnetic strip or integrated circuit (i.e., the chip) of the card;
- complying with all instructions given by us or Greenway regarding the security of the card and the security details;
- using only secure Internet sites and trusted merchants to carry out transactions;
- choosing strong passwords that mix alpha and numeric characters when managing the card via the user interface;
- checking that ATMs show no signs of tampering, such as false façades, before using them;
- destroying any personal information or security details relating to the card that could be used by an identity thief; and
- reporting the loss, theft or misuse of security details relating to the card to customer services and to any competent body in order to alert them to any potential attempt at identity theft on your behalf.

7.4 Card users are never required to provide the PIN by phone or on the Internet to pay for goods or services or to carry out any other transaction. If someone asks a card user to disclose their PIN, they must refuse to do so and report the incident to customer services.

7.5 The PIN may be disabled if an incorrect PIN is entered three (3) times at any ATM and/or point of sale. If the PIN is disabled, the card user must go to the user interface or contact customer services to reactivate the PIN. A period of twenty-four (24) hours may be necessary to reactivate the PIN.

7.6 Card users must under no circumstances send us active and/or loaded cards, to us, to Greenway or to a third party, by post or by any other non-secure delivery method.

ARTICLE 8 — AUTHORISING TRANSACTIONS

8.1 Card users must authorise each transaction so that we can verify its authenticity. For point-of-sale transactions using the physical card, card users may be asked to authorise them, where applicable: a) by entering the PIN on a payment terminal (i.e., a chip and PIN payment terminal); or b) by signing a sales slip.

Transactions of an amount less than or equal to 50 euros may be authorised simply by tapping the physical card (or the mobile device, if an electronic wallet is enabled for the card) on a contactless payment terminal. However, contactless transactions above 50 euros require an additional authorisation step, such as entering your PIN into the point-of-sale terminal.

8.2 When card users use it to make online purchases of 30 euros or more, they are asked, in addition to providing the card details, to confirm their identity. Depending on the authentication technology used, they may be asked to authenticate the transaction by: (i) something they know, e.g., a password; (ii) something they have, e.g., an access code sent to their mobile phone, a card reader or other device generating a one-time access code; and (iii) something they are, e.g., using a fingerprint scanner, facial recognition or other authentication methods enabling the card user to be verified as the one authorising the transaction. A technology called 3D Secure is often used by merchants to facilitate secure online authentication, and some technologies allow card users to use the user interface as part of the transaction authorisation process. Please note that we are not responsible for these authentication technologies and we cannot be held liable for anything related to the use of these technologies.

8.3 Once a transaction has been authorised by a card user, it cannot be cancelled and the time of receipt of a transaction order is when we receive the card user's authorisation.

ARTICLE 9 — LOSS, THEFT AND MISUSE OF CARDS

9.1 If a card is lost, stolen, misused or likely to be misused by a third party or if you suspect that another person may know the PIN or other security details or has carried out an unauthorised transaction, the card user must stop using the card and inform customer services directly (and block your card via the user interface, if this feature is available). The card user must do so as soon as they become aware of the loss, theft, misuse or unauthorised use of the card or security details. Unless it has already been blocked via the user interface, the card will be suspended in order to prevent further losses.

9.2 The card user must confirm to us in writing the details of the loss, theft or misuse and you and the card user may be asked to assist us, our agents or the police in the event of theft of the card or suspected misuse of the card.

9.3 Replacement cards will be sent to the most recent address notified to us as the delivery address for the card and may be subject to a fee as defined in the annex.

9.4 If a card declared lost is subsequently found, it must not be used without you having contacted customer services and obtained their agreement.

ARTICLE 10 — UNAUTHORISED AND DISPUTED TRANSACTIONS

10.1 You or the card user concerned must inform customer services as soon as you/they become aware (and at the latest within 24 hours) of a transaction that was not authorised by the card user in accordance with clause 8.1 above, or if you or the card user consider that we have incorrectly executed a transaction. We must be informed no later than thirty (30) days after the date on which such transaction affected the available balance on the card.

10.2 We will investigate the circumstances that led to the unauthorised or incorrectly executed transaction. We may ask you and/or ask the card user concerned to provide us with information and supporting documents to assist us in our investigation and you agree to cooperate with us and to procure that the card user concerned cooperates with us.

10.3 Subject to the other provisions of this clause 10, we will refund the amount of the transaction (together with applicable fees and interest) and restore the available balance to the level it would have been at if the transaction had not occurred, at the latest on the business day following the date on which we became aware of an unauthorised or incorrectly executed transaction, unless we have reasonable grounds to suspect fraud.

10.4 You will not be entitled to a refund for an unauthorised or incorrectly executed transaction if:

- you or the card user concerned did not inform customer services in accordance with clause 10.1;
- the unauthorised transaction is the result of: (i) fraud committed by you or by the card user; or (ii) the card user's failure, intentionally or by gross negligence, to comply with the security requirements relating to the card (as specified in clause 7 above).

If you are not entitled to a refund due to the above and we have already processed it, we will be entitled to deduct the amount of the refund from your available balance.

10.5 If the unauthorised transaction results from the loss, theft or misuse (i.e., use by someone else) of the card or security details, you will be liable for all costs of the unauthorised transaction.

10.6 Any refund received by you is your sole remedy and we will not be liable to you for any other loss suffered as a result of an unauthorised transaction.

10.7 If we have correctly processed a transaction authorised by the card user, but you or the card user decide to dispute the transaction and request a refund, the card user must contact the merchant who carried out the payment. If the merchant refuses to issue a refund, we may be able to raise the dispute with the card scheme and, if the dispute is successful, the card scheme may issue a chargeback on the card. We will handle all chargeback requests in accordance with the applicable card scheme rules and we cannot guarantee that chargebacks will be issued. Unless we receive the chargeback amount from the card scheme, we are not required to credit chargebacks to the card.

10.8 If we erroneously refund or credit a card, we are entitled to claim the corresponding amount to the card by deducting it from the available balance.

ARTICLE 11 — LIABILITY

11.1 References to liability in this clause 11 include any type of liability arising out of or in connection with these conditions, including, but not limited to, liability in contract, tort (including negligence), misrepresentation, restitution or otherwise.

11.2 Neither party may benefit from the limitations and exclusions set out in this clause with regard to any liability arising from its wilful default.

11.3 Nothing in these conditions excludes or limits our liability for death or personal injury caused by our negligence, our liability for fraud or fraudulent misrepresentation, or any other liability which the law does not allow us to exclude or limit.

11.4 We are not liable for:

- any matter arising out of or in connection with your relationship with Greenway (including with respect to the Greenway agreement) and/or any third party engaged by Greenway in connection with the card programme, or any loss or damage caused by other third parties;
- any dispute concerning the quality of goods or services purchased from a merchant that has accepted the card or additional charges billed by the operator of point-of-sale terminals or ATMs (e.g., where a card user is offered dynamic currency conversion at a point of sale);
- loss of profits, loss of sales or business, loss of agreements or contracts, loss of anticipated savings, loss of use or corruption of data or information, loss of or damage to goodwill, and any indirect or consequential loss;
- loss or damage that is not due to a breach of these conditions or of applicable laws;
- loss or damage caused by events beyond our control (or that of our agents or subcontractors) and that we could not have avoided (e.g., war or a strike);
- loss or damage caused by your or a card user's breach of these conditions or of any applicable law;
- loss or damage caused by goods or services purchased by means of a card, if a merchant refuses to accept a card or if an ATM or other cash withdrawal service provider refuses to accept the card; or
- was caused by a transaction declined due to an insufficient available balance to cover the amount of the transaction and all applicable fees.

11.5 Subject to clause 10.3 (refund of unauthorised transactions) and clause 11.3 (liability not excluded or limited), if we are held liable to you, our total liability to you under this agreement shall not exceed 10,000 euros.

11.6 You must notify us of your intention to bring a claim against us within 6 months from the date of the event giving rise to your claim. If you fail to do so, and subject to clause 11.3, we shall have no liability to you in connection with that event.

11.7 You shall indemnify us in full and on demand for any loss or damage we suffer (including any expenses and costs we incur, such as legal fees) as a result of a breach of these conditions, if we have to enforce any of the provisions of these conditions against you (for example, if you fail to pay us the sums owed to us), or if you or your card users use the cards fraudulently. You shall remain liable even after termination of this agreement.

11.8 If a card is defective or damaged due to our fault, our liability is limited to the obligation to replace the card and pay the shipping costs without charging you for the replacement. The defective card must be returned to us in its current state by registered mail.

ARTICLE 12 — OUR RIGHTS OF SUSPENSION

12.1 We have the right to refuse to process a transaction and/or to suspend one or all of the cards (as applicable) in exceptional circumstances such as:

- we suspect that the security of a card has been compromised in any way or that the card, the PIN or any other security information has been or is likely to be misused;
- if we have reasonable grounds to suspect that you or the card user concerned are engaging in fraudulent behaviour, are involved in illegal or unlawful activity (e.g., money laundering or terrorist financing) or are using the card for any other unlawful purpose;
- we are required to do so under applicable law or if we believe that continued use of the card may constitute a breach of applicable law;

- your access or that of the card user concerned to the user interface has been suspended or terminated, or if your Greenway agreement is terminated;
- if you or the card user concerned commit a serious breach of these conditions (serious breach includes repeated breaches);
- if we have reasonable grounds to believe that this is necessary for security reasons (e.g., any security issue affecting the user interface or card processing facilities);
- if the information you or the card user concerned have provided to us is false or incomplete, or if you or the card user concerned fail to provide us with information that we reasonably request;
- if we have asked you to pay us the money you owe us under these conditions and you have failed to do so despite a reminder;
- you suffer an insolvency event or you cease to carry on your activity;
- there is a significant risk that you will not be able to meet your payment obligations to Greenway under the Framework Contract;
- your Framework Contract concluded with Greenway, including the deferred payment arrangements, is suspended or terminated for any reason whatsoever;
- the card has not been activated during the notified activation period; or
- the card user concerned does not access their card during the period specified in the card programme description as the "card unused limit".

12.2 Where possible and appropriate in the circumstances, we or Greenway will inform you before your card is suspended. We will only reactivate a suspended card if we are satisfied that the reason(s) for the suspension is (are) no longer applicable. If we reasonably believe that the reasons for the suspension cannot be rectified, we shall have the right to cancel the card concerned.

ARTICLE 13 — TERMINATION

13.1 These conditions may be terminated at any time by you by sending at least thirty (30) days' written notice to customer services.

13.2 We may terminate these Conditions at any time and without giving you a reason by sending you at least thirty (30) days' written notice, which will normally be delivered to you by Greenway.

13.3 We may also terminate these conditions on shorter notice if we consider it appropriate in the exceptional circumstances listed in Article 12 and where the suspension of a specific Card account is not sufficient to remedy the circumstances. We, or Greenway on our behalf, shall inform you of the reasons why we have decided to terminate these Conditions.

13.4 Termination of these conditions means that all cards are cancelled.

13.5 Where a card has been cancelled, has expired or has been found after being declared lost or stolen, the card user concerned must destroy it by cutting it in two through the magnetic strip and the chip.

ARTICLE 14 — DATA PROTECTION

14.1 We are the controller of all personal data associated with the application for and use of the cards and we will collect certain information about the account holder and card users in order to operate the card programme. The provision of card users' personal data and the processing of such data by us are necessary for us to fulfil our obligations under these conditions. If you or the card users concerned do not provide the personal data we request, we may not be able to continue to provide our services to you or to provide our services to the card users concerned and we may refuse to accept a card application or activation, or even take steps to terminate these conditions.

14.2 We manage and protect your personal data and/or that of the card users in accordance with all applicable data protection laws. For full and detailed information on when and why we collect personal information about card users, on how we use it and on the conditions under which we may disclose it, please refer to our privacy notice which is provided to you at the time we collect your personal data and which is available on the following website: https://enfuce.com/privacy-and-data-protection/.

ARTICLE 15 — AMENDMENTS TO THESE CONDITIONS

15.1 If we have to make changes to these Conditions, we will ask Greenway to inform you of the new Conditions, or we will contact you directly, at least thirty (30) days before the changes are implemented. In exceptional circumstances, where it is impossible for us to give you at least thirty (30) days' notice (e.g., in the event of urgent legislative changes or changes required by the card scheme), the notice period may be shorter, but we will do our best to give you as much notice as possible ("change notice").

15.2 If we have to introduce changes that are less favourable to you than the conditions you agreed to by accepting these conditions, and you do not accept these new conditions, you may notify customer services that you refuse the new conditions proposed. You must notify customer services before the expiry of the change notice, i.e., before the date on which we propose to apply the new conditions. If we do not hear from you before that date, we will consider that you have accepted the changes and you will be deemed to have accepted the new conditions.

15.3 If you refuse the new conditions, this means that you terminate this agreement. Termination of this agreement in such circumstances will not be charged to you.

ARTICLE 16 — GENERAL

16.1 By accepting these conditions, you consent to this agreement and all information and notifications relating to the services provided to you under this agreement being drawn up in English.

16.2 The English version of these conditions shall prevail over any other language version we may publish from time to time.

16.3 All notices and communications between you and us will be in English. If we have to notify you of anything, we will normally communicate with you through Greenway. We may also use your email address or home address to send you notifications or communications. You must send all notices or communications via the user interface or contact customer services first. If you need to send us a notice or communication directly, you may do so by email to complaints@enfuce.com.

16.4 You are not entitled to transfer your rights or obligations under these conditions to anyone without our prior written consent. We may transfer our rights and obligations under these conditions to another company in our group without your consent, but we will inform you of the transfer and ensure that your rights are not affected by it.

16.5 Nothing in these conditions shall be construed as conferring on a third party any benefits or rights, including the right to enforce these conditions.

16.6 If any provision of these conditions (or any part of a provision) is or becomes illegal, invalid or unenforceable, the legality, validity and enforceability of any other provision of these conditions shall not be affected.

16.7 If you breach these conditions and we take no action, we may still exercise our rights and remedies in any other situation where you breach these conditions.

16.8 These conditions constitute the entire agreement between us.

16.9 This agreement is entered into between you and us and no one else has the right to rely on or enforce these conditions.

16.10 These conditions cancel and replace any prior agreement between us concerning the cards, including any written or oral agreement relating to the subject matter of these conditions.

ARTICLE 17 — COMPLAINTS

17.1 The card programme is managed by Greenway. If you wish to contact us or complain about any aspect of our service, please contact customer services.

17.2 If, after receiving a response from the customer services team, you are not satisfied with the outcome, you may address your complaint to us at the following address: complaints@enfuce.com.

17.3 We will do our utmost to find a solution to your complaint. If we are unable to resolve your issue to your satisfaction, we will explain the reasons for our decision.

ARTICLE 18 — LAW AND JURISDICTION

18.1 These conditions and any dispute arising therefrom shall be exclusively governed by and construed in accordance with the laws of Finland and subject to the exclusive jurisdiction of the courts of the Helsinki district.

ANNEX 11 — ARIA: DEBTOR GENERAL TERMS — NOTIFICATION OF ASSIGNMENTS OF RECEIVABLES

1. DEFINITIONS

Capitalised terms in these Debtor General Terms are defined below.

"Assignor" or "Greenway": designates the simplified joint-stock company whose registered office is at 5 rue Pleyel, 93200 Saint-Denis, registered with the RCS of Bobigny under number 978 860 062. In the context of its activity, Greenway markets payment cards issued by Enfuce License Services Ltd and grants its Clients, on an ancillary basis to the Services, a deferred payment facility for the settlement of Transactions carried out by means of the Card, in accordance with Article L.511-7, I, 1° of the French Monetary and Financial Code. The commercial receivables resulting from this deferred payment are assigned to the Assignee in accordance with these Debtor General Terms.

"Assignee": designates Aria, simplified joint-stock company whose registered office is at 5 rue Pleyel, 93200 Saint-Denis, registered with the RCS of Bobigny under number 839 836 608, or any other person substituted by Aria.

"Client": designates any legal entity that has subscribed to the deferred debit card payment service offered by Greenway and has accepted the Debtor General Terms.

"Receivable": designates a commercial receivable of Greenway against the Client, arising from the deferred payment granted for the settlement of Transactions carried out by means of the Cards.

"Assigned Receivable": designates a commercial receivable of Greenway against the Client, under the deferred payment granted for the settlement of Transactions carried out by means of the Cards.

"Debtor General Terms": designates these general terms of assignments of Receivables.

"Aria Service" designates the advance payment of Receivables by the Assignee in consideration of the acquisition by the latter of the Receivables held by the Assignor against a Client.

2. PURPOSE

A framework agreement for the assignment of receivables has been concluded between Aria and Greenway concerning the Aria Service.

Under this agreement, the Assignor undertook to assign to the Assignee the Receivables of which it is the holder against the Client, subject to all the conditions set out in this agreement being fully met, in particular the compliance with certain eligibility criteria. The assignment of each Receivable takes place when Greenway communicates the payment operation files to Aria via Aria's API or dashboard. The Debtor General Terms aim to inform the Client of the assignment of the Assigned Receivables to the Assignee.

3. ASSIGNMENTS OF RECEIVABLES

The Client undertakes to pay all sums due in respect of each Assigned Receivable of which it is the debtor, directly to the Assignee in accordance with the instructions communicated to it.

In the event of non-repayment of the sums due in respect of such Receivable, the Assignee may initiate any recovery procedure, amicable or judicial, against the Client in order to obtain payment of the sums due, including by implementing conservatory measures.

Any amount paid into the hands of the Assignor or of any other third party after notification of the assignment shall not be discharging, and the Client shall remain liable for the full amount of its debt towards the Assignee.

4. PERSONAL DATA PROTECTION

Collection and processing of personal data: In the performance of this contract, Aria may be required to collect and process personal data concerning the Client. This data may include, without limitation, information such as name, email address, postal address, phone number, etc. Aria undertakes to collect and process this data in accordance with the provisions of the General Data Protection Regulation (GDPR) and the national laws in force on data protection.

Purposes of data processing: The personal data collected by Aria are used in the context of the performance of the assignment of receivables, as well as in compliance with the legal and regulatory obligations incumbent upon Aria.

Data retention: Aria shall retain the personal data only for the duration necessary to achieve the purposes for which they were collected, unless a longer retention period is required by law.

Data security: Aria implements the appropriate technical and organisational measures to ensure the security and confidentiality of the personal data, in order to prevent any loss, alteration, unauthorised disclosure or unauthorised access to this data.

Rights of data subjects: In accordance with the GDPR, the persons concerned by the processing of their personal data benefit from the following rights: right of access, right of rectification, right to erasure, right to restriction of processing, right to data portability, right to object to processing. They may exercise these rights by contacting Aria at the contact details provided below.

Data transfer: Aria undertakes not to transfer the personal data collected to third parties without the prior consent of the data subject, unless such transfer is necessary to perform its contractual obligations or is required by law.

Contact: An independent Data Protection Officer (DPO) has been appointed to best ensure the protection and integrity of the Client's data. For any question concerning the collection, processing or protection of personal data, the Client may at any time and free of charge contact Aria's DPO at the following address: privacy@helloaria.eu.

5. APPLICABLE LAW

This deed of acceptance is governed by and construed in accordance with French law. The resolution of any dispute or difference whatsoever between the Client, the Assignor, the Assignee and/or Aria, in the context of or arising out of this deed of acceptance, in particular with regard to its existence, validity, interpretation or performance or non-performance, shall be subject to the exclusive jurisdiction of the Paris Commercial Court, even in the event of summary proceedings, third-party proceedings or multiple defendants, whether the basis is contractual or tortious.