

GENERAL TERMS OF USE AND SALE v6.4

Last update: July 2026

IMPORTANT NOTE: The French version of this document shall govern our relationship - this translated version is provided for convenience only and shall not be construed as a modification of the French version. The French version can be found on the following page:

Table of contents

1	Purpose	3
2	Definitions.....	3
3	Creating and closing an account - cancelling an account	5
4	Swik request.....	7
5	Acceptance or Refusal of a Swik – Option to subscribe to the Zen Security Deposit	8
6	Closure of a Swik	10
7	Financial conditions.....	12
8	Right of recourse in the event of contesting an Activation Request for a Swik.....	14
9	Services provided by the Company.....	15
10	Obligations and liability of the Company.....	17
11	Obligations and liability of the User	19
12	Intellectual property.....	21
13	Objection to a transaction by a User	21
14	Personal data.....	21
15	Management of cookies	26
16	Language	26
17	Conditions applicable to offers and Trial Periods	27
18	Applicable law and jurisdiction.....	27
19	Distinctive features of use of the Service via an API	27
20	Distinctive features of the Service due to the Supplier belonging to a network/partnership	27

21	Security Deposit Insurance Service	28
22	Reversibility.....	28
APPENDIX 1.	COMPENSATORY PAYMENT - Table of SERVICE ACTIVATION REQUESTS	30
APPENDIX 2.	General collection mandate	33
1	Purpose.....	33
2	Acceptance of the Mandate	33
3	Guarantees	33
4	Obligations of the Company	33
5	Obligations of the Supplier	34
6	Duration and expiry of the Mandate	34
7	Transfer of the amounts collected	34
8	Fees.....	34
APPENDIX 3.	GENERAL AGREEMENT ON THE PROCESSING OF PERSONAL DATA	35
APPENDIX 4.	Mangopay PAYMENT SERVICES MASTER AGREEMENT	42
APPENDIX 5.	MANDATE FOR THE MANAGEMENT OF THE MANGOPAY ACCOUNT	43
1.	Purpose.....	43
2.	Acceptance and Content of the Mandate.....	43
3.	Revocation of the Mandate	43
4.	Responsability.....	43

1 Purpose

The present General Terms of Use and Sale detail the rights and obligations of SWIKLY (hereinafter referred to as the “Company” or “Swikly”) and of all users of the Swikly service (hereinafter referred to as the “Service” and the “Users”) accessible after downloading the application on any smartphone or on the responsive website www.SWIKLY.com (hereinafter referred to as the “Website”) or via any other third party website that makes it possible to use the Service via an API (hereinafter referred to indiscriminately as the “Application”). In the latter case, the specific stipulations of Article 19 will apply to the User concerned.

2 Definitions

- **Swikly API** refers to the application programming interface made available where appropriate in order to use the Service via any other application, Website or platform, under the conditions specified in Article 19;
- **Application:** has the meaning defined in Article 1;
- **Deposit** refers to payment of an amount by a Customer in order to indicate their intention to buy or rent a property or service from a Supplier or to guarantee the full payment of a property or service; deposits are understood as defined in Article L214-1 of the French Consumer Code unless otherwise stated in the Supplier’s general terms and conditions;
- **Supervisory authority:** has the meaning given in the GDPR;
- **Security Deposit** refers to the security deposit paid by a Customer to a Supplier to guarantee the return of a property in good condition; the Security Deposit is understood according to its standard meaning; consequently the Users must take the usual precautions to ensure that the security deposit is effective, and in particular Users must carry out an inventory of fixtures of the property before and after renting it, to avoid any disputes;
- **Customer** refers to the people who want to buy, rent a property or service, or pay a security deposit via the Service;
- **Payment Commission:** refers to the expenses due to the Company in the event of use of the Single Payment function.
- **General Terms** refers to the present document and all of its appendices which constitute an integral part of it;
- **Debts:** refers to the debts of Suppliers that the Company is required to collect from Customers who have accepted a Swik on the Application, for which a request for Collection has been made by the Supplier but which has not been successful for various reasons (fraudulent card, chargeback, insufficient funds, etc.);
- **Personal Data:** has the meaning given in the GDPR;
- **Period of Validity** refers to the period during which the Swik issued by a Supplier is valid, once it has been accepted by the Customer. By default, the Period of Validity of a Swik is a maximum of six (6) months. It can be configured by the Supplier. In any case, the Period of Validity must cover the planned date of delivery of the property or provision of the service in the event of a purchase, or of the expiry of the lease, or more generally the collection period of the sum concerned. Consequently, the Supplier who requests the Swik is alone responsible for determining a sufficiently long Period of Validity in view of the transaction concerned;
- **Collection of a Swik** refers to the actual transfer of all or part of the Customer’s Deposit, Guarantee, Security Deposit or Invoice to the Supplier, that was previously secured by a Swik in accordance with Article 6.a);
- **Supplier** means any person who wishes to sell a property or service of any kind whatsoever, rent a property or receive a security deposit for the renting of a property, via the Service; the Supplier within the meaning hereof can also be the authorised agent of a seller or lessor of a property who has been entrusted by it with some or all of the missions relating to the sale or lease. The Supplier can be a natural person or a legal entity; it can be a private individual, a professional or a public institution;
- **SWIKLY Collection Charges** refers to the charges owed by the Supplier to the Company in the event of Collection of a Swik;
- **SWIKLY Service Charges** refers to the service charges owed by the Supplier or by the Customer, depending on the case, to the Company during creation of a Swik;
- **Guarantee** refers to the deposit of an amount made by the Customer with a Supplier in order to guarantee full payment of a property or service;

- **Mandate:** means the mandate for the collection of Debts entrusted to the Company by the Supplier included in APPENDIX 2 or the one for managing the MangoPay account in APPENDIX 5
- **MangoPay** refers to the electronic money institution approved and registered in Luxembourg under registration number B173459, a subsidiary of Crédit Mutuel, whose head office is located at 10 boulevard Royal, L-2449 Luxembourg, which the Company uses to provide payments in electronic money for the purposes of the Service;
- **SWIKLY Trademark** refers to the French trademark No. 4200552 and the EU trademark No. 15010291;
- **Total Amount of the Swik** refers to the amount of the Deposit, Guarantee, Security Deposit or Invoice that is subject to a payment commitment due to the issue of a Swik or an actual transfer of the total amount of the Customer's Deposit, Guarantee, Security Deposit or Invoice if the Supplier has chosen that option or in the event of a request for Collection of a Swik by the Supplier that is justified; in any case, the Total Amount of the Swik cannot exceed two thousand five hundred euros (€2,500), and the total amount is adapted according to the offer negotiated between the Supplier and the Company. In exceptional cases, the company can grant a maximum Total Amount of a Swik of five thousand euros (€5,000);
- **Single Payment** refers to the immediate transfer of money from a Customer to a Supplier to pay for a transaction, following a request made via the Application in accordance with Article 7.e);
- **Trial Period:** has the meaning indicated in Article 17;
- **Permalien** refers to a permanent link issued by the Company on behalf of the Supplier, which the Supplier can use for each of its Customers, by sending it to them by email at the time of confirmation of the sale or lease, and enabling them to accept the Swik. All clicks on a Permalien generate SWIKLY Service Charges at the time of acceptance of the Swik as defined in Article 5. A Supplier can use several Permalien;
- **Data Subject:** has the meaning given in the GDPR;
- **Third Party Platform:** has the meaning indicated in Article 19;
- **Invoice:** means the invoice payable by the Customer to the Supplier following the provision of a service;
- **Service Activation Request:** has the meaning indicated in Article 6.a/b/;
- **Data Controller:** has the meaning given in the GDPR;
- **GDPR:** refers to the General Data Protection Regulation No. 2016/679 of the European Parliament and of the Council of 27 April 2016;
- **Service:** has the meaning indicated in Article 1;
- **Security Deposit Insurance Service:** refers to the insurance product distributed by the Company;
 - **Standard Security Deposit Buy-Back:** refers to the insurance product distributed by the Company that may be offered to the Customer after the deposit of its Swik and that allows the Customer to be reimbursed for a debit on its bank card following an Activation Request;
 - **Shield Security Deposit Buy-Back:** refers to the insurance product distributed by the Company that may be offered to the Customer after the deposit of its Swik and that allows the Customer to avoid a debit on its bank card in the event of an Activation Request;
 - **Zen Security Deposit:** refers to the insurance product distributed by the Company that may be offered to the Customer at the time of the deposit of its Swik and that allows the Customer to avoid a debit on its bank card in the event of an Activation Request;
- **Website:** has the meaning indicated in Article 1;
- **Company:** has the meaning indicated in Article 1;
- **Processor:** has the meaning given in the GDPR;
- **Subprocessor:** means any Company affiliated or not with SWIKLY which the Processor may call upon to carry out the Processing activities;
- **Swik** refers to any commitment notified to a Customer to confirm that their request to buy or rent a property or service, including a subscription, or to pay a Security Deposit in connection with the renting of a property, or to pay a Guarantee in connection with the sale or renting of a property or a service or to pay an Invoice, has been taken into account. It results either in the Company providing pre-authorisation of the debit of a specific amount, without any cash transfer taking place between the Users, or in the actual transfer of the total amount of the Deposit, Guarantee, Security Deposit or Invoice, from the Customer's account to the electronic purse managed by MangoPay and allocated to the Supplier, in the event that the Supplier has

chosen the actual transfer option described in Article 4. b) or in the event of a request for Collection of a Swik by the Supplier that is justified;

- **Processing:** has the meaning given in the GDPR;
- **User** has the meaning set out in Article 1; it means the user of the Services at the Supplier and the Customer;
- **Personal data breach:** has the meaning given in the GDPR.

3 Creating and closing an account - cancelling an account

Before being able to use the Service, the Supplier must download the Application free of charge or access the Application via the Website. It must then register via the Application and open an account in its name. Accounts can be created by any natural person who has full legal capacity and a bank card in their name, and any legal entity whose legal representative has full legal capacity, and has a bank card in its name. Natural persons or legal entities can only open one account in their name via the Application. Creation of an account implies full acceptance of the present General Terms, including APPENDIX 4 which provides the general terms and practical details and APPENDIX 5 authorising the Company to manage the account for the Supplier, which is confirmed by clicking on Accept when creating the account. The General Terms are made available to the Supplier when the account is created, before finalising the account and the aforementioned acceptance. A Supplier that is a legal entity undertakes to require any authorised person within its company to accept the General Terms by clicking on Accept. In any case, any start of performance hereof constitutes ratification of the General Terms by all of the Parties. The General Terms and Conditions are accepted by the Provider at the time of the creation of their account and are intended to apply to each subsequent Swik request made by the Provider.

Customers do not need to create a Swikly account to use the Service. They must nevertheless accept the General Terms when they accept a Swik under the conditions specified in Article 5.a/ below, as well as the general terms of MangoPay, and when they are charged the SWIKLY Service Charges.

The User can print or save the General Terms after reading them. The Company reserves the right to change the General Terms at any time. For each new version of the General Terms and Conditions, the Company shall send them by email to the Provider, who shall be deemed to have read and accepted them within 48 hours following the sending of the message.

The Customers will be informed when they next accept a Swik. Users who accept the General Terms subject to reservations, or do not accept the General Terms, cannot access the Application or use the Service.

In the event that the Service is offered within a third-party service, the Company's General Terms and Conditions may be incorporated into the contractual framework of the said third-party service. In such a case, they shall be deemed accepted and shall be binding upon the Users.

When creating an account, any Suppliers who wish to use the Service must declare whether they are (i) a private individual, (ii) a professional or (iii) an association. Any private individuals or associations who wish to use the Service for their ordinary activities, must declare that they are professionals. Any failure to declare that capacity shall be unenforceable if it can be shown, in particular in the event of a dispute with another User or with the Company, that the Supplier concerned actually used the Service in connection with its professional activity.

When creating the account, the Supplier must provide all of the information indicated as compulsory, and if necessary the related documentary evidence. In any case, the Supplier undertakes to provide accurate information and update it regularly. This information remains confidential, apart from the information (i) that may be required by MangoPay to open a MangoPay account, in accordance with the conditions of MangoPay included in APPENDIX 4 hereto, (ii) that the Supplier has deliberately chosen to make visible and (iii) that the Supplier is required to make visible in accordance with the law. By default, the Supplier's first name and surname or its trade name must in any case be accessible enable its Customer to use the various functions of the Service under optimum conditions. The Supplier acknowledges that in the event of insufficient, inconsistent or out-of-date information, the Company may refuse to provide or suspend the Service, without giving rise to any right to compensation.

Suppliers who agree to link their SWIKLY account to their other social network accounts such as in particular, LinkedIn®, Facebook® etc., declare that they have accepted that other personal data may be accessible which the Company cannot check or be liable for. Suppliers must read the general terms of use of these social networks which

explain the use of users' personal data and make it possible to check the personal data that are visible. The SWIKLY account is personal to each Supplier, and the Supplier cannot on any account transfer it to a third party.

When opening the SWIKLY account or if the Supplier wishes to take full advantage of all of the functions of the Service (including when a Swik is requested in accordance with Articles 4 and 5), it must enter its bank card payment details. In this case, the Company will request a pre-authorisation for a total of one (1) euro in order to check that the Supplier's card actually belongs to them.

Once its SWIKLY account has been opened, the Supplier can ask the Company at any time to issue a Permalien. The Supplier can make a Permalien available to each Customer that is specific to the Customer, to enable the Customer to accept a Swik. The functioning and payment of Permalien are described in Article 5.c).

Suppliers are notified that if they make the Permalien available directly on their website, they take the risk that the Permalien will not be used by actual customers. The Suppliers must cover the financial cost of untimely use by a third party by paying the SWIKLY Service Charges, even if they have opted for payment of the aforesaid Charges by the Customer.

Since the Service is based on the use of MangoPay electronic purses, the Supplier is expressly informed and accepts that the Company will use the electronic purse opened in the Supplier's name, managed by MangoPay. A mandate is expressly entered into between the Provider and the Company, authorizing the Company to manage, on the Provider's behalf, the MangoPay account thus opened. The Mandate is set out in APPENDIX 5 of the General Terms and Conditions. Regarding the Customer, SWIKLY reserves the right to open an electronic purse in its name for the purposes of the Service. The Supplier accepts the general terms and practical details of MangoPay (APPENDIX 4) by ticking a box when it opens its SWIKLY account. The Customer accepts them when it accepts a Swik, in accordance with Article 3. If there is a contradiction between the general terms and/or practical details of MangoPay (APPENDIX 4) on the one hand and the General Terms on the other, the latter shall have precedence, unless otherwise provided by law.

The opening of the SWIKLY account by the Supplier is confirmed by an email sent by the Company to the Supplier. Moreover, SWIKLY reserves the right to ask the Supplier at its discretion, for any documents and information that it considers necessary in order to complete the registration, and creation of the account may be dependent on receipt of these documents and information. Collection of this information and these documents is subject to obtaining the Supplier's consent, and more generally the provisions of Article 14 Personal Data.

Throughout the period of validity of its SWIKLY account, the Supplier is responsible for keeping its username and password confidential and for the use that is made of its account, and must take all of the usual precautions to regularly change its password. In the event of loss or discovery of an intrusion into its account, the Supplier must immediately change its password or follow the security procedure proposed by the Company to recover its username or password.

After opening the SWIKLY account, the Supplier can access all of the functions of the Service.

Suppliers can decide to close their account at any time: in this case they must send an email to the Company at the following address: contact@swikly.com. The account closure date is the date of receipt by the Company of the email requesting closure, unless there is a valid Swik at the time of closure. In this case, the account will be closed at the end of the transaction concerned by the Swik.

In the event that a SWIKLY account remains inactive for more than twenty-four months, the Company will send an email alert to the Supplier asking it whether it wishes to keep its account or close it. If there is no response from the Supplier, Swikly will close its account. In case of funds present on the SWIKLY account, the Company will be entitled to collect these funds not claimed by the Supplier before closing the SWIKLY account.

Similarly, if a Client's electronic wallet contains funds that are blocked by MangoPay for any reason whatsoever, or if the Client fails to request the transfer of the available funds, the Company shall be entitled to dispose of said funds after a period of 13 months.

In the event of a serious breach by a User of any of their commitments under the present General Terms that is not remedied within fifteen (15) days of receipt of a registered letter with acknowledgement of receipt or an email with a delivery receipt from the Company, the Company shall be entitled to suspend or cancel the account of the User concerned, depending on the seriousness of the acts, or if necessary to ban use of the Service. The letter or email will indicate the acts concerned. In addition, it will be impossible for the User to access their account and/or the functions of the Service, without prejudice to any other damages that the Company may claim. In the event of a manifestly unlawful disturbance or violation, the time limit to remedy the breach may be shorter.

4 Swik request

a/ General remarks

A Swik can be requested by the Supplier in the form of a Swik Deposit if it is intended to ask the Customer to confirm a commitment to buy a property or service, or to rent a property. A Swik can be requested by the Supplier in the form of a Swik Guarantee if it is intended to cover full payment of property or a service in the event of non-payment by the Customer. A Swik can be requested in the form of a Swik Security Deposit if it is intended to ask the Customer to undertake to keep the property rented in the condition in which it was received. A Swik can be requested in the form of a Swik Invoice if it is intended to cover the payment of a sum that remains due by the Customer to the Supplier.

The Swik request is made by the Supplier who fills in a form directly in its Supplier account on the Application or sends a request to the Company to create a Swik via its Supplier account. To create the Swik, the Company must obtain the following information from the Supplier or the Customer: surname, first name, email address, telephone number, date of birth and postal address of the Customer.

In any case, the Supplier undertakes to check the aforementioned information and guarantees that it complies with the requirements of Article L 111- 1 of the French Consumer Code and with the requirements for pre-contractual and/or contractual information resulting from any specific regulations applicable to the planned transaction. The Customer undertakes to provide information that is accurate and up-to-date.

The Swik requested must include the Supplier's identity and all of the compulsory information in accordance with Article L111-1 of the French Consumer Code and with any specific regulations applicable to the planned transaction if the Supplier is a professional. If the Supplier is not a professional, the Swik must include the Supplier's first name and surname. The Supplier acknowledges that this disclosure is required for proper use of the Service: it cannot on any account call it into question or hold the Company liable due to this disclosure. Validation by the Supplier of all of the information contained in the Swik constitutes confirmation of the Swik request and implies confirmation of acceptance of the present General Terms, and in particular acceptance, where appropriate, by the Supplier of payment of the SWIKLY Service Charges to the Company if the Swik requested is accepted by the Customer.

The transaction is indicated in the Application as "Pending acceptance".

The Swik takes the form of a URL link and is sent to the Customer by the Company or by the Supplier, for acceptance via an email or SMS. The Supplier guarantees the Company that it has the Customer's authorization to receive SMS messages from the Company.

The Supplier is informed of, and expressly accepts, that the Company offers the Customer insurance products that it distributes in its capacity as broker, in connection with the acceptance of the Swik (Standard Security Deposit Buy-Back, Shield Security Deposit Buy-Back or Zen Security Deposit).

b/ Option for actual transfer of the total amount of the Customer's Deposit or Security Deposit

When creating the Swik, the Supplier has the option to transfer the total amount of the Deposit or Security Deposit from the Customer's account to the electronic purse managed by MangoPay and allocated to the Supplier.

The Supplier acknowledges that this option generates SWIKLY Service Charges which it agrees to pay by accepting these General Terms.

If the Supplier has decided to charge some or all of the SWIKLY Service Charges to the Customer, the amount will be notified to the Customer by the Company, and the Customer expressly agrees to make this payment by accepting these General Terms.

Furthermore, Customers will be informed that the total amount of the Deposit or Security Deposit will be transferred when they accept the Swik.

5 Acceptance or Refusal of a Swik – Option to subscribe to the Zen Security Deposit

Customers who receive a Swik request sent to them will receive an email or SMS containing the information relating to the Swik and a link enabling them to accept it within a specific time limit. The email or SMS will also contain a link enabling them to read, download and print out the General Terms and if necessary the Supplier's general terms of sale or service, before accepting the Swik. In any case, the Customer can accept or refuse the Swik:

a/ Acceptance of the Swik:

If the Customer wishes to accept the Swik, they must click on the link included in the email or SMS they have received.

The Customer must then (i) approve all of the characteristics of the proposed transaction and the Total Amount of the Swik, (ii) indicate at least their surname, first name and all of the information expressly requested by MangoPay, (iii) enter their bank card number, and after reading them, (iv) accept these General Terms and the Supplier's general terms of sale or service, by ticking the appropriate box.

The use of certain bank cards does not make it possible to provide the bank guarantee required to use the Service. In this case, to enable Customers to finalise acceptance of the Swik, they can select the following option: Customers can agree to the actual and immediate transfer of the total amount of the Swik concerned. They will then be immediately debited the total amount, as well as, where appropriate, the related SWIKLY Service Charges which will be notified to them when they accept the Swik.

The Company will send a Swik acceptance confirmation email to inform both of the Users concerned.

In the event of acceptance of the Swik, both of the Users concerned will no longer be able to question the characteristics of the proposed transaction: from then on the Customer and Supplier are contractually bound to carry out the transaction which is shown as "Active" in the Application: the Swik remains effective throughout the Period of Validity.

If the Supplier has decided to charge some or all of the SWIKLY Service Charges to the Customer, the amount will be notified to the Customer by the Company, and the Customer expressly agrees to make this payment by accepting these General Terms.

Acceptance of the Swik means that the SWIKLY Service Charges must be paid to the Company by the Supplier, and/or where appropriate, by the Customer, under the conditions defined in Article 7. b).

Each time a Swik is accepted, the Company guarantees the Supplier that it will carry out the following checks:

- Check of the validity of the bank card used by the Customer, to limit the use of stolen or lost cards;
- Check of the identity of the card holder by 3-D Secure authentication;
- Check that the bank card expiry date matches the dates of the rental of goods or services by the Customer from the Supplier and more generally of the Period of Validity of the Swik;
- Check of the type of bank card used by the Customer to prevent the use of Maestro and Prepaid cards that do not make it possible to debit a deposit;
- Total or partial check of the payment limit of the bank card used by the Customer.

Acceptance of the Swik by the Customer also leads to its acceptance, in the event of a request for Collection of the Swik justified by sufficient documents, that the Company will be responsible, on the Supplier's behalf, for collecting the funds from the bank card registered by the Customer. The Company undertakes to repeat its attempts to debit the card in the event of failure. In this case, the procedure described in Article 8 will apply.

The Company undertakes to make every effort to carry out the controls and checks specified above. By express agreement, these commitments are solely an obligation of best efforts. The Company does not provide any guarantee concerning the result of these controls and checks and cannot be held liable in the event of non-payment by the Customer.

b/ Zen Security Deposit in the case of a Security Deposit Swik

Where the purpose of the Swik is to secure a security deposit, the Company offers the Customer the choice of either depositing a Swik or subscribing to the Zen Security Deposit. This choice is offered to the Customer at the time they accept the Swik on the Application. The Zen Security Deposit is an insurance product distributed by the Company and underwritten by the insurer Seyna. Seyna is responsible for the compliance of the Zen Security Deposit with applicable regulations. Where the Customer opts for the Zen Security Deposit, their bank card is nevertheless pre-authorised by the Company, as is the case for a standard Swik.

As part of subscribing to the Zen Security Deposit, the Customer signs a contract with the insurer under which they grant the Supplier a mandate to report a claim to the insurer in the event of a Service Activation Request. The Company is not a party to the contract signed between the Customer and the insurer. The Company acts as the distributor of the insurance product and as the insurer's agent for managing the product. The Company's liability cannot be sought in the event of a dispute between the Customer and the insurer, within the limits of applicable regulations.

The claim report made by the Supplier will trigger the application of the Zen Security Deposit by the insurer.

The cases excluded from the Zen Security Deposit are identified in the information documentation provided by the insurer when subscribing to the Zen Security Deposit.

Where the claim reported by the Supplier was excluded from the Zen Security Deposit by the insurer, the Customer acknowledges that the Company shall be entitled to operationally execute the Swik, under the conditions described in Article 6.a) of these General Terms. Accordingly, if the claim reported by the Supplier is excluded from the Zen Security Deposit by the insurer, the Customer's bank card will be debited up to the Swik Amount and the Supplier will receive the corresponding funds.

The Company's liability may under no circumstances be sought where the insurer decides to exclude the claim from the Zen Security Deposit, the insurer being solely responsible for the performance of the contract entered into with the end Customer.

c/ Refusal of the Swik:

The Swik request may not be accepted by the Customer if they decide that the characteristics of the Swik do not meet their expectations, or if they do not accept these General Terms or the Supplier's terms of sale or service. In this case, the Swik is deemed to have been "refused" and the Customer must not fill in the form that opens after clicking on the link included in the SMS or email received: the Customer must not give their bank card number or accept the General Terms.

Furthermore, the Swik is automatically deemed to be "refused" at the end of the acceptance period, if it is not expressly accepted by the Customer.

In the event of refusal of a Swik, the Company immediately informs the Supplier. The transaction concerned is then abandoned. The SWIKLY Service Charges are not due.

d/ Acceptance of the Swik via the Permalien:

The Supplier can ask the Company to create a Pernalien at any time. The Supplier must inform the Company of the characteristics of the required Pernalien.

The Company will configure the Pernalien in accordance with the characteristics notified by the Supplier, and send the Pernalien to the Supplier.

The Supplier makes the Pernalien available to its Customer by email, SMS or on its website etc.

The Customer can accept the Swik by clicking on the Pernalien within a fixed time limit (maximum one year). The Pernalien enables the Customer to read, download and print out the General Terms and if necessary the Supplier's general terms of sale or service, before accepting the Swik. In any case, the Customer can accept or refuse the Swik.

Acceptance of the Swik means that the SWIKLY Service Charges must be paid to the Company by the Supplier, or where appropriate, by the Customer, under the conditions defined in Article 7. c).

Customers who click on the Pernalien must then (i) approve all of the characteristics of the proposed transaction and the Total Amount of the Swik, (ii) indicate at least their surname, first name, email address, phone number and all of the information expressly requested by MangoPay, (iii) enter their bank card number, and (iv) after reading them, accept these General Terms and the Supplier's general terms of sale or service, by ticking the appropriate box.

The Supplier will receive confirmation of acceptance of the Swik by email and will be sent the information provided by the Customer (surname, first name, email address, phone number).

The Pernalien can be cancelled by the Company at the Supplier's request or by decision of the Company at any time in the event of failure to comply with the General Terms.

The use of certain bank cards does not make it possible to provide the bank guarantee required to use the Service. In this case, to enable Customers to finalise acceptance of the Swik, they can select the following option: Customers can authorise the immediate debit of the total price of the Swik concerned, and will be immediately debited that amount, as well as the related Service Charges which will be notified to them when they accept the Swik.

The Company will send a Swik acceptance confirmation email to inform both of the Users concerned.

In the event of acceptance of the Swik, both of the Users concerned will no longer be able to question the characteristics of the proposed transaction: from then on the Customer and Supplier are contractually bound to carry out the transaction which is shown as "Active" in the Application: the Swik remains effective throughout the Period of Validity.

If the Supplier has decided to charge some or all of the SWIKLY Service Charges to the Customer, the amount will be notified to the Customer by the Company, and the Customer expressly agrees to make this payment by accepting these General Terms.

Acceptance of the Swik means that the SWIKLY Service Charges must be paid to the Company by the Supplier, and/or where appropriate, by the Customer, under the conditions specified in Article 7.c/.

6 Closure of a Swik

A Swik can be closed after it has been accepted by the Customer in accordance with Article 5 paragraph a), in one of the three following cases:

a/ On the Supplier's initiative by a request for Collection of a Swik

The Supplier can decide to request the Collection of a Swik, i.e. collection of some or all of the Total Amount of the Swik. In this case it must indicate via the Application the reason for the collection and provide any documents justifying the request for Collection of a Swik (invoices, quotations, photos of damage etc.). Within this context, the

Supplier must do its best to provide the probative and contradictory supporting documents. A request for Collection of a Swik by the Supplier constitutes a "Service Activation Request" against the Customer. The request for Collection of a Swik by the Supplier constitutes acceptance of the General Terms and in particular of payment of the SWIKLY Collection Charges by the Supplier to the Company.

On receipt of the request, the Company can ask the Supplier to indicate the reason for the Claim and to complete its request with additional supporting documents.

Once the request for Collection of a Swik is complete, the request for Collection of a Swik is processed by the Company. At the same time, confirmation is sent to the Supplier and notice is sent by the Company to the Customer by email, to inform the Customer of the Collection of the Swik and of their right of recourse in accordance with Article 8.

In the event of Collection of the Swik: the SWIKLY Collection Charges are owed by the Supplier to the Company. The Total Amount of the Swik actually paid must correspond to the Collection of the Swik requested by the Supplier. The SWIKLY Collection Charges will however be paid by direct debit from the Supplier's bank card or debited from its bank account at the start of each calendar month, and in a single instalment if other SWIKLY Service Charges or SWIKLY Collection Charges are due.

The Swik will be closed once the Total Amount of the Swik has been collected by the Supplier (the Total Amount of the Swik may be collected via several Swik Collection requests) or once its Validity Date has expired.

In certain cases, SWIKLY may suspect fraudulent use of the Customer's bank card to accept a Swik, based on corroborating and objective pieces of evidence. In this case, the Users will be informed that SWIKLY is obliged to inform MangoPay which will block the Total Amount of the Swik and the electronic purse(s) of the Users concerned. The Total Amount of the Swik will not be transferred to the Supplier's bank account and the payment order will be permanently blocked.

In the event of fraudulent use of a bank card, and if at the end of the statutory time limit for chargebacks of thirteen months, the holder of the bank card has not exercised their right to a chargeback, the Total Amount of the Swik will be permanently forfeited by the Supplier and received by the Company in respect of its Service Charges. The Supplier will be free to instigate any legal action it is entitled to take against the Customer behind the fraud.

b/ On the Supplier's initiative by a cancellation request

The Supplier can decide to cancel the Swik, and this cannot on any account be challenged by the Customer. This cancellation constitutes closure of the Swik.

In this case, if the Swik is a Swik Security Deposit, this involves the Supplier cancelling the virtual deposit cheque: the Customer is informed of this by email and is therefore no longer bound by the transaction for the Total Amount of the Swik.

In the case of a Swik Deposit, cancellation allows the Supplier to retract and, unless otherwise stated in the Supplier's terms of sale, the cancellation has the scope specified in Article L214-1 of the French Consumer Code.

In the case of a Swik Guarantee or Invoice, this involves the Supplier cancelling the virtual cheque guaranteeing full payment of the goods or service: the Customer is informed by email and is therefore no longer bound by the transaction for the Total Amount of the Swik.

The Supplier alone is liable for its decision to cancel a Swik and for any consequences of it.

On no account can the Supplier or Customer hold the Company liable for the consequences of cancellation of a Swik on the Supplier's initiative.

c/ At the end of the Period of Validity of a Swik

Since all Swiks have a Period of Validity set by the Supplier that requested the Swik, the Swik is automatically closed within a time limit of twenty (20) days from the expiry date, unless a specific request is made to the Company. Users are informed when the Swik is closed.

7 Financial conditions

a/ Supplier's electronic purse

Each Supplier is allocated an electronic purse managed by MangoPay, in order to make the payments provided for under the present General Terms. It makes it possible to collect the amounts due to the Supplier following Collection of a Swik. The Supplier grants a mandate to the Company to manage the account (APPENDIX 5).

b/ Customer's electronic purse

Each Customer may be allocated an electronic purse managed by MangoPay, in order to make the payments provided for under the present General Terms. This makes it possible to temporarily deposit in it the amounts due to the Supplier following collection of a Swik.

c/ Acceptance and payment of SWIKLY Service Charges and SWIKLY Collection Charges

Issue of a Swik by a Supplier implies one-click acceptance of the General Terms. This acceptance therefore constitutes acceptance of payment by the Supplier of the SWIKLY Service Charges relating to use of the Application, once the Swik has been accepted by the Customer, unless the Supplier has chosen the "Customer Pays" option, whereby the SWIKLY Service Charges are borne by the Customer. The date of acceptance of the Swik by the Customer constitutes the due date of the SWIKLY Service Charges.

Request for Collection of a Swik by the Supplier implies one-click acceptance of the General Terms. It constitutes acceptance of payment by the Supplier of the SWIKLY Collection Charges for closure of the Swik, once the Customer has accepted actual payment of the Total Amount of the Swik, including where appropriate after exercising their remedies. The date of acceptance by the Customer of payment of the Total Amount of the Swik constitutes the due date of the SWIKLY Collection Charges.

The exact amounts of the SWIKLY Service Charges and the SWIKLY Collection Charges are indicated when they are accepted by the Supplier, or where appropriate by the Customer, and depend on the Total Amount of the Swik. It is specified that these amounts may be revised annually under the conditions defined in point (f) of this article.

The SWIKLY Service Charges are:

- Billed to the Supplier at the start of the calendar month for the month preceding that in which the invoice is sent, and payable by direct debit from the Supplier's bank card or deducted from its bank account.
or
- Paid directly by the Customer by being debited partly or fully from their bank card. The part of the SWIKLY Service Charges that remains payable by the Supplier is billed at the start of the month, for the month preceding that in which the invoice is sent.

The sales agreement concluded between the Company and the Supplier is a distance sales agreement. However, if the Supplier is a professional, it acknowledges that it does not have a right of withdrawal due to its capacity as a professional. If the Supplier is a private individual or association and has not declared that it is a professional, it has the capacity of a consumer: however it acknowledges that it does not have the right of withdrawal provided for under Articles L221-18 et seq. of the French Consumer Code since it benefits immediately from the Service provided by the Company, i.e. before expiry of the withdrawal period. Consequently it declares that it waives this right of withdrawal.

The sales agreement concluded between the Company and the Customer, if the Customer must pay the SWIKLY Service Charges, is a distance sales agreement. However, the Customer acknowledges that they do not have the right of withdrawal provided for under Articles L221-18 et seq. of the French Consumer Code since they benefit

immediately from the Service provided by the Company, i.e. before expiry of the withdrawal period. Consequently they declares that they waive this right of withdrawal.

d/ Collection of the Swik

During Collection of the Swik, the aforesaid Total Amount is deducted directly from the bank card of the Customer concerned, and paid into the Supplier's electronic purse, except in cases where the end Customer has subscribed to the Shield Security Deposit Buy-Back or the Zen Security Deposit insurance products distributed by the Company. In such cases, the amounts are paid directly by the Company to the Supplier, by virtue of the insurance subscription covering the Customer, and the bank card is not debited (except in the event of an exclusion of cover). The Total Amount of the Swik is transferred to the bank account indicated by the Supplier when the Swikly account was opened, during the week or month following the payment into the Supplier's electronic purse, in accordance with the option chosen by the Supplier.

e/ Single Payment

The Company has introduced an extra function for Single Payments, which enables any Supplier to request payment of an amount by a Customer (whether or not it is related to a transaction involving a Swik). In this case, the Supplier initiates a request for distance payment via the Application, specifying the price including taxes, and the Customer receives a link by email or SMS enabling them to confirm the amount of the request for Single Payment. Use of the Application as a method of payment by the Supplier involves acceptance of the automatic payment of Payment Commission to the Company, the amount of which will be notified to the Supplier when the Supplier initiates the payment request (before confirming the request).

Consequently, when the Single Payment is made, the aforesaid amount is deducted directly from the Customer's bank card, and paid into the Supplier's electronic purse. This amount is paid by transfer onto the Supplier's bank account, during the week or month following the payment into the Supplier's electronic purse, in accordance with the option chosen by the Supplier. Transfers outside the SEPA may lead to additional costs, which may be deducted from the amounts transferred by the Company and banks. The Supplier can ask the Company for the specific rates for transfers outside the SEPA.

By way of exception to the foregoing, in the event that the Company observes a decrease in the use of the Service by the Provider, the Company reserves the right to block any transfer of the amounts corresponding to Isolated Payments credited to the Provider's electronic wallet to the Provider's bank account.

This blocking is expressly authorized by the Provider in order to cover potential bank repudiation risks which systematically result in the reimbursement by the Company to the Customer of the amount paid as an Isolated Payment.

The blocking of transfers to the Provider's bank account will be lifted once the bank repudiation risks have expired, either after the expiration of the repudiation management periods, which may extend up to a period of 11 months, or when the level of use of the Service by the Provider once again makes it possible to cover the risks of bank repudiation.

All invoices issued by the Company are issued in electronic format, which the Supplier accepts by accepting these General Terms.

f/ SYNTEC indexation

The Service Fee, the SWIKLY Collection Fee, the Payment Commission and any amount due under these General Terms and Conditions will be adjusted periodically by the Company according to the variation in the Syntec Index.

Indexation will apply to Suppliers who have been using the Services for more than six months from the date of registration of the Supplier's account and will take place annually, on the 1st day of the new year.

The following formula will be applied:

$$P1 = P0 \times S1 / S0$$

Where :

P1 = revised price

P0 = original contract price

S0 = SYNTEC reference index used

S1 = last published index at the revision date.

The reference SYNTEC index is the actual index on the date of the Supplier's initial registration on the platform for the use of the Services.

8 Right of recourse in the event of contesting an Activation Request for a Swik

It is specified firstly that, in the event of rental of property and use of a Swik Security Deposit:

By accepting the Swik, the Customer has undertaken to:

take photographs of the property rented from the Supplier, when taking possession of it and when returning it, and to keep them for the time required to investigate any Service Activation Request,
keep all written exchanges with the Supplier for the time required to investigate any Service Activation Request (emails, text messages, etc.)
submit accurate and complete information to the Company in the event of a Service Activation Request.

the property that is rented is presumed to have been provided in good condition to the Customer by the Supplier.

These two principles are essential to apply the provisions of this Article.

a/ When the Supplier makes a request for Collection of a Swik, the Customer is informed by email of the request by the Company at the time of the attempted Collection. This information is accompanied by the information required so that the Customer, if they refuse or contest the request for Collection of a Swik, can exercise their right of recourse, as specified in paragraph b/ below.

The Collection of the Swik by the Supplier via the intervention of the Company, does not on any account deprive the Customer of their rights to exercise the remedies specified in paragraph b/ below, granted to the Customer, subject to the legal time limits, in accordance with any legislation applicable to the transaction that was covered by the Swik.

If the Customer makes an objection on receipt of notice from the Company of Collection of the Swik, the Customer can send the Company any supporting documents proving its good faith, and the Company undertakes to send them to the Supplier, so that, as far as possible, the dispute can be settled amicably between the Users concerned. The Customer can also decide to exercise the remedies specified in paragraph b/ below.

On receipt of the documents the Company will give an advisory opinion on the state of the dispute, that is not binding on the Customer and the Supplier and does not on any account deprive the Customer of any right of recourse as specified below.

b/ The Customer is free to exercise any remedies at any time following the first notification by the Company to the Customer of the existence of a request for Collection of a Swik: pursuant to Article 750-1 of the French Code of Civil Procedure, the Customer can therefore settle the dispute with the Supplier using alternative methods of dispute settlement, such as mediation, conciliation or an agreement to seek an amicable settlement, or any other method of judicial or non judicial dispute settlement to which the Customer is entitled in accordance with the law. The Company shall make available to the Customer all of the supporting documents provided by the Supplier with its request for Collection of the Swik, to enable the dispute to be settled as quickly as possible.

The Customer is also requested to find out about the methods of dispute settlement from <https://www.economie.gouv.fr/dgccrf/contacter-dgccrf#0> or <https://www.vie-publique.fr/fiches/reglements-alternatifs-des-conflits> or by using the European platform for online dispute resolution at any time, pursuant to Regulation (EU) No 524/2013: webgate.ec.europa.eu

In any case, the Company shall repay the Total Amount of the Swik to the Customer in the event that the Supplier has kept a Swikly account open with the Company throughout the duration of the claim, on production of one of the following documents:

- final court order,
- conciliation or mediation decision with judicial approval,
- joint request by the Users concerned, after checking the reality of the request.

The Company has an obligation of best efforts regarding the implementation of the process described above. The Company cannot be held liable or incur liability on this account.

9 Services provided by the Company

a) General services

The Company will provide the following Services hereunder, for the duration of the General Terms:

- Amicable management, before any claims, of any disputes between the Customer and the Supplier, under the conditions specified in Article 8 above;
- Management of refusals to pay in the event of a chargeback on the Customer's initiative; if the refusal to pay is not resolved, the Supplier acknowledges that the SWIKLY Service Charges shall remain due to the Company and will be payable by deduction from the Supplier's bank account. Furthermore, the Total Amount of the Swik will be transferred to the Company by debit from the Supplier's bank card or by deduction from the Supplier's bank account. The Supplier undertakes to return to the Company the Total Amount of the Swik for which the chargeback has been confirmed by the Customer's bank. The Company does not guarantee the Supplier the Total Amount of the Swik in question in the event of failure of the objection to the chargeback.

The Service is available in certain countries, a list of which is accessible by clicking on the following link: <https://support.mangopay.com/s/article/which-are-the-authorized-countries-where-you-can-process-payments?language=fr>. This list is liable to change.

The Service is only available for certain types of bank cards defined by the Company and excludes in particular the use of certain bank cards that do not allow debits afterwards.

b) Services for Swiks for an amount exceeding one hundred (100) euros

Management of collection in the event of non-payment by the Customer: SWIKLY carries out Debt collection on behalf of the Suppliers who give them a mandate to do so. The Mandate is included in APPENDIX 2. This service is limited to a certain number of countries, for a maximum period of 6 months during which SWIKLY will attempt to recover the sums, and does not include judicial recovery (in particular the service does not include the payment order procedure); the Supplier undertakes to give the Company the invoice issued to its Customer for which recovery is required. Launch of the amicable recovery procedure is subject to transmission of the invoice to the Company by the Supplier, which shall refrain during that stage from recovering the amount from the Customer, themselves or through a third party. If the collection procedure is unsuccessful due to cancellation of the procedure by the Supplier, the Supplier shall be required to pay all of the expenses incurred by the Company, linked to the attempted collection, in accordance with the quotation sent to it previously by the Company. The Company reserves the right not to manage collection for a Supplier for which there is an increasing number of cases of non-payment. The Company will notify this to the Supplier concerned, which will retain the right to directly use the services of a specialised debt collection company.

The Company undertakes to make every effort to provide the services specified above in points a) and b). By express agreement, these obligations are solely an obligation of best efforts. The Company does not provide any guarantee concerning the result of these services.

c) Additional services as part of the premium service and service limitation

(i) *General Terms*

Subject to compliance with the eligibility conditions defined by the Company, certain Suppliers may benefit from the premium service, which includes an enhanced support and dispute and payment incident management service offered by the Company to the Supplier. Within the framework of the premium service, the Company may, on a commercial basis, pay the Supplier a compensatory amount in the event of a payment incident or unresolved chargeback of the Customer's bank card, within the limits and conditions defined in this article. This mechanism does not constitute either a payment guarantee or an insurance transaction. These are in particular professional Suppliers that have at least one manager who is a citizen of a euro zone member state, and whose registered office is located in a euro zone member state. Exceptionally, the Company may extend the premium service to Suppliers that do not meet these eligibility conditions. Suppliers that meet the eligibility conditions for the premium service have been informed by the Company of their ability to benefit from this service when subscribing to the Service. The conditions of application have been communicated to them by quotation. APPENDIX 1 specifies the applicable scope of the Service guarantee. Any loss of revenue or of profits suffered by the Supplier, and repayment of Swikly Service Charges and Collection Charges are expressly excluded from the scope of the guarantee relating to a Swik Security Deposit.

The Premium service includes:

- A compensatory payment within thirty (30) business days from the date of sending of the first email notification of an Activation Request for a Swik by the Company to the Customer concerned, within the framework of Article 8 of the present General Terms.
- A compensatory payment in the event of failure of the objection to a chargeback initiated by a Customer.

The aforementioned compensatory payment applies to amounts actually spent by the Supplier, supported by a document that the Supplier must upload via the Application when making the request for Collection. For example, any Service Activation Request due to late departure by a Customer and penalised by the Supplier by sending an additional invoice to the Customer (such as a fixed rate for late departure) is excluded from the scope of the compensatory payment. Consequently, the compensatory payment covers only the expenses actually incurred by the Supplier. If the late departure caused additional and specific costs payable by the Supplier (such as additional cleaning costs), the compensatory payment may apply on production of the supporting documents.

For any Swik Security Deposit, the validity period of the premium service is open to the benefit of the Supplier for a period of three months from the acceptance of the Swik by the Customer, unless otherwise agreed in writing in advance by the Company.

The Company reserves the right to unilaterally request pre-authorisation for the Total Amount of the Swik for each bank card of the Customers concerned, of the Supplier that has subscribed to the premium service, as soon as the Supplier has a high failure rate after too many Collection attempts. The Company can apply this decision immediately.

If a Supplier opens a new account after closing its previous account, or after it has been closed by decision of the Company, the Company reserves the right, at its discretion, to include the history of the aforementioned Supplier prior to the closure of its initial account. Furthermore, within the framework of the premium service, the Company reserves the right, retroactively and after the request for Collection has been made, to verify the consistency of the Service Activation Request and the elements used by the Supplier to justify it. In this regard, the Supplier undertakes to use service providers that charge standard market rates and to provide detailed invoices for the services carried out justifying the amount of the Service Activation Request. Failing that, the Company reserves the right to refuse to make the compensatory payment under the premium service, in particular when the amounts billed in connection with the Service Activation Request appear excessive and/or the requests are recurrent, without such refusal being construed as a refusal of compensation or the implementation of an insurance contract. The Supplier acknowledges and accepts that the premium service does not constitute an insurance activity, a credit insurance transaction, or an insurance intermediation activity. The compensatory payments made in this regard are not insurance compensation but a commercial service subject to conditions and caps defined by the Company.

For further information, you can contact the Company directly at the following address: contact@swikly.com.

(ii) *Premium service limitations: cap on the compensatory payment*

It is expressly agreed that the premium service provided by the Company is subject to a rolling cap on compensatory payments determined by the Company according to the parameters defined below. Beyond this cap, no further commercial payment shall be made under the premium service. The cap value retained shall be the highest of:

- The amount set forth in these terms or in the quotation provided by the Company to the Supplier (the “maximum cap amount”), or
- The total amount of Fees invoiced to the Supplier and its Customers multiplied by a cap limitation coefficient (value defined in the quotation or in these terms).

The maximum payable amount to which the Supplier may be entitled shall be calculated by the Company on D+15 of the Service Activation Request submitted by the Supplier (D being the day on which the Service Activation Request is made by the Supplier). The total amount of payments that may be made to the benefit of the Supplier under the premium service over a rolling twelve (12)-month period may not exceed the overall cap defined above. Therefore, for each new payment request under the premium service, the Company shall calculate the maximum amount still available as follows: Maximum payable amount over 12 months calculated on D+15 minus the amount already paid under the premium service during the last twelve months. The amount potentially paid to the Supplier under the new request may not exceed this available amount.

(Maximum reimbursable amount as determined on D+15) – (Amount already paid under the Premium Service over the past 12 months).

The Supplier shall only be entitled to the remaining amount, even if such remaining amount does not fully cover the total amount of the ongoing Service Activation Request.

Furthermore, once the cumulative amount paid by the Company to the Supplier under the premium service during the previous 12 months reaches or exceeds the maximum payable amount calculated on D+15, no further payment shall be due, even in the event of additional Service Activation Requests. The amounts taken into account correspond to funds that could not be recovered from the Customer's card, within the coverage limits defined by the premium service as set out in APPENDIX 1.

The maximum payable amount constitutes an overall limiting cap applicable to the premium service and applies regardless of the number of Service Activation Requests submitted by the Supplier over the last 12 months.

Under the premium service, the Company shall automatically apply a cap limitation coefficient of three and a maximum cap amount of 5,000 euros, unless otherwise stated in the quotation accepted by the Supplier.

10 Obligations and liability of the Company

The Company cannot be held liable for any unavailability of the Application, the Service or the electronic purse made available by MangoPay due to technical hazards linked to the internet, a force majeure event, the internet connection of a User or their equipment, or the maintenance operations required for the smooth functioning of the Application, the Service, or the service offered by MangoPay. The Company is bound by a best-efforts obligation with respect to the technical functioning of the Application. It is not liable for any refusals, delays or errors in the execution of payment transactions attributable to MangoPay and card networks, nor for any blockages or suspensions decided for reasons of security, anti-fraud or compliance by those same entities. The Company reserves the right to interrupt access to the Application or Service at any time, in particular in order to protect the confidentiality or integrity of Suppliers' accounts and the data stored, in the event of a virus attack.

The Company shall implement the technical means at its disposal to maintain as far as possible the integrity and security of the Service and Application and the confidentiality of Users' personal data. Where appropriate, it may be required to guarantee an availability rate or SLAs; in this case, this is indicated in the agreement concluded with the Supplier. However, there is no guarantee that the Service is free from errors, bugs, flaws or defects.

Regarding the Swik Deposit, the Company cannot guarantee that it will function as specified in Articles L 214-1 and L 214-2 of the French Consumer Code, since the Supplier can include any statement to the contrary in its general terms applicable to the transaction concerned. It is therefore the Customer's responsibility to read carefully the general terms of the Supplier applicable to the transaction concerned and reject them if necessary. Regarding the Swik Security Deposit, the Company guarantees the existence of an authorisation by the Customer's bank for the Total Amount of the Swik at the time of acceptance of the Swik by the Customer; in the event of a refusal to pay, the Company can decide to repay the Total Amount of the Swik to the Supplier. In this case, a transaction of this kind cannot on any account constitute an assignment of receivables to the Company.

The Company cannot be held liable for any damage resulting from an intrusion or fraudulent maintenance by a third party affecting a User's SWIKLY account or illicit data extraction, in spite of implementation by the Company of security measures in accordance with current technical standards.

Since the Company merely has the role of a service provider who enables Users to secure the payment of a virtual Deposit or Security Deposit or to guarantee the payment of property or a service, it cannot on any account be declared to be an intermediary in the transaction between the Users to sell or rent property or a service, or as a payment service provider or electronic money institution. Only MangoPay has the role of electronic money issuer and manager as defined in the regulations. In this regard, access to all or part of the Service is dependent on the services provided by MangoPay and card networks, which may restrict or suspend certain transactions. MangoPay and card networks implement fraud detection systems that may also lead to the suspension or verification of certain transactions, in particular in the event of an apparent anomaly. Such suspension shall not give rise to any liability of the Company, nor to any compensation in favour of the Users. In parallel with these suspensions, MangoPay and card networks may apply certain charges to the Company, which may pass them on to Users where such charges result from their conduct. Users are also informed that card networks require the Company to constitute financial reserves which, if insufficient, may lead to the temporary deactivation of all or part of the Service. Such temporary deactivations of the Service due to financial reserve requirements shall not give rise to any liability of the Company.

In particular, the Company disclaims all liability regarding (i) the legality, security, compliance, nature, content and characteristics of the goods or services sold or rented by Users and, more generally, regarding the manner in which the Application is used by Users, (ii) the terms and conditions of sale or rental applied by Providers to Customers, and (iii) any data, information, image or other content published by a Provider through the Application that infringes the rights of third parties or violates in any way the applicable laws and regulations.

In particular, the Company does not carry out any moderation, selection, verification or control of the content published on the Application and acts solely as a hosting service provider in this respect.

In the event of a complaint by a third party or User concerning any content published by another User, the Company must be notified in accordance with Law No. 2004-575 of 21 June 2004 regarding confidence in the digital economy.

The Company cannot be held liable for any damage to a third party or User resulting from the breach or non-compliance by another User with one of its obligations under the General Terms. Consequently, in the event of action or a claim by a third party against the Company, the Company may institute third party proceedings against any User who, by failing to respect the commitments of the present General Terms, causes the complaint by the aforementioned third party to the Company.

The Company is responsible to Users for the proper functioning of the Service, and solely for the breaches attributable to it, unless it demonstrates that the non-performance or improper performance of the Service is attributable to one of the Users, or to an unforeseeable and insurmountable act by a third party, or to a force majeure event.

However, the Company's liability towards Suppliers who have the capacity of professionals is as follows:

- Limited to the direct damage suffered by the Supplier, within the limit of thirty (30) % of the total amount exclusive of tax of the monthly Service invoice issued by the Company in the name of the Supplier for the month concerned by the event that led to the Company being held liable;
- Excluded for any indirect damage suffered by the Supplier, such as in particular, without this list being exhaustive, loss of profit, loss of revenue, data breach, damage to reputation and/or brand image etc.

Any contract with a Supplier that has the capacity of a professional that specifies exclusions or limitations other than those indicated above shall take precedence over those indicated above.

The Company shall retain for a period of ten (10) years the data relating to all transactions carried out through the Service, the aforementioned data constituting prima facie evidence in writing in the event of a dispute between the Company and a User, or between two Users, which all Users acknowledge and accept. Consequently, in connection with such a dispute, even if the matter is referred to the Company via the Amicable Settlement Procedure, the Company may make this data available to any person in order to settle the dispute.

11 Obligations and liability of the User

All Suppliers, whether or not they are professionals, undertake to:

comply with the provisions of Articles L111-1 et seq. of the French Consumer Code, as well as Articles L121-4 et seq. of the aforementioned code concerning misleading commercial practices and the obligations linked to distance sales;

if necessary, make available to Customers its own general terms of sale or service prior to any sale or lease, so that the Customers act with full knowledge of the facts;

if necessary, specify in their general terms of sale the consequences of cancellation for payment of the deposit, these stipulations being applied in full to the Swik Deposit in the event of cancellation;

if necessary, specify in their general terms of sale, the consequences of non-payment;

if necessary, specify in their general terms of sale, the consequences of early termination of a fixed-term subscription;

comply, in the course of its use of the Service, with all applicable rules of payment card schemes (including in particular Visa Core Rules, Mastercard Rules, and Cartes Bancaires CB) as well as any rule imposed by MangoPay pursuant to its own obligations towards those schemes. Certain limitations, suspensions or payment malfunctions may result from decisions by MangoPay and/or card schemes and cannot be attributed to the Company. The Supplier acknowledges that the Company may suspend or terminate its account in the event of proven non-compliance with these rules, in particular at the request of MangoPay or a card scheme, without any right to compensation for the Supplier; comply with the security rules applicable to access to the Service (confidentiality of credentials, compliance with strong authentication rules, non-disclosure of codes to third parties) and promptly notify the Company of any suspected fraudulent or unauthorised transaction; comply with the latest technology as regards computer security and interoperability between their computer system and the Service, in particular by implementing sufficient technical means to ensure that the Service is operational for the Swik requests of its Customers;

in general, comply with all of the legal provisions applicable to their activity and guarantee the Company against any claims in this regard.

Any contract concluded with a Supplier that has the capacity of a professional that mentions other specific commitments by the Supplier shall complete the preceding provisions, or where appropriate shall take precedence over them.

Once the Supplier has provided all of the information concerning a transaction to a Customer and a Swik has been requested, the conditions of the transaction (price or maximum amount, duration, dates, characteristics of the property or service etc.) can no longer be modified by the Supplier. The Supplier acknowledges that if there is any change in the characteristics of the transaction, the Customer is entitled to cancel the Swik and is not required to make any payment whatsoever, in accordance with the law.

The Supplier alone is liable towards the Customer for the availability of property or a service proposed via the Service and the terms and conditions of the transaction proposed via the Service and its legality; the Company is in no way party to the transaction and its intervention is limited to providing the Service making it possible to submit dematerialised Deposits or Security Deposits or to guarantee the full payment of the Supplier's Invoice following the purchase of property or a service by the Customer.

The User remains liable for the proper performance of all formalities, in particular the administrative, fiscal and/or social security formalities, and for all payments, contributions, taxes and duties of any kind whatsoever that he is required to make in connection with the sale or lease of property or services via the Application. The Company cannot on any account be held liable for this reason.

When using the Service, the User undertakes to moderate its language and not disclose or publish content (words, images, videos, links etc.):

of an advertising or promotional nature, for regulated or illicit products or services,
contrary to public order or good conduct and/or that do not comply with the laws and regulations in force,
of a slanderous, offensive, extreme, untruthful, discriminatory or libellous nature with regard to a User, third party or the Company,
of a racist, xenophobic or revisionist nature, encouraging discrimination, hatred or violence towards a person or group of people due to their origin, sex, family situation, physical appearance, patronymic, handicap, genetic characteristics, morals, actual or presumed sexual orientation, age, political opinions, union activities, actual or presumed membership of a specific ethnic group, nation, race or religion,
containing viruses or any computer program likely to disrupt, interrupt or wholly or partly destroy the Application and/or the Service.

Similarly, the User cannot publish content that infringes the intellectual property rights of a third party, invades privacy or damages the image of a person or the reputation of a company.

In particular, the User declares that they will only disclose or publish content of which they are the owner and hold the related intellectual property rights, or failing that for which they have first obtained the intellectual property rights from the author or initial holder. The User declares that they have obtained any authorisations or transfers required to use images, trademarks and videos in the content published, and has paid any amounts due (and will pay any amounts due in future) to any person on this account, including to any person whose image is reproduced in that content. In this connection, the User will provide any written evidence of this on request by the Company.

The User declares that they will not publish or disclose any content that is confidential or of which publication would constitute a breach of a contractual commitment towards a third party.

The User guarantees the Company full and quiet enjoyment of the content, due both to third parties and to the User, and shall cover all costs of action by a third party against the Company due to use of the content.

All Users waive all claims against the Company in connection with proceedings instigated by a third party against it due to the publication or use of the content they have published using the functions of the Application.

When creating a hypertext link, the User must ensure that all of the above obligations are respected.

In view of the above, the User waives all recourse against the Company:

based on an infringement of their intellectual property rights, provided the present General Terms are respected by the Company,
in the event of a dispute with another User.

All Users guarantee the Company that they have the required authorisations to use the bank account attached to their SWIKLY account due to their registration. Consequently they undertake to take all necessary measures to ensure that their bank account has the funds required for the transactions that they intend to carry out via the Application.

It is the User's responsibility to make sure that their equipment and internet connection are sufficient to access the Application and/or the Service. All Users remain liable at all times for use of their SWIKLY account, username and password.

All Users acknowledge that any action likely to interrupt the Service, limit its availability or prevent its continuity, is prohibited. The Company is entitled to take action against the User for any intrusion or attempted intrusion into the Application, hijacking of data, infringement of the security and authentication measures of the Service, and more generally any breach of the present General Terms.

Any User who discovers abuse or a breach of the commitments made by each User under the present General Terms undertakes to immediately notify the Company by email at the following address: contact@swikly.com

12 Intellectual property

The Company has full ownership of the Service, the functions it provides, the Application and all of the elements they comprise, including the related intellectual property rights.

The Company grants all Users a free, limited, personal, non-transferable and non-exclusive licence to download, install and use a copy of the Application on any mobile device or computer. Any other use is expressly excluded.

13 Objection to a transaction by a User

If a User denies having authorised the Swik Payment via the Service, they must comply with Article L133-23 et seq. of the French Monetary and Financial Code. They can refer the matter to the Company's customer service department at the following address, which must reply within fifteen (15) working days: SWIKLY, MAMA WORKS, 92 Cours Lafayette, 69003 Lyon, FRANCE – contact@swikly.com

The Company can pass on to MangoPay all of the proof of acceptance of the transaction by the User, which the User accepts.

The User has thirteen months following the date of the debit to take action regarding any unauthorised Swik Payment. Regarding objections by a User to a Swik Payment for which the exact amount was not specified or for an amount that was not expected by the User, the objection must be transmitted by the User within eight weeks of Payment of the Swik.

In the event of loss or theft of user names and passwords allowing use of SWIKLY accounts, any unauthorised transaction carried out before notification of the opposition will be payable by the User concerned, up to a limit of €150. The Company cannot be held liable in the event of misconduct by the User, serious negligence or deliberate breach, bad faith or late notification of its objection.

If the transaction was not authorised by the User and the objection is recognised as legitimate, the amount concerned will be repaid within ten working days of receipt of the objection.

14 Personal data

a/ Processing for which the Supplier and the Company are the Data Controllers

The Company and the Supplier shall comply in all circumstances with the regulations applicable to them on the protection of Personal Data and in particular the provisions of the French Data Protection Act No. 78-17 of 6 January 1978 as amended and the GDPR.

The Company and the Supplier undertake, as Data Controllers for the Personal Data Processing operations that they respectively carry out for their own needs in connection with these General Terms, to comply with all of their obligations arising from the GDPR.

In particular, they undertake to give relevant information on the protection of their Personal Data to the Data Subjects whose Personal Data are likely to be processed.

For processing related to the distribution of insurance products, Swikly acts as joint controller with the insurer. The Company makes available to Customers the main terms of the joint controllership agreement entered into between the Company and the insurer, in accordance with Article 26 of the GDPR, in point d) of this article.

b/ Processing for which the Company is the Processor of the Supplier

The Supplier and the Company agree that any Processing of Personal Data carried out by the Company as Processor in connection with the use of the Services and the Application by Users, shall be governed by the terms and conditions of the Data Protection Agreement attached to the General Terms in APPENDIX 3.

Such processing includes any Processing of Personal Data collected when the Supplier account is created and in connection with use of the Services by any User, the purpose of which is to supply the Application and the Services.

In these cases, the Data Controller is the Supplier and Swikly acts as Processor and follows the instructions of the Data Controller, as set out in APPENDIX 3.

c/ Informing of Users

The protection of your personal data is important for Swikly. Swikly undertakes to comply with the laws and regulations applicable to Personal Data protection, in particular the General Data Protection Regulation No 2016/679.

In connection with the provision of the Application and the Services, Swikly acts as a Personal Data Processor within the meaning of the GDPR when it processes Users' Personal Data on behalf of and on the instructions of the Supplier (who is the Data Controller).

Swikly is the Data Controller for the Processing that it carries out on its website.

The purpose of this section is to give the Users information on the Processing carried out by Swikly in connection with the provision of the Application on the instructions of the Supplier.

Users declare that they have read it and accept all its terms.

i) Personal Data collected by Swikly

As Processor, Swikly is required to collect the Customer's Personal Data when the Customer accepts the Swik request made by the Supplier. This involves the following Personal Data: Surname, first name, telephone number, email address, date of birth, postal address, bank card number.

When the Service is used by a Provider that is a healthcare facility, data that may reveal information about the Client's health status may be transmitted to us (e.g., the specific name of the healthcare facility, the name and/or specialty of the healthcare professional consulted).

Swikly uses hosting certified for Health Data Hosting (Hébergeur de Données de Santé – HDS).

Swikly is also required to collect the Supplier's Personal Data when:

- The Supplier registers on the Application and opens a SWIKLY account;
- The Supplier sends a Swik request to the Customer.

This involves the following Personal Data: user name and password, surname, first name, email address, telephone number, home address and date of birth of the company's legal representative, country of residence, nationality, means of payment (bank account or bank card), business sector, identity papers and proof of address where appropriate.

Processing of the Supplier's and the Customer's Personal Data is based on the performance of a contract (i.e. the performance of SWIKLY's General Terms), compliance with Swikly's legal obligations and on Swikly's legitimate interest.

The Personal Data must be provided in order to accept the General Terms. Users must provide the aforementioned Personal Data. If they are not provided, Users will not have access to the Service.

These Data will be retained by Swikly for the purposes of the Service.

All Personal Data collected by Swikly are processed lawfully, fairly and in a transparent manner with regard to the Users. The Personal Data are adequate, relevant and limited to what is necessary with regard to the Purposes of Processing defined below.

ii) Why and how are the Data processed?

We process the Data for different purposes, which are explained below.

Processing 1: Provision of the Service and the Application

Purposes of the Processing: To manage the Application, create the SWIKLY accounts of Suppliers, make the Service provided by SWIKLY available to Users, display the table for monitoring Swiks for Suppliers, manage the Customers and Suppliers.

Legal basis of the Processing: the Processing is necessary in order to implement the General Terms and provide the Service (Article 6 (1) b of the GDPR).

Data retention period: Duration of active use of its SWIKLY account by the Supplier, plus 2 years.

For the purposes of improving the Application, the Company acts as the data controller and relies on its legitimate interest. It uses **Tally** (form submission) and **Google Tag Manager** (tag tracking) to collect information enabling it to improve the Application.

Processing 2: Checking the identity of the Suppliers

Purposes of the Processing: Check that the declared identity is the Supplier's real identity.

Legal basis of the Processing: compliance with legal obligations (Article 6 (1) c) of the GDPR)

Data retention period: The identity papers are retained for the time required to check the identity of the Data Subject. A copy of proof of identity may be retained for 6 years if it is required for evidential purposes or to meet a legal obligation.

Processing 3: Combating fraudulent behaviour

Purposes of the Processing: Combating fraudulent use of bank cards, combating behaviour causing damage to the rental property, combating multiple no-shows, combating cases of outstanding payments, drawing up an exclusion list of Customers with fraudulent behaviour.

Legal basis of the Processing: compliance with a legal obligation and legitimate interest of the Company (Article 6 (1) b and f) of the GDPR)

Data retention period: Period required to fulfil these purposes, and at most 5 years.

Processing 4: Claims management

Purposes of the Processing: Management of complaints by the holder of the payment card used

Legal basis of the Processing: performance of the General Terms (Article 6 (1) b) of the GDPR)

Data retention period: 13 months following the debit date or 15 months following the debit date in the event of deferred debit (Article L.133-24 of the French Monetary and Financial Code).

Processing 5: Performance of the Mandate as defined in APPENDIX 2 of the General Terms

Purposes of the Processing: Collection of Suppliers' unquestionable, liquid and due claims against Customers who have accepted a Swik

Legal basis of the Processing: performance of the General Terms (Article 6 (1) b) of the GDPR)

Data retention period: Duration of the Mandate plus five years from the end of the Mandate.

iii) Recipients and transfers of Personal Data

Personal Data are solely shared for purposes linked to the supply of the Service, in-house with the Company's employees.

The Users is informed that the transmission of their Personal Data collected by the Company in the framework hereof to the service providers and subcontractors with whom it has contractual relations for the sole purpose of providing the Service, provided that the third party recipients of the Personal Data are subject to rules that guarantee an appropriate and suitable level of protection as defined by the GDPR.

A list of the Company's subcontractors can be accessed by clicking on this link:

<https://support.swikly.com/fr/support/solutions/articles/101000452068-rgpd-liste-des-sous-traitants-de-swikly>

Some transfers outside the European Union may take place due to the third-party tools used to provide you with the Service. The location is indicated in the list of subcontractors. In this case, the Company undertakes to comply with the regulations in force and to put in place any measures required to ensure the security and confidentiality of the Personal Data transferred in this way.

iv) The rights of Users

In accordance with Articles 15 to 22 of the GDPR concerning your Personal Data held by us, you have the following rights:

- right of access (Article 15 of the GDPR)
- right of rectification (Article 16 of the GDPR)
- right of erasure (Article 17 of the GDPR)
- right to restriction of processing (Article 18 of the GDPR)
- right to notification of rectification, erasure or restriction of processing (Article 19 of the GDPR)
- right to portability of the Personal Data (Article 20 of the GDPR)
- right to object (Article 21 of the GDPR)
- right not to be subject to profiling (Article 22 of the GDPR)

Swikly does not make any automated decisions.

You may exercise your rights by submitting a simple request to the Company's Data Protection Officer at the following address:

SWIKLY
Data Protection Officer
MAMA WORKS 92 Cours Lafayette, 69003 Lyon
France
or by email: rgpd@swikly.com

You can also lodge a complaint with the Commission Nationale de l'Informatique et des Libertés (CNIL) if you think that we have not respected your rights.

d/ JOINT DATA CONTROLLER AGREEMENT SWIKLY / SEYNA

Key points of the joint data controller agreement

In the context of your subscription to the insurance service distributed by Swikly, SEYNA and Swikly have entered into a joint controller agreement, the key points of which are made available to you in accordance with the GDPR.

1. Identity of the data controllers

The processing operations carried out require the joint involvement of Swikly (RCS Lyon n°819 514 076) and SEYNA (RCS Nanterre n°843 974 635) and involve cooperation in the processing of personal data, a sharing of purposes and means within a common set of operations.

2. Purposes and means of processing

- 1) While each party pursues its own individual purposes, both parties participate in achieving a common general purpose, which is to provide you with the insurance service.
- 2) Indeed, while SEYNA provides the insurance product in its capacity as insurer, Swikly distributes it through its Swikly platform.
- 3) The parties have jointly defined the main purposes of the processing, which are as follows: the management and execution of the cover, including claims management, pre-litigation, litigation and the defence of their rights, as well as the implementation of due diligence obligations in the context of the fight against money laundering and the financing of terrorism, asset freezing measures, the fight against the financing of terrorism and financial sanctions, including the triggering of alerts and suspicious activity reports, and the implementation of measures aimed at combating insurance fraud.
- 4) The action of each party is necessary to achieve these purposes.
- 5) The intertwining of the objectives pursued demonstrates that the processing operations carried out in the context of the implementation and execution of the insurance product serve the common interest of the parties.
- 6) The parties jointly participate in defining the means of processing operations by agreeing on the means used to ensure the implementation and execution of the insurance product.

3. Data

- 1) The data concerned by the processing operations have been jointly determined by the parties in accordance with the "data minimisation principle" specific to the GDPR, and fall within their joint responsibility.
- 2) The provision of data marked with an asterisk is mandatory as it is necessary to obtain the cover and to manage the subscription. This includes: your last name, first name, email address, telephone number, contract reference, IBAN, a description of your claim and the damages noted, and the subject of your request.
- 3) Swikly and SEYNA each ensure the hosting of data in accordance with the GDPR and commit to ensuring that the processed data is hosted and accessible only within a Member State of the European Union or within a country with an adequate level of protection or with which contractual guarantees compliant with the GDPR have been signed when hosting is carried out by a subcontractor.
- 4) Any false or irregular declaration may be subject to specific processing aimed at preventing or identifying fraud and may result in registration on a list of persons presenting a fraud risk.
- 5) Your telephone conversations with Swikly or Seyna may be recorded for quality control purposes or in the context of claims management.

4. Legal basis for processing

The parties implement the processing operations subject to their joint controller agreement to perform the subscription to the insurance product on the basis of contractual performance.

5. Obligations of the data controllers

- 1) **Informing data subjects about processing operations.** It is agreed that both parties will provide data subjects with the information referred to in Articles 13 and 14 of the General Data Protection Regulation, without prejudice to the respective obligations of the parties for the processing they carry out independently as data controllers.
- 2) **Your rights regarding your data.** You may exercise your rights of access, objection, rectification, restriction, portability and erasure, as well as the right to issue post-mortem instructions, at the following email addresses: rac@swikly.com or dpo@seyna.eu. You may address your complaints to the above-mentioned email addresses. In the event of a persistent disagreement, you have the right to contact the CNIL at the following address: <https://www.cnil.fr/fr/plaintes>.
- 3) **Bloctel.** You may register on the telephone marketing opt-out list by visiting the website www.bloctel.gouv.
- 4) **Security.** Swikly and SEYNA implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in the context of processing operations carried out under joint responsibility.
- 5) **Recipients.** Each party is responsible for defining the persons who have access to the data processed within the scope of the parties' joint responsibility. The parties only grant access to data to persons whose access is necessary for the performance of their duties and, where applicable, to supervisory authorities.
- 6) **Cross-border transfers.** No cross-border transfers are carried out by the joint controllers.
- 7) **Data retention period.** The data processed under this agreement are retained for the duration of the subscription to the insurance product, plus applicable statutory limitation periods and mandatory retention periods.
- 8) **Information of data subjects in the event of a data breach.** In the event of a personal data breach likely to result in a high risk to the rights and freedoms of one or more natural persons, the parties undertake to inform the data subjects concerned without undue delay.
- 9) **Liability.** The parties to the joint controller agreement are jointly and severally liable to you for the operations carried out under joint responsibility.

6. Contact point

If you have any questions or would like further information, you may contact SEYNA's Data Protection Officer at the following postal address: 20 bis rue Louis Philippe, 92200 Neuilly sur Seine or by email at dpo@seyna.eu or to the personal data officer of Swikly at the following postal address: 92 cours Lafayette, 69003 Lyon, or by email at dpo@swikly.com, specifying your contact details.

15 Management of cookies

The Company informs you that it installs cookies.

The Company uses cookies to enable and facilitate electronic communication, and to provide functions suited to Users' requirements. Cookies identify Users each time they connect, thereby facilitating their access to the Service. Users can refuse cookies when they access the Application or by changing the configuration of their browser. However, this may change the functions of the Application, which the User accepts.

16 Language

If the present General Terms are translated into one or more languages, the French version hereof shall prevail between the Parties in the event of a contradiction or dispute regarding the meaning of a term.

17 Conditions applicable to offers and Trial Periods

Users who wish to benefit from a trial offer must open a SWIKLY account for the first time, in accordance with Article 3, during the subscription period of the offer. Once they have subscribed, Users have full access to the Service for the period specified in the offer, from the time they open the SWIKLY account (hereinafter the “Trial Period”), and within the limit of the number of Swik requests specified in the offer.

During the Trial Period the Service is only free of charge for the SWIKLY Service Charges linked to the Swik requests included in the offer. The SWIKLY Collection Charges remain due to the Company under the conditions specified in these General Terms which apply in full.

18 Applicable law and jurisdiction

The present General Terms are governed by French law. In the event of a dispute regarding the validity, interpretation and/or performance hereof, the Parties agree that the courts of Lyon shall have jurisdiction to settle any dispute.

19 Distinctive features of use of the Service via an API

If, as a Supplier, you have developed your own booking, leasing or purchasing website, application or platform (hereinafter the “Third Party Platform”) and wish to use the Service via a Swikly API, you agree to be bound by the following terms:

- you have declared your Third Party Platform to the Company beforehand via an email sent to the following address: contact@swikly.com;
- the aforementioned declaration implies in all cases the creation of a SWIKLY account in accordance with the present General Terms, which we will connect technically to your Third Party Platform, as well as express acceptance of the General Terms;
- your Third Party Platform must not allow any storage, export, or use of data belonging to Users of the Service other than those of which the use is authorised herein, and other than for the use authorised herein;
- your Third Party Platform must not have the same purpose as the Service;
- you acknowledge that you alone are responsible for the smooth functioning and use of the Swikly API;
- you cannot give the Swikly API access codes that we will give you to anyone else; these codes constitute confidential information under these General Terms;
- you recognise the rights of ownership, including the intellectual property rights, of the Company to the Swikly API;
- you have a non-exclusive, limited and non-transferable licence to use the Swikly API in order to develop, test and maintain your Third Party Platform and enable your customers to use the Service via your Third Party Platform due to the inclusion of the Swikly API;
- you must use the Swikly API under the same conditions as the Service and the Application, and in particular in accordance with Article 11;
- you must immediately delete any User data at our request;
- in addition you have a licence to use the SWIKLY Trademark for the sole purpose, where appropriate, of identifying the Service on your Third Party Platform;
- you must take all necessary measures to ensure the technical security of the data transmitted on your Third Party Platform and the Application;
- you acknowledge that the rights resulting from this Article can be terminated at any time in the event of non-compliance with the General Terms, by decision of the Company.

20 Distinctive features of the Service due to the Supplier belonging to a network/partnership

The Service can be used by a group of Suppliers belonging to the same network/partnership. In this case, the head of the Supplier's network can make the Swikly Service available to all of the Suppliers attached to its network/partnership.

Within this framework, the Supplier that is the head of the network, can:

Pay some or all of the Swikly Service Charges, Swikly Collection Charges and Payment Commission generated by all of the Swiks and Single Payments initiated by its Suppliers via the Swikly Service;
Receive in its electronic purse a percentage, the rate of which is determined in the special financial terms (quotations) signed by the Company and the head of the Supplier's network and calculated for all of the amounts subject to Single Payments and Collections of a Swik generated by the Suppliers belonging to the network/partnership.

Within this framework, the Supplier that is the head of the network is responsible for obtaining the authorisations required from its Suppliers concerning in particular the deduction of the aforementioned percentage from their electronic purse opened by the Company to provide the Service. It shall indemnify and hold harmless the Company from and against any actions and claims by a Supplier in its network that contests the deduction of the aforementioned percentage from its electronic purse.

By accepting these General Terms, the Supplier belonging to the network/partnership accepts, where necessary, the principle of deduction of this percentage from its electronic purse, for the benefit of the head of the network. It waives its right to take any action against the Company on this account.

21 Security Deposit Insurance Service

The Security Deposit Insurance Service does not concern all Suppliers. It is activated by the Company, at its sole discretion. The Shield Security Deposit Buy-Back Service operates in a manner similar to that described for the Zen Security Deposit in Article 5.a) of these General Terms. The same conditions of application and the same limitations of liability as those described in Article 5.a) apply, except that the Shield Security Deposit Buy-Back Service is offered to the Customer after they have accepted the Swik.

22 Reversibility

At the end of the use of the Service by the Provider, the Company undertakes to ensure the reversibility and portability of the Provider's data under the conditions defined in this article. This obligation is part of the interoperability and portability requirements for exportable data provided for in Article 28, II, 2° of Law No. 2024-449 of May 21, 2024 and by Regulation (EU) 2023/2854 of December 13, 2023 on data ("Data Act").

Reversibility covers all exportable data belonging to the Provider and hosted within the Application. Exportable data refers to input and output data generated through the use of the Application, excluding metadata and derived data belonging to the Company that are protected by intellectual property rights or trade secrets.

The data will be returned in a structured, commonly used, machine-readable format (CSV) and, where applicable, in compliance with open standards ensuring interoperability. The data will be made available from the Provider's account, from which it may be downloaded at any time.

The Company undertakes to cooperate in good faith with the Provider or its new service provider to facilitate the migration where applicable, without unreasonable interruption of service and within a reasonable timeframe allowing the Provider to ensure continuity of service.



No fees will be charged by the Company, except in the case of complex and specific requests. In such cases, the fees may not exceed the actual and direct costs incurred by the Company and directly related to these operations. In accordance with the Data Act, no fees will be charged from January 12, 2027.

Following written confirmation from the Provider of the proper receipt of all data, and no later than 60 days after the end of the use of the Service, the Company will proceed with the secure and irreversible destruction of all Provider data present on its systems, including backups, and will provide a certificate of destruction upon request.

APPENDIX 1. COMPENSATORY PAYMENT - TABLE OF SERVICE ACTIVATION REQUESTS

Applicable for the housing sector for Swik Security Deposits (e)

Type of collection	Grounds for collection	Type of damage accepted by Swikly	Included in the premium service
Damage (a)	Piece of furniture damaged or broken, bathroom door removed, key broken in the lock, stainless steel scratched (credence, fridge, bar, worktop etc.) leg of a piece of furniture damaged, roller shutter damaged, garden furniture damaged, candle wax stain etc.	Yes	Yes
	Curtain rod damaged, curtain damaged, sofa/armchair material stained or damaged etc.	Yes	
	Materials, carpet, rug, duvet and sheets stained or damaged etc.	Yes	
	Hi-fi equipment, speaker, TV, decoration, light broken or damaged etc.	Yes	
	Holes in the walls, stained walls, scratches on the parquet, broken handle, robotic pool cleaner or swimming pool roller shutter broken etc.	Yes	
	Hob, food processor, ice maker broken or damaged, burned worktop, burns and splinters of wood in the chimney, BBQ burns on wooden terrace etc.	Yes	
Cleaning	Extended cleaning	Yes	Yes
	Waste bin not emptied	Yes	
Damage to plumbing due to improper use	Blocked sink	Yes (a)	No(f)
	Blocked shower	Yes (a)	
	Blocked toilets	Yes (a)	
	Leak	Yes (a)	
	Macerator unit-type toilets blocked	Yes (a)	Yes
Non-compliance with rules of use/contract or Supplier's General Terms of Sale	Noise pollution	No	No
	Smoking	Yes	Yes(d)
	Extra days without notice (squatting)	Yes	No
	Customer behaviour	No	No
	Outstanding payments (VOD, left without paying, overconsumption)	Yes	No
	Party without damage resulting in a complaint or a fine	Yes (b)	No
	Lodging of additional people	Yes (b)	No
	Misuse of the apartment (e.g. unauthorized filming)	Yes (b)	No
Theft/Failure to return equipment	Intrusion into the room whereas the reservation has been cancelled	Yes	No
	Key lost	Yes	Yes
	Key left in the apartment	Yes	
Check-in/Check-out	Theft of objects, equipment (CDs, DVDs, books, comic books stolen etc.)	Yes	
	Late	Yes (b) (c)	Yes(c)
Chargeback for a Swik	n/a	Yes	Yes

(a) Damage due to obsolescence, i.e. normal wear and tear over time, are excluded

(b) If specified in the Supplier's rental Terms & Conditions

(c) Late departure by the Customer with billing by the Supplier of a flat rate is excluded

(d) Only on production of an invoice for cleaning or a deodourizing service

The cumulative compensatory payments may not exceed the sum of the deductible amounts defined in the insurance contracts offered by a third party and applicable to the collection request. The amount of the

deductibles must be justified by supporting documentation from the insurance company. (e) Damage to common areas is excluded from the premium service.

(f) Only upon presentation of an invoice from a plumber specifying the improper use of the sanitary equipment.

Applicable to all sectors for Swik Deposits

Type of collection	Grounds for collection	Type of damage accepted by Swikly	Covered by the Premium Service
No-show	Absence on any grounds	Yes	Yes
Last minute cancellation	according to the time limit provided for in the Supplier's General Terms of Sale	Yes	Yes
Chargeback for a Swik	n/a	Yes	Yes

Applicable for the vehicle rental sector for Swik Security Deposits

Type of collection	Grounds for collection	Type of damage accepted by Swikly	Covered by the Premium Service
Damage	Scratches on bodywork, rear-view mirror broken off, headlamp insert broken, window deliberately smashed, graffiti on the vehicle etc.	Yes	Yes (c)(d)
Use of the rented property and outstanding payments	Ticket/fine not paid	Yes	Yes(d)
	Mileage or rental period exceeded	Yes	No
	Fuel refilling or energy recharging not or only partly carried out	Yes	Yes(d)
	Cleaning of the property not or badly carried out	Yes	Yes(d)
Theft/Failure to return equipment	Key lost	Yes	Yes(d)
	Missing object/part required for smooth functioning	Yes	
	Theft of an object or of the vehicle	Yes	
Chargeback for a Swik	n/a	Yes	Yes

(c) Damage to wearing parts and damage attributable to obsolescence are excluded

(d) The cumulative repayment cannot exceed the sum of the excess amounts specified in the insurance policies proposed by a third party and applicable to the request for Collection. The excess amounts must be proved by a supporting document from the insurance company.

Applicable to the vehicle rental sector for Security Deposit Swiks

Claim	Reason for the Claim	Type of damage accepted by Swikly	Included in the Premium Service
Damage	Scratches on the bodywork, wing mirror torn off, broken headlight, deliberately broken window, graffiti on the vehicle, etc.	Yes	Yes ^{(c)(d)}
Use of the rental and non-payment	Unpaid traffic fine	Yes	Yes ^(d)
	Mileage or rental duration overrun	Yes	No
	Fuel or energy top-up not done or only partially done	Yes	Yes ^(d)
	Cleaning of the property not done or poorly done	Yes	Yes ^(d)
Theft/Non-return of equipment	Lost key	Yes	Yes ^(d)
	Missing item/part necessary for proper functioning	Yes	
	Theft of an item or the vehicle	Yes	
Bank chargeback of a Swik	n/a	Yes	Yes

(c) Damage to wear parts and damage attributable to wear and tear is excluded

(d) Cumulative payments may not exceed the total amount of the deductibles defined in the insurance contracts offered by a third party and applicable to the Claim. The amount of the deductibles must be substantiated by supporting documentation issued by the insurance company.

APPENDIX 2. GENERAL COLLECTION MANDATE

1 Purpose

In connection with its activities, the Company is required to collect Suppliers' unquestionable, liquid and due claims against Customers who have accepted a Swik on the Application. The Swik has been subject to a request for Collection by the Supplier which was unsuccessful for various reasons (hereinafter the "**Debts**"). The Company carries out its debt collection activity in compliance with the laws and regulations, within the framework set by this debt collection mandate which the Supplier grants to the Company (hereinafter the "**Mandate**") and in accordance with Articles L124-1 et seq. of the French Code of Civil Enforcement Procedures.

2 Acceptance of the Mandate

The Mandate is deemed to have been expressly accepted by the Supplier for the Debts specified once the Supplier has ticked the corresponding box on the Application after sending evidence of the Debts indicating that *"By ticking this box, you agree to give SWIKLY a mandate to collect debts, the basis and amounts of which appear in the elements transmitted via the Application"*.

3 Guarantees

The Company declares that (i) it has taken out professional liability insurance with HYALIN Assurances, which covers it against the financial consequences it may incur due to its debt collection activity, (ii) it has declared its activity to the Public Prosecutor, and (iii) it has opened a bank account to receive the funds collected on the Supplier's behalf.

In connection with the Mandate, the Company declares that it carries out debt collection by sending emails with acknowledgement of receipt to the Customer, without additional measures by the Company, which the Supplier accepts. No obligation to achieve a result is stipulated regarding the actual collection of the Debts.

The Supplier guarantees that it has the capacity to commit itself and give its consent to the collection of the Debts covered by the Mandate. Furthermore, it guarantees that the Debts are unquestionable, liquid and due. Consequently, the Company cannot be liable for any consequences that may result from the absence of the conditions required above regarding the Debt. For this reason, the Supplier shall reimburse any costs incurred and any sentence pronounced against the Company.

4 Obligations of the Company

According to the terms of the Mandate, the Company acts in the name and on behalf of the Supplier in order to collect the Debts. The Supplier therefore authorises the Company to receive payment of all of the Debts on its behalf and authorises it to carry out any acts required to obtain the Debts, including exchanging letters with the Customer (including sending emails), collecting the sums recovered, and more generally, all amicable steps required to collect the Debts.

The Company will not carry out any legal recovery of the Debts.

The Supplier authorises the Company to claim from the Customer any interest on arrears, penalties, compensation and penalty clauses, whether they are by rights, contractual or compromise settlements, that are incidental to the Debt, and authorises it to compromise on these incidental amounts.

5 Obligations of the Supplier

The Supplier undertakes to give the Company all the information required to collect the Debts and guarantees that the information provided is accurate. Otherwise, the Company can be reimbursed for any recovery costs incurred to collect the Debts. In the event of direct contact with the Customer, the Supplier undertakes to inform the Company immediately and to redirect the Customer to the Company.

From the date of acceptance of the Mandate by the Supplier, the Supplier undertakes not to make any further attempts to collect debts from the Customer, and to have given a mandate to collect the Debts solely to the Company, to the exclusion of any other collection agency.

The Debts to be collected and evidence are transmitted via the Application.

6 Duration and expiry of the Mandate

The Mandate is concluded for an indefinite period. Consequently, the Mandate will be terminated on the Supplier's initiative by email.

From the effective date of termination of the Mandate, the Company will stop all procedures to collect Debts from the Customer.

7 Transfer of the amounts collected

The amounts collected shall be transferred by the Company no later than thirty (30) days following receipt of the funds collected by bank transfer.

8 Fees

a) Setting.

The fees set for collection of the Debts are indicated in the estimate of service prices signed by the Supplier, or failing that, 5% of the amounts collected + 25 cts.

The fees set are per Debt.

b) Payment.

The Company reserves the right to deduct its fees before the amounts collected are transferred to the Supplier as stipulated in Article 7 of the Mandate. The fees are due even if the amounts are paid directly to the Supplier. In this case, the Supplier undertakes to pay the Company the amount of the corresponding fees as set out above. If it appears in the course of management that the Debt has been paid by the Customer before the date of transmission of the case, the Company will invoice the specified fees to the Supplier. All the Company's invoices are payable in cash and in the event of non-payment on the due date, the Supplier will be obliged to pay interest on arrears at the legal rate in force plus ten (10) points. Late payment penalties are due without any prior formalities. Furthermore, lump-sum compensation for recovery amounting to forty (40) euros will be due in the event of a commercial debt.

APPENDIX 3. GENERAL AGREEMENT ON THE PROCESSING OF PERSONAL DATA

i. Recitals

WHEREAS this appendix, the "General agreement on the Processing of Personal Data" (the "Agreement") forms part of the General Terms applicable between SWIKLY (the "Processor") and the Supplier (the "Data Controller").

WHEREAS the Agreement is drawn up in order to cover the Processing of Personal Data that takes place due to the provision of the Application to Users by the Processor.

ii. Purpose

In the course of their contractual relations, the Parties undertake to comply with the regulations in force applicable to the processing of Personal Data, and in particular the **GDPR**.

The purpose hereof is to define the conditions under which the Processor undertakes to carry out the Personal Data processing operations defined below on behalf of the Data Controller, in accordance with Article 28 of the GDPR.

A description of the Processing of Personal Data carried out on behalf of the Data Controller by the Processor is given in paragraph "Description of the Processing" page 38.

The Processor is authorised to process, on behalf of the Data Controller, the Personal Data required to provide the Service(s), the Application and the Mandate defined in the General Terms.

iii. Entry into force - Duration of the Agreement - Contractual order of precedence

This Agreement will come into force on the date of acceptance of the General Terms by the Supplier and will apply throughout the period of validity of the Supplier's SWIKLY account.

In the event of a contradiction between this Agreement and any other element of the General Terms, and in particular concerning the articles referring to Personal Data, the Agreement shall prevail.

iv. Processor's obligations towards the Data Controller

The Processor undertakes to:

1. Process the data only on the instructions of the Data Controller and solely for the purpose(s) defined in Appendix "Description of the Processing" below

If the Processor considers that an instruction by the Data Controller constitutes a breach of the GDPR or of any other provision of EU law or Member State law relating to data protection, it shall immediately inform the Data Controller and will be able to refuse to follow the instructions.

Furthermore, if the Processor is required to transfer Personal Data to a third country or an international organisation, in accordance with EU law or the law of the Member State to which it is subject, it must inform the Data Controller of this legal requirement before the processing, unless the law concerned forbids it from informing the Data Controller on important public interest grounds;

2. Guarantee the confidentiality of the Personal Data processed.

3. Ensure that the persons authorised to process the Personal Data:

- undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality
- receive the necessary training on protecting Personal Data

4. Take all the measures required under Article 32 of the GDPR concerning the security of Personal Data for which Processing is subcontracted to the Processor;

5. Sub-processing - General authorisation

The Processor is expressly authorised to call upon one or more Subprocessors after having previously informed the Data Controller of the identity and contact details of the Subprocessor and of the Processing activities that it will carry out. The list of Subprocessors is available by clicking here:

- <https://support.swikly.com/fr/support/solutions/articles/101000452068-rgpd-liste-des-sous-traitants-de-swikly>.

The Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of one or more Subprocessors, who will have the opportunity to object to such changes. If the Data Controller does not object within a time limit of ten (10) days, it will be deemed to have authorised the Processor to use the new Subprocessor.

The Processor is obliged to transfer and impose the same obligations regarding the protection of Personal Data as those set out in this Agreement on any Subprocessor in its contract with the Subprocessor. In particular, the Processor must ensure that the Subprocessor offers sufficient guarantees regarding the implementation of appropriate technical and organisational measures so that the Processing meets the requirements of the GDPR.

If the Subprocessor fails to fulfil its data protection obligations, the initial Processor shall remain fully liable to the Data Controller for the performance of its obligations by the other Processor.

6. Transfers to third countries

In the event of transfer of Personal Data outside the European Union, the Processor undertakes to comply with the provisions of Article 44 of the GDPR. Consequently, Personal Data may only be transferred to a third country if the European Commission has issued an adequacy decision for the non-EU country concerned, recognising an adequate level of protection, or if, in the absence of an adequacy decision, the Processor has provided for appropriate safeguards such as Standard Contractual Clauses, binding corporate rules or any other types of safeguards provided for in Articles 46 et seq. of the GDPR.

7. Right to information of Data Subjects

The Processor publishes information for Data Subjects, [available here](#). This section provides information on the Processing carried out in connection with the provision of the Application, the Service and the Mandate, and describes the rights of Data Subjects regarding their Personal Data and how they can exercise them.

8. The exercise of the rights of data subjects

As far as possible, the Processor shall help the Data Controller, by means of appropriate technical and organisational measures, to fulfil its obligation to deal with requests by Data Subjects to exercise their rights: right of access, rectification, erasure and to object, right to restriction of processing, right to Personal Data portability, and right not to be subject to automated individual decision-making (including profiling).

When Data Subjects make requests to the Processor to exercise their rights, the Processor must send these requests to the Data Controller on receipt, by email to the email address provided by the Supplier when its SWIKLY account was created, or to any address for exercising the rights of Data Subjects provided by the Supplier.

9. Notification of Personal Data Breaches

The Processor shall notify the Data Controller of any Personal Data Breaches within a maximum of seventy-two (72) working hours after discovering it and by any means. The Data Controller will receive these notifications at the email address provided by the Supplier when creating its SWIKLY account or at any address for exercising the rights of Data Subjects provided by the Supplier.

In the event of verbal notification, this must be confirmed in writing.

The notification must be accompanied by any necessary documentation to enable the Data Controller, if necessary, to notify the Breach to the competent Supervisory Authority and to give the competent Supervisory Authority the information specified in Article 33 of the GDPR. The Processor undertakes to give the Data Controller all of the information required for the notification specified in Article 33 of the GDPR, as and when it becomes aware of it.

10. Assistance by the Processor for compliance by the Data Controller with its obligations

The Processor shall help the Data Controller to carry out data protection impact assessments.

The Processor shall help the Data Controller to carry out the prior consultation of the Supervisory Authority.

11. Data Protection Officer

Any questions relating to Personal Data can be sent to the Processor's Data Protection Officer by the Data Controller at the following email address: contact@swikly.com

12. Records of categories of Processing activities

The Processor declares that it maintains a written record of all categories of Processing activities carried out on behalf of the Data Controller, containing:

- the name and contact details of the Data Controller on whose behalf it is acting, of any Subprocessors, and where appropriate, of the data protection officer;
- the categories of Processing carried out on behalf of the Data Controller, as well as the categories of Personal Data and Data Subjects;
- where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the GDPR, the documentation of suitable safeguards;
- where possible, a general description of the technical and organisational security measures, including among others, according to requirements:
 - o the pseudonymisation and encryption of Personal Data;
 - o the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
 - o the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
 - o a process for regularly testing, analysing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

13. Documentation and audit/inspection

In order to demonstrate compliance with all its obligations, the Processor shall make available to the Data Controller the necessary documentation, including the possibility of an audit by the Data Controller or an auditor appointed by it.

The Data Controller can carry out, at its own expense, one (1) audit of the Personal Data protection and security measures taken by the Processor for the Personal Data processed on behalf of the Data Controller, at most once every twelve (12) months, except in exceptional circumstances due to a Personal Data Breach attributable to the Processor justifying an additional audit.

This audit can be carried out by the Data Controller or a third party auditor independent of the Processor and duly appointed by the Data Controller, provided that this third party auditor does not also carry out an activity competing with that of the Processor and/or has no legal relationship with a competitor of the Processor.

A confidentiality agreement must be signed beforehand between the Parties and the third party auditor.

The Data Controller must inform the Processor in writing, giving one (1) month's notice, of its intention to have such an audit carried out and of the identity of the third party auditor selected, where applicable (together with the mandate given), as well as the scope of the planned audit.

The audit carried out by the Data Controller will relate solely to the Processor's compliance with its obligations under the GDPR, in particular in terms of the security and protection of Personal Data processed on behalf of the Data Controller under this Agreement and the General Terms. In any case, the audit operations must not disrupt the functioning of the Processor's services and business.

V. Data Controller's obligations towards the Processor

The Data Controller undertakes to:

1. Determine the purposes and means of Processing in accordance with the GDPR;
2. Obtain the consent of the Data Subjects when it constitutes the legal basis for the Processing carried out;
3. Give the Processor the Data required to describe the Processing that is subcontracted.;
4. Document in writing all instructions concerning Data Processing by the Processor;
5. Ensure, beforehand and throughout the duration of the Processing, compliance by the Processor with the obligations laid down by the GDPR;
6. Supervise the Processing, including carrying out audits and inspections of the Processor in accordance with III. 13. hereof;
7. Keep a detailed record of the Processing activities it carries out;
8. Put in place the technical and organisational measures required in view of the requirements of the GDPR;
9. Use the Services and Mandate in accordance with the GDPR.

VI. Fate of Data

On the expiry of the Supplier's SWIKLY account, for any reason whatsoever, the Processor undertakes to delete the Personal Data or to return them to the Supplier, according to the Supplier's choice.

The Processor will destroy existing copies, unless EU law or French law requires the Personal Data to be retained.

VII. Liability

The Processor and its Subprocessors will only be held liable for any damage arising from the Processing of Personal Data insofar as they have not complied with the obligations resulting from this Agreement or the GDPR, or have acted outside or contrary to the lawful instructions of the Data Controller.

VIII. Description of the Processing

A - Governance of the Processing

Person in charge of GDPR compliance/SWIKLY's DPO	Designated DPO with the CNIL Cabinet Trois(point)quatorze rgpd@swikly.com
Person in charge of GDPR compliance/Supplier's DPO	DPO appointed for the CNIL or person appointed for SWIKLY as responsible for compliance by the Supplier

B - Description of the Processing

Categories of Data Subjects	Users of the Application and Services at the Customer and at the Suppliers
Categories of Personal Data	- For Customers: surname, first name, telephone number, email address, date of birth, postal address - For certain types of Providers (notably healthcare facilities), information revealing a person's health status may be provided to SWIKLY. - For the Supplier: user name and password, surname, first name, email address, telephone number, home address and date of birth of the company's legal representative, country of residence, nationality, means of payment (bank card or bank account), copy of identity papers, proof of address
Purposes of the Processing	- Provision of the Application to Suppliers - Provision of the Services to Suppliers and Customers - Execution of the Mandates Granted by the Supplier and Management of the MangoPay Account - Creation of SWIKLY accounts for Suppliers - Display of the monitoring chart for the Supplier - Implementation of SWIKS - Checking the identity of Suppliers - Alerts and management of fraudulent behaviour - Drawing up an Exclusion List of Customers deemed to be high-risk in particular in order to combat fraudulent use of bank cards and/or behaviour causing damage to the rental property (the criteria for inclusion on the Exclusion List are specified in the General Terms)
Duration	For Supplier Data: duration of the commercial relationship established with the Supplier for data linked to the account For Customer Data: duration of activity on the Supplier's SWIKLY account plus two years. After two years of inactivity, the SWIKLY account will be cancelled For banking data (of the Customer and Supplier): stored for 13 months following the debit date for claims management

Transfers outside the EU	Yes, Only for the support provided to Users. No Application Data is transferred outside the EU (United States - see list of subprocessors below)
--------------------------	--

C - Security measures put in place by SWIKLY

The Processor shall put in place and keep in force the security measures described in this section. The Processor can periodically update or modify these Security measures, provided that the updates and modifications do not lead to a deterioration in the overall security of the Processor's systems and the Services.

1. Infrastructure security

Server security is provided by Microsoft Azure and Amazon Web Services (AWS). Computer access to the server is protected firstly by all the access control measures put in place by AWS and Microsoft Azure, and secondly by the authentication methods detailed below. The hosting providers are certified as Hébergeurs de Données de Santé (HDS – Health Data Hosting certified), in accordance with French regulations.

2. Security of the authentication of persons

a. Authentication of Swikly employees in the internal information system

Each Swikly employee has a unique login user name, i.e. their email address on the Swikly domain. This email address, combined with a password, enables them to access their workspace and applications for which authentication is via a single sign-on (SSO). An access control system makes it possible to identify each user and prevent unauthorised users from accessing or using information resources, as indicated below. The email addresses of all of the users are checked at least twice a year and all inactive email addresses are cancelled, after sending a warning message.

Users are required to use a password to access any electronic information at both system and workstation level.

At system level, to access the Swikly workspace and all of the applications that use a SSO for authentication, a password is required together with the Swikly user's email address.

At workstation level, all Swikly workstations and physical systems are secured before use. This includes:

- encryption of hard disks
- installing a firewall for the operating system.
- installing anti-virus software.
- automatic updating of operating systems.
- password protection of workstations.

b. Authentication of Swikly employees and Users of the Application

Access to the Application by Swikly employees is protected by a single sign-on (SSO) mechanism on the Swikly domain, whereby a specialised department acts as a trusted third party regarding security alerts for potential attempts to log in to the accounts of one of Swikly's employees.

For Suppliers, they can access the Application using multi-factor authentication. Passwords are stored in encrypted form. Encryption keys are used in accordance with best practice for computer security to avoid any fraud and malicious attacks.

3. API key encryption measure and methods of managing encryption keys

The Application's API keys are encrypted. In accordance with best cryptographic practice, Swikly prohibits the extensive re-use of encryption keys wherever possible and regularly rotates keys to generate new cryptographic

material. In addition, access to the encryption keys used in the Swikly application is strictly limited to developers who need to access the application during production.

4. Organisational measures

Swikly makes its employees aware of computer security by using strong passwords and regularly conducting tests of employees for the risk of phishing. A regular audit is carried out of new user access. A security and privacy training course is regularly provided for Swikly employees in order to improve their knowledge of the basic principles of the applicable regulations (in particular the GDPR).

The use made of the cryptographic system in the Application is controlled by the entire team, with developers collaborating regularly in compliance with best practice.

Swikly regularly makes its developers aware of the security of the data they are required to process, as well as of the right procedures to follow when sending alerts, in particular in the event of loss or theft of the company's computer hardware.

Swikly has appointed a Data Protection Officer (DPO) with the CNIL, the French data protection authority responsible for enforcing privacy regulations under the European General Data Protection Regulation (GDPR).

D - Subprocessors authorised for Processing carried out by SWIKLY in the capacity of Processors

The updated list of Subprocessors can be consulted at the following address:

<https://support.swikly.com/en/support/solutions/articles/101000452068-gdpr-list-of-swikly-s-subcontractors>



The solution for your security deposits

APPENDIX 4. MANGOPAY PAYMENT SERVICES MASTER AGREEMENT

APPENDIX 5. MANDATE FOR THE MANAGEMENT OF THE MANGOPAY ACCOUNT

1. Purpose

Within the scope of its activities, the Company may be required to manage the accounts and electronic wallets opened by MangoPay on behalf of the Provider. To carry out the necessary actions for this management, the Provider expressly grants the Company a mandate to manage, on its behalf and for its account, the Provider's MangoPay account (hereinafter the "Mandate") in accordance with the provisions of Articles 1984 et seq. of the Civil Code.

2. Acceptance and Content of the Mandate

The Mandate shall be deemed to have been expressly granted to the Company by the Provider for the following actions as soon as the Provider has accepted the Company's General Terms and Conditions:

- Open an account with MangoPay governed by the MangoPay Payment Services Framework Agreement set out in ANNEX 4 of the General Terms and Conditions within the Swikly environment;
- Initiate, on its behalf, any transfer from the Provider's MangoPay account within the Swikly environment to the Provider's external account(s) previously communicated;
- Consult the balance of the MangoPay account within the Swikly environment and the associated transactions;
- Register, modify, or delete the Provider's external accounts (as trusted beneficiaries) with MangoPay that have been communicated by the Provider to the Company;
- Update the Provider's personal information (email, phone) stored with MangoPay, in accordance with any changes communicated by the Provider to Swikly.

3. Revocation of the Mandate

The Mandate is required for the use of the Swikly Services and may be revoked at any time by sending a simple email to contact@swikly.com.

The portion of the Mandate relating to actions that can be performed on the MangoPay account by the Company may also be revoked directly with MangoPay.

However, in the event of revocation of all or part of the Mandate granted by the Provider to the Company, the Company reserves the right to suspend or immediately terminate access to all or part of the Swikly Service, insofar as the inability to act on behalf of the Provider with MangoPay would make continued use of the Swikly Service impossible.

4. Responsability

The Company is bound by an obligation of best efforts and diligence in carrying out its Mandate. The Company's liability shall be limited to direct damages related to the Principal, within the limits set out in Article 10 of the General Terms and Conditions.

TERMS AND CONDITIONS FOR MANGOPAY PAYMENT SERVICES

Version in force from 30 June, 2026

Presentation

Mangopay S.A. is a limited liability company having its registered office at 4 rue du Fort Wallis, L-2714 Luxembourg and registered with the Luxembourg Trade and Companies Register under number B173459.

Mangopay S.A. ("Mangopay", "we", "us", "our") has created an API for online platform operators allowing them to integrate a payment solution ("the Mangopay Solution") on their website or mobile application, through which Mangopay processes payments between users.

In order to process these payments, Mangopay holds an electronic money institution licence, allowing it to provide payment services throughout the European Economic Area. This licence was issued by the *Commission de Surveillance du Secteur Financier* (CSSF – supervisory authority for the financial sector in Luxembourg 283 route d'Arlon L-1150 Luxembourg, www.cssf.lu) and can be consulted on the [CSSF's official website](http://www.cssf.lu) and on the [European official register \(Euclid\)](http://europa.eu).

Section 1. Definitions

Capitalised terms used in the Mangopay Terms and Conditions shall have the meanings set forth below.

AML/CFT	means the fight against money laundering and terrorist financing.
Chargeback	means any transaction processed through a Payment Method that, after being disputed by the Payer, is partially or fully returned to the Payer, initiated by the issuing payment services provider of the Payment Method used to remit funds to you.
External Account	means the external payment account or external bank account opened with a Third-Party PSP that you have provided to us so that we can pay you the funds available on your Mangopay Account.
External Payment Method	means the payment methods and/or instruments offered to a Payer by a Third-Party PSP to carry out a Transaction on the Platform.
IBAN	means International Bank Account Number (under ISO 13616 standard) and allows to identify a payment account in the payment systems
Identity Data	means the data that you must provide us with in order to register for and use Mangopay Services.
Interface	means the user interface made available to you by the Partner on its Platform

(its website and/or mobile application).

CDD (Customer Due Diligence)	means the identification, verification and ongoing due diligence procedures carried out by Mangopay in relation to you, in accordance with applicable AML/CFT regulations and Mangopay's internal policies. These procedures may include, without limitation, the collection and verification of Identity Data and Supporting Documents, and any additional checks or information required by Mangopay to assess and monitor risks.
Legitimate Ground	means (i) any case where Mangopay has reason to believe, on reasonable ground(s), that there is a risk with respect to the Transaction(s) Mangopay is processing, such as, but without limitation, in case of risk of fraud, risk of Chargeback or risk of dispute of any kind, (ii) any case where Mangopay has reason to believe, on reasonable ground(s), that You will not meet your obligation(s) under the Terms and Conditions, (iii) any case where You breach your obligation(s) under the Terms and Conditions, (iv) any case where Mangopay is not able to verify your identity, (v) any case of dispute regarding your Mangopay Account or (vi) any case where requested by an authority and/or mandated by law.
Mangopay Account	means the account that we have opened in your name after successful completion of the identity verification procedures (CDD) to provide the Mangopay Services.
Mangopay Methods of Payment Method	means the payment methods and/or instruments accepted by Mangopay and which are offered to a Payer to carry out a Transaction on the Platform.
Mangopay Services	means all of the services we provide to you: the Payment Services associated with your Mangopay Account, the ability to request refunds, as well as any other services described in these Terms and Conditions, its annexes or any specific terms and conditions where applicable.
Mangopay Branches	means branches of Mangopay S.A., and includes: - <u>Spanish Branch</u>: Mangopay S.A. Sucursal en España, with registered offices at Calle de Velázquez, 34, Salamanca, 28001 Madrid, Spain; - <u>French Branch</u>: Mangopay S.A. with Registered offices at 4 rue de la Tour des Dames, 75009 Paris, France; and - <u>German Branch</u>: Mangopay S.A. with registered office at c/o WeWork, Stresemannstraße 123, 10963 Berlin – Germany. Individually a "Branch" or collectively the "Branches".
Specific Terms	means the Specific terms for Transfers and Top-ups, as attached to these documents, and that applies only when those services are made available to you through your use of the Platform, as approved by Mangopay.
Terms and Conditions	means these Mangopay Terms and Conditions for the use of the Mangopay Services.

Transfer	means a transfer of funds initiated from your Mangopay Account to another Mangopay Account or received on your Mangopay Account from another Mangopay Account (in relation to the use of the Platform), as framed in the Specific Terms related to Transfers and Top-ups.
Platform Agreement	means the agreement you have entered into with the Partner to use its services and Platform.
Supporting Document	means any supporting document that we request from you in order to validate or verify your identity.
Payment Method	means an External Payment Method and/or Mangopay Payment Method.
New User	means a user of the Platform that uses Mangopay Services for the first time.
Partner	means the entity that operates the Platform (the website and/or mobile application) you use and that has integrated the Mangopay Solution to process payments on its Platform.
Payer	means a person who makes a payment to you on the Platform via the Mangopay Solution.
Payment Operation	means all the payment operations executed by Mangopay as part of the Services provided to you, including receiving Transactions, execution of Payouts, and where the case may be, execution of Transfers.
Payment Services	means certain payment services as defined in EU Directive 2015/2366 (also known as "PSD2") that we provide to you as part of your use of the Platform. These services include the acceptance and processing of Payment Operations in order to transfer the corresponding funds to you.
Payout	means the withdrawal of all or part of the funds recorded in your Mangopay Account to your External Account
Platform	means the website or mobile application operated by the Partner that integrates the Mangopay Solution in order to process payments via the Methods of Payment.
Reserve	means a minimum amount of funds that you may be required to hold in your Mangopay Account which can be reserved by Mangopay and which may be temporarily not available for payment to your External Account. The amount of the Reserve may correspond (i) to a percentage of the Transactions received on your Mangopay Account on a given frequency or (ii) to a lump sum.
SCA Procedure	refers to a strong customer authentication process that Mangopay may require you to complete, as deemed necessary by Mangopay and/or required by certain laws and regulations to reduce fraud risks.
Third-Party PSP or	means any payment service provider other than Mangopay.

PSP

Transaction means the funds that a Payer transfers to you, which we collect on your behalf in order to allocate the funds to you.

Section 2. Purpose and Scope of the Terms and Conditions

These Terms and Conditions govern the Mangopay Services we provide to you. When we refer to "you" (or "your"), we mean any person who subscribes to the Partner's services via its Platform who uses the Mangopay Services to receive payments related to their activities on the Platform. The Services provided by Mangopay can only be used in connection with your activities on the Partner's Platform. In certain cases, our Branches may be involved in the provision of Services to you; for instance where an IBAN is assigned to your Mangopay account.

These Terms and Conditions only apply to persons who meet the conditions described above and for whom CDD has been successfully completed, in accordance with Article 3. In particular, these Terms and Conditions do not apply to persons who use the Platform solely for the purpose of making a payment to another user using one of the proposed Mangopay Payment Method (identified as a Payer). We invite these individuals to consult our Privacy Policy (<https://mangopay.com/privacy-statement>) to find out specificities of the data we collect when processing payments.

You agree to comply with the Terms and Conditions, as well as any related specific terms and conditions where applicable, at all times during the term of your business relationship with Mangopay.

Section 3. Registration and use of Mangopay Services

3.1. Eligibility conditions

The eligibility requirements for our Mangopay Services depend on your status. The conditions specific to each situation are described below.

If you are a natural person not acting for professional purposes. To use Mangopay Services as a natural person acting as a consumer, you declare and guarantee that:

- You are at least 18 years of age;
- You have the legal capacity to accept these Terms and Conditions and to use Mangopay Services;
- You are not acting in the context of a professional activity (commercial, industrial, craft, liberal or agricultural activity);
- All information you provide at registration, or provided by you while using Mangopay Services, is true, accurate and up to date;
- You are registered with the Partner as acting for non-professional purposes;
- You are acting in your name and on your own behalf when using Mangopay Services;
- You are not acting in the context of activities prohibited by law;
- You are not engaging in any activity prohibited by Mangopay. Prohibited activities are indicated on our website (<https://mangopay.com/prohibited-businesses>).

If you are a legal entity (e.g. a company or association). To use Mangopay Services as a legal entity you declare and guarantee that:

- You are a legal representative of the registered legal entity and have full authority to legally bind them to these Terms and Conditions;
- All information you provide at registration, or provided by you while using Mangopay Services, is true, accurate and up to date;
- The legal entity is duly incorporated as a company, association or otherwise and is registered in a country supported by Mangopay. The supported countries are indicated on our website (<https://docs.mangopay.com/guides/users/country-restrictions>);
- The legal entity is listed on the Partner's Platform as acting professionally or, where applicable, for non-profit purposes if the legal entity has a non-profit purpose;
- The legal entity is acting on its own behalf when using the Mangopay Services;
- The legal entity does not carry out activities prohibited by law;
- The legal entity does not carry out an activity prohibited by Mangopay. Prohibited activities are indicated on our website (<https://mangopay.com/prohibited-businesses>).

If you are an individual acting for professional purposes. To use Mangopay Services, you declare and guarantee that:

- All information you provide at registration, or provided by you while using Mangopay Services, is true, accurate and up to date;
- You regularly carry out your professional activity in accordance with the regulations of your country of operation and, where this regulation so requires, you are duly registered and/or listed with the competent authorities (including tax) and/or relevant registers in a country that is a party to the agreement on the European Economic Area or in a third country imposing equivalent obligations in terms of AML/CFT;
- You are listed on the Partner's Platform as acting for professional purposes;
- You are acting on your own behalf when using Mangopay Services;
- You are not engaging in any activity prohibited by Mangopay. Prohibited activities are indicated on our website (<https://mangopay.com/prohibited-businesses>).

3.2. Onboarding process and conditions for registration with Mangopay Services

To register with Mangopay Services, you must follow the registration procedure indicated by the Partner. Unless the Partner advises you differently, the Terms and Conditions are concluded remotely via an interface hosted by Mangopay (or via the Partner's Interface, as the case may be) and this is confirmed by an online acceptance procedure. In this regard, you must have the appropriate equipment (hardware and software), for which you are solely responsible.

The acceptance of the Terms and Conditions forms part of the onboarding process with Mangopay. However, these Terms and Conditions enter into force only upon the successful completion of CDD. Prior to such completion, no contractual relationship exists between you and Mangopay.

Prior to the entry into force of the Terms and Conditions, you may be required to provide information and documents for the purpose of CDD. Mangopay reserves the right to accept or reject any onboarding request at its sole discretion.

During the onboarding procedure (or at any time during the use of the Mangopay Services), you may be required to complete a strong customer authentication enrollment process in order to allow the performance of any further SCA Procedure. Failure to complete this enrollment process may result in one or more of the following consequences: (i) you will be unable to complete your registration and use the Mangopay Services and; (ii) Mangopay reserves the right to take actions as outlined in Section 7.

Notwithstanding the above, Mangopay may, at its sole discretion, enable access to certain limited functionalities prior to the completion of some or all of the CDD process. Where relevant, such limited functionalities are made available on a temporary and exceptional basis and may be restricted, suspended or withdrawn at any time by Mangopay until the required CDD process has been successfully completed. The availability of such limited functionalities shall not affect the principle that access to the full scope of Mangopay Services contemplated under these Terms and Conditions remains subject to successful completion of the CDD process.

3.3. Mandatory information and documents

Applicable regulations require us to identify you and verify your identity (CDD) in order to provide you with the Mangopay Services. As part of your business relationship with Mangopay, you will be required to provide us with specific Identity Data and Supporting Documents via the Partner's Interface or via a Mangopay interface, as the case may be. This information must be correct, complete and up to date at all times.

The initial provision of Identity Data and Supporting Documents forms part of a pre-contractual onboarding process prior to the entry into force of these Terms and Conditions.

You agree to provide the requested Identity Data and Supporting Documents promptly upon request and acknowledge that Mangopay may request such information at any time.

For registration with the Mangopay Services and until CDD has been successfully completed:

- no contractual relationship shall exist between you and Mangopay;
- Mangopay Services shall not be provided;
- no Mangopay Account shall be opened.

Mangopay reserves the right to reject any onboarding request or to discontinue the onboarding process where CDD cannot be successfully completed. Mangopay may also reject onboarding requests that are not completed within a reasonable period of time.

The list of required Identity Data and Supporting Documents is as follows (not exhaustive):

	Identity data	Supporting documents
--	---------------	----------------------

Legal entity	Company name; company email address; surname, first name, date of birth, nationality and country of residence of the legal representative(s). For associations: name of the association; name of the legal representative(s) (chairperson or co-chairperson, treasurer or secretary).	Identity document of the legal representative(s); articles of association of the legal entity; certificate of registration in the companies register. For associations: proof of registration; articles of association; a document confirming the capacity of the legal representative(s) (if it is not stated in the articles of association).
Natural person acting for professional purposes	Company name; company email address; surname, first name, date of birth, nationality and country of residence of the legal representative.	Identity document of the legal representative; certificate of registration in the companies register.
Natural person over the age of 18 acting for non-professional purposes (consumer)	Surname, first name, date of birth, nationality and country of residence; email address.	Identity document

We may adapt this list at any time, depending on changes in the regulations that apply to us, our internal procedures or where Mangopay deems it necessary to complete certain verifications. We may also request that you provide us with updated Identity Data and Supporting Documents as part of our obligations to maintain up-to-date information concerning our users, and you are required to provide such information upon request.

If the information provided (Identity Data and/or Supporting Documents) is incomplete or incorrect, the registration request will be declined and no Mangopay Services will be provided. We may also ask you for any other additional documents we consider necessary for our AML/CFT controls, and you are required to provide such information upon request.

3.4. Conditions for access to Mangopay Services

Mangopay Services are only available once CDD has been successfully completed. Until CDD has been successfully completed, Mangopay shall not provide any Mangopay Services and any attempted Transaction, including any payment made in your favor, shall be declined or not processed by Mangopay.

3.5. Receiving payments (Transactions) and making refunds

3.5.1. Transactions made via a Mangopay Payment Method

The following provisions shall apply in the event that the Partner has integrated one or more Mangopay Payment Methods on its Platform. The Payment Methods provided by Mangopay are identified as such

on the Platform. Mangopay Services allow you to receive Transactions from a Payer as part of your activities carried out on the Platform. We collect these Transactions and record them in your Mangopay Account. To carry out a Transaction, Payers can choose the Mangopay Payment Methods available on the Partner's Platform, under the terms we have agreed with the Partner. The Mangopay Payment Methods that are available to Payers may vary from time to time, the availability of Mangopay Payment Methods will be indicated by the Partner. This may include card payments, receipt of transfers (SEPA or international), and receipt of direct debits.

Transactions may only be received and recorded in a Mangopay Account once CDD has been successfully completed. Where CDD has not yet been successfully completed, any attempted Transaction shall be declined or not processed. Mangopay does not process, receive or hold any funds on your behalf prior to the successful completion of CDD. Once CDD is successfully completed, Transactions orders we receive on your behalf are recorded in your Mangopay Account, provided that we have received all necessary instructions and the corresponding funds from the Payer's PSP.

Disputing Transactions we have received for you – Depending on the Mangopay Payment Method used by a Payer, the Payer may be entitled to dispute a Transaction in accordance with the rules of said Mangopay Payment Method, even in the absence of fraudulent grounds ("Disputed Transaction"). This is particularly the case for card and direct debit Payment Methods. In the event that the Payer disputes a Transaction and we are required to return the funds to the Payer via the Mangopay Payment Method used for the Transaction, which is deemed to constitute a Chargeback, you remain financially liable to Mangopay for the full amount of such Chargebacks or refunds. Therefore, we reserve the right to deduct the corresponding amount from your Mangopay Account, including by offsetting such amount. In this case, we may proceed with the total or partial reversal of the disputed Transaction. Where applicable, we may also recover, by any means, including the Withholding Mechanism stated in section 3.8, the amount corresponding to the return of the funds for each Transaction in the event that you have insufficient funds in your Mangopay Account, without prejudice to our legal capacity to subrogate to your rights in order to recover the sums due by the Payer by any other means.

If a disputed Transaction can be contested by providing supporting evidence, you shall fully cooperate and provide the Partner and/or Mangopay, as requested, with all necessary information and documents deemed necessary to handle the dispute. Such information must be submitted within the timeframe specified in the request.

The recording of Transactions on your Mangopay Account in various currencies – We may be able to record Transactions we received on your behalf in the currency used by the Payer, depending on the geographical scope of the Partner and the currencies that are made available by us in this regard. You may therefore have several Mangopay Accounts in various currencies; every Mangopay Account will be denominated in a single currency.

Refunding a Transaction – If you wish to refund a Payer in connection with a Transaction, you may request the total or partial cancellation of a Transaction we have received for you in accordance with this article. Cancellation of the Transaction will only be possible if the funds corresponding to the amount to be refunded are available in your Mangopay Account.

The total or partial cancellation of the Transaction will be carried out using the Mangopay Payment Method initially used by the Payer for the respective Transaction, within the limits of the rules of each Mangopay Payment Method (specifically card schemes and SEPA rules), no later than ten (10) business days following receipt of the refund request.

The cancellation of a Transaction may not always be possible for various reasons (such as when the refund takes place more than 11 months after the date of the Transaction to be reimbursed for Mangopay Payment Methods such as card). In this case, the Transaction will be refunded to the Payer using another Payment Method.

You agree that any information we may need to make a refund will be sent to us directly by the Partner.

3.5.2. Transactions carried out via an External Payment Method

The following provisions shall apply in the event that the Partner has integrated one or more External Payment Methods on its Platform. The External Payment Methods are made available to Payers by the Third-Party PSP selected by the Partner, in accordance with the terms agreed between the Partner and the Third-Party PSP. Transactions are processed by the Third-Party PSP and settled with Mangopay by the Partner or directly by the Third-Party PSP. Transactions we receive on your behalf are recorded in your Mangopay Account, provided that we have received all necessary instructions and the corresponding funds. In any case, transaction orders will only be accepted and Transactions processed once CDD has been successfully completed. Where CDD has not been completed, such Transactions shall not be processed or shall be declined.

Dispute by the Payer – We inform you that the Payer is entitled to dispute any Transaction with their PSP, up to thirteen (13) months following the date on which the account linked to the External Payment Method they used to carry out the Transaction was debited. These disputes are managed exclusively by the Partner. We invite you to contact them directly for any request related to disputes.

Refunding a Transaction – If you wish to refund a Payer, you can request the cancellation of a Transaction. If your refund request is initiated more than one day after the date of the receipt of the Transaction, it may only be executed if the funds we hold on your behalf are sufficient to cover your request.

3.6. Paying funds into your External Account

(i) Registering an External Account

Funds recorded in your Mangopay Account will be transferred to the External Account you registered. In this regard, you must hold the External Account that you register, unless otherwise permitted by Mangopay. You must provide the following information via the Platform's Interface: IBAN number, BIC (optional), your surname, first names and exact postal address in your capacity as an External Account holder. You may add or change your External Account at any time via the Platform's Interface provided you follow the procedure for the registering of the External Account and provided you completed the SCA Procedure, where applicable.

(ii) Paying funds into your External Account

We will make payments to your External Account automatically and periodically (except where Article 3.7 below applies). In this regard, you agree that the information relating to the frequency of payments into your External Account will be communicated directly to us by the Partner. In some cases, you may change the payment frequency on the Platform's Interface on a one-off or permanent basis.

We may block a payment if we suspect fraudulent or unlawful use of the Mangopay Account, breach of the Mangopay Account's security, if CDD requirements are not fulfilled or are no longer satisfied or for AML/CFT reasons, including in the event of an asset freezing measure made against you by an administrative authority or any other reason as set out in Article 7.

If you notice that a payment is made with errors, you can notify the Platform's customer service department of this error. If the error is attributable to us, we will rectify the situation as soon as possible.

The execution of any transaction, including payment into your External Account is subject to the continued compliance with Mangopay's CDD and AML/CFT obligations.

(iii) Currency of payments remitted to your External Account

Funds recorded in your Mangopay account will in principle be paid into your External Account in the currency in which the Transactions were recorded in your Mangopay Account and in which you expect a payment. We recommend that you check whether any additional fees can be applied by the PSP holding the External Account in the event that the currency of funds payment indicated in your Mangopay Account is not the currency of your External Account.

3.7. SCA Procedure

You acknowledge that certain actions you may take using the Mangopay Services are subject to the SCA Procedure, at Mangopay's discretion.

These verifications may be required in various situations, including but not limited to:

- Accessing to your Mangopay Account
- Updating your Identity Data (including those used for SCA Procedure)
- Registering or modifying an External Account
- Executing a Payment Operation

Failure to complete the SCA Procedure may result in one or more of the following consequences: your request may be denied (such as the execution of the Mangopay Services) or Mangopay Services may be restricted at Mangopay's discretion.

3.8. Verification of payee

You acknowledge that certain actions you perform using the Mangopay Services — such as registering your external account or paying funds into your external account — may, where required, be subject to the verification of payee process under Regulation (EU) 2024/886 on instant credit transfers in euro. This rule is particularly important for Mangopay Accounts that have an associated IBAN.

Before authorising the said action, you will be informed by the Partner about whether or not the payment account identifier (IBAN) and the name of the payee that you have provided match with the corresponding data kept by the payment service provider of the payee.

If the IBAN and the name of the payee do not match or when the verification check is not possible, you will be informed that authorising the action might lead to transferring the funds to an external account

not held by the payee indicated by you. If you go ahead with this action, we cannot get your funds back if they are sent to the wrong payee.

3.9. Other services

3.9.1. Top-up and Transfers

In the event that you have the option on the Platform to use the balance available in your Mangopay Account to transfer funds to another Platform user or to fund your own Mangopay Account through a Top-up, the specific terms relating to the Transfers and Top-up also apply in addition to these General Terms and Conditions. You can consult the [Specific Terms](#) below.

The services described in this Article 3.9.1 and in the Specific Terms are only available once CDD has been successfully completed and a Mangopay Account has been opened.

3.10. Withholding Mechanism and Reserve

The following provisions aim to mitigate the risks for Mangopay and its customers (i.e. the Platform) related to Transactions in particular in case of Chargebacks, fraud or other potential risks.

(i) Withholding Mechanism

By way of derogation to article 3.6 (ii) of the Terms and Conditions, in the event that you are a New User or in case of Legitimate Ground, we reserve the right to defer the time at which we will pay the funds into your External Account (the "Withholding Mechanism").

Except where mandated by law and/or an authority, we will cease to apply the Withholding Mechanism as soon as there are reasonable grounds to consider that the risk(s) identified by us (i) to us, (ii) to the Partner, (iii) to any other user of the Platform and/or (iv) to any other user of Mangopay Services have decreased or been managed in such a manner that the Withholding Mechanism is no longer deemed necessary.

You acknowledge and agree that we may set-off the amount withheld on your Mangopay Account under the Withholding Mechanism against any sums due by you to us under the Terms and Conditions, including but not limited to Chargebacks.

(ii) Reserve

We reserve the right to apply a Reserve on your Mangopay Account in case of Legitimate Ground. Before requiring a Reserve, we consider various risk factors such as, but not limited to: your Mangopay Account history, the amount and the number of refunds, disputes or Chargebacks linked to your Mangopay Account, the amount of Transactions we process on your behalf on the Platform, the number of Transactions we process on your behalf on the Platform, your risk profile and funds you may owe Mangopay.

If we apply a Reserve on your Mangopay Account, we will provide you with written notice specifying the terms of the Reserve.

Except where mandated by law and/or an authority, the Reserve is released by us as soon as there are reasonable grounds to consider the risk(s) identified by us (i) to us, (ii) to the Partner, (iii) to any other user of the Platform and/or (iv) to any other user of Mangopay Services have decreased or been managed in such a manner that the Reserve is no longer deemed necessary.

You acknowledge and agree that we may set-off the amount of the Reserve against any sums due by You to Mangopay under the Terms and Conditions.

The Withholding Mechanism and the Reserve can be cumulative.

3.11. Fees payable to the Partner

You authorise us to deduct from your Mangopay Account any fees agreed between you and the Partner in the Platform Agreement in connection with the services provided by the Partner. In this regard, you agree that the amounts to be deducted will be communicated to us by the Partner. In the event of a dispute relating to the amount of the fees agreed between you and the Partner and which we have deducted, we invite you to contact the Platform's customer service department.

3.12. Protection of funds

The funds we hold on your behalf are protected in accordance with the terms of Article 24-10 (5) and Article 14 of the Law of 10 November 2009 published in Memorial A No. 215 of 11 November 2009 of the Grand Duchy of Luxembourg.

3.13. Blocking your Mangopay Account and Mangopay Services

We may block your Mangopay Account and suspend Mangopay Services for reasons relating to the security of the Mangopay Account, on the presumption of unauthorised, unlawful or fraudulent use of the Mangopay Account and/or Mangopay Services, in the event of serious breaches under these Terms and Conditions, suspicions of money laundering or terrorist financing, asset freezing measures made against you, if CDD requirements are not fulfilled or are no longer satisfied or at the justified request of our banking partners or card schemes where the latter consider that your use of the Mangopay Services is in breach with their rules. For any questions relating to the blocking of your Mangopay Account or the suspension of Mangopay Services, we invite you to first contact the Platform's customer service. We inform you that in some cases, we are prohibited by law from providing you with reasons for blocking the Mangopay Account or suspending the Mangopay Services.

Mangopay, as a subsidiary of a company based in the United States of America, takes into account the economic sanctions and other restrictive measures implemented in particular by the Office of Foreign Assets Control (OFAC) of the US Treasury Department. Where Mangopay deems it appropriate or necessary, Mangopay may restrict a Transaction, suspend and/or stop providing you with all or part of the Mangopay Services and/or terminate these Terms and Conditions immediately if we detect that you are a person designated in the OFAC measures/sanctions and/or that Transactions in your Mangopay Account more generally involve (i) persons, (ii) countries or (iii) specific products/services originating from certain countries/geographic areas covered by the OFAC, in addition to trade restrictions imposed by related laws and regulations.

We will unblock your Mangopay Account and Mangopay Services when the reasons justifying the blocking no longer exist.

3.14. Security

We may temporarily suspend use of the Mangopay Account and/or Mangopay Services for technical, security or maintenance reasons, without these operations giving rise to any form of compensation. We will use our best efforts to limit these types of interruptions to what is strictly necessary.

You must take all reasonable steps to control and ensure the security of the devices you use to access the Platform and Mangopay Services. If you are a legal entity, you must also ensure that only persons authorised by you use the Mangopay Services. You are fully responsible for the use made of the Mangopay Services and access to the Mangopay Account by anyone authorised by you in this regard, and our liability shall not be sought in this respect. You must notify us without undue delay upon becoming aware of any loss, theft, misappropriation or unauthorised use of or unauthorised access to, your Mangopay Account or any personalised security credentials associated with it. In such a case, your notification to Mangopay shall not in itself, affect the allocation of liabilities under these Terms and Conditions.

3.15. Anti-Money Laundering and Countering the Financing of Terrorism

In order to provide you with the Mangopay Services, the applicable regulations concerning anti-money laundering and countering the financing of terrorism (AML/CFT) require us to identify you and verify your identity, as well as that of your beneficial owner in the event that you are a legal entity.

In some cases, we may also need to obtain information concerning a Payment Operation (such as its purpose, origin or destination) or the use of your Mangopay Account. As such, if we consider that the information available to us is not sufficient, or if this information reveals any concerns regarding money laundering or terrorist financing, we may at any time suspend the use of your Mangopay Account and the provision of Mangopay Services, without prejudice to our entitlement to request the termination of the Terms and Conditions binding us, if we believe that by continuing to provide you with the Mangopay Services we will be unable to comply with our AML/CFT obligations.

We inform you that the Mangopay Services we provide to you may be subject to the exercise of the right of communication by the competent authorities, such as the national financial intelligence unit. No civil liability suit or action may be brought or any professional sanction imposed against Mangopay, its directors or its agents who have reported the suspicious activity to their national authority in good faith.

Mangopay may, at any time, require you to provide updated Identity Data and Supporting Documents as part of its ongoing CDD obligations. Failure to comply with such requests may result in the suspension of Mangopay Services, the blocking of your Mangopay Account, refusal to execute any Transaction or closure of your Mangopay Account.

3.16. Authorised Proxy

You may grant a power of attorney to any authorised person (an “**Authorised Proxy**”), including the Platform, to perform certain actions on Your behalf on Your Mangopay Account, among which

accessing to your account balance and associated transactions, executing Payment Operations, registering and/or modifying an External Account and change of personal information (e.g. email or telephone number).

Any action requested by an Authorised Proxy will be deemed validly authorised by you and executed on your behalf, as long as the proxy remains applicable. We will not be responsible for any dispute arising from any instruction received from an Authorised Proxy or from any disagreement between you and an Authorised Proxy. You accept full responsibility for granting such authority. You may at any time revoke a proxy granted to an Authorised Proxy by notifying Mangopay.

Section 4. Modification, term and termination

4.1. Modification of the Terms and Conditions

We may amend the Terms and Conditions at any time. You will be notified of any amendments by Mangopay or through the Partner. If amendments to the Terms and Conditions are made necessary due to legislative or regulatory provisions, they shall apply immediately. In other cases, you will be informed of any amendments at least two (2) months before they come into effect and you will have the option to refuse the amendments by notifying us of your refusal. By continuing to use Mangopay Services through the Platform after the two-month period, it means that you acknowledge and agree to the amended version of the Mangopay Terms and Conditions. If you decide that you do not agree to it, then it is necessary to close your Mangopay account. This closure will mean you are no longer able to receive payments through the Platform. To proceed with the closure of your Mangopay account, you will have to withdraw all remaining funds to an External Account. You can also notify the Platform or Mangopay customer support services of your desire to close your Mangopay account.

4.2. Entry into Force, term and termination

These Terms and Conditions are concluded for an indefinite period. They shall enter into force only upon the successful completion of CDD, at which point your Mangopay Account will be open and you will be able to access the Mangopay Services, subject to any limited functionalities that may exceptionally be made available prior to such completion pursuant to Section 3.2. Prior to such completion, no contractual relationship shall exist between you and Mangopay.

You may terminate these Terms and Conditions at any time. We may also terminate the Terms and Conditions at any time by giving two (2) months' notice. Regardless of whether the termination is at your or Mangopay initiative, it must be notified to the other party by any means, including by email. If you wish to terminate by email, termination at your initiative may be sent to the Platform's customer service department or to Mangopay at: eu-account-closure@mangopay.com. You agree that your termination request can be sent to us by the Partner where applicable. If an investigation is ongoing at the time of the request to terminate your Mangopay Account, we may block your Mangopay Account as stated in Article 3.12.

We may also terminate these Terms and Conditions by simple notification (including by email) without prior notice in all the cases provided for in Article 7 as well as in the following cases: serious breaches under these Terms and Conditions; non-compliance with the eligibility conditions provided for in Article 3.1; refusal or failure to provide the mandatory or updated required under Article 3.3; fraudulent or unlawful use of Mangopay Services; serious suspicion of money laundering or terrorist financing;

upon justified requests from our banking partners or card networks where the latter consider that your use of Mangopay Services is contrary to their rules, or when you are subject to or if one of your Payment Operation is subject to restrictive measures or economic sanctions.

We may also terminate the Terms and Conditions upon notification in the following cases:

- If your Mangopay Account is inactive, as defined below;
- In the event that your Platform Agreement ends (at your initiative or at the Partner's initiative).

We inform you that the termination of the Terms and Conditions (and therefore the closure of your Mangopay Account) is only effective when the Mangopay Account has a zero balance.

4.3. Inactivity

Your Mangopay Account will be considered inactive if you have not initiated any action on your Account (such as initiating a Payout, Transfer or funding your Account) for a period of two (2) years (i.e. 730 days) and have not contacted us within that timeframe. When the balance of your inactive Mangopay Account is positive, you will receive a notification of inactivity. If your Mangopay Account has a positive balance and you do not demonstrate your willingness to continue using Mangopay Services, you will need to recover the funds in an External Account held by you to enable the closure of your Mangopay Account, or where possible, the recorded funds will automatically be deposited in your External Account. In the event that we are unable to pay you the funds, we will continue to administer your assets diligently, in return for which we reserve the right to deduct an administrative management fee of thirty (30) euros per year.

These administrative management fees will be limited to the positive balance available in the Mangopay Account. Once the balance of your Mangopay Account becomes zero, we reserve the right to close the Account and to terminate these Terms and Conditions permanently. Until you take the necessary steps to recover the funds recorded in your Mangopay Account, the Account will remain blocked and maintained solely for the purpose of transferring the amounts due to the External Account you have registered, without prejudice to the administrative management fees charged by Mangopay.

4.4. Consequences of the end of the contract between Mangopay and the Partner

We inform you that, if the contract we have entered into with the Partner for the integration of the Mangopay Solution ends, we will terminate the Terms and Conditions, by giving two (2) months' notice.

If applicable, if the balance of your Mangopay Account is zero, the Account will be closed at the end of the notice period and the Terms and Conditions will be deemed terminated.

If your Mangopay Account has a positive balance, you must transfer the funds to an External Account held in your name in order to close your Mangopay Account. If you do not recover your funds, we will continue to administer your assets with due diligence in accordance with the provisions below.

If the Partner no longer uses the Mangopay Services, Your Mangopay Account will be considered inactive if you have not initiated any action on your Account (such as a Payout, Transfer or funding your Account) for a period of one (1) year (i.e. 365 days) and have not contacted us within that timeframe. You will receive a notification of inactivity by email inviting you to transfer the funds to an

External Account held in your name in accordance with the procedure that will be stated in the inactivity notification. If you are unable to transfer the funds from your Mangopay Account to your External Account, your funds will be held by Mangopay, in return for which we will deduct an administrative management fee of thirty (30) euros per year.

These administrative management fees will be limited to the positive balance available in the Mangopay Account. Once the balance of your Mangopay Account becomes zero, the Account will be closed and the termination of these Terms and Conditions will be completely effective. .

Until you take the necessary steps to recover the funds recorded in your Mangopay Account, the Account will be maintained solely for the purpose of transferring the amounts due to the External Account you have registered, without prejudice to the administrative management fees charged by Mangopay.

4.5. Death (Natural Person)

In the event of death, we will cease to provide the Mangopay Services. We will also restrict payments to the External Account until we receive instructions from the beneficiaries or notary in charge of the estate. Your funds may only be remitted to your beneficiaries when the documents allowing us to verify their legitimacy and identity are provided.

4.6. Consequences of termination

In the event of notice of termination of the Terms and Conditions, you will no longer be able to use all of the Mangopay Services and your Mangopay Account will be restricted to the operations necessary to transfer the funds recorded in your Mangopay Account into your External Account. The funds we hold in your Mangopay Account will be transferred to your External Account, subject to compliance with the identification requirements set out in Article 3.3. Your Mangopay Account will be permanently closed and the termination of the Terms and Conditions completely effective once the Mangopay Account has a zero balance.

Section 5. Fees

We do not receive a fee for the use of Mangopay Services except in the event of inactivity of your Mangopay Account as set out in Article 4.3.

Section 6. Limitation of liability

Our liability is limited to the provision of Mangopay Services. We do not intervene in any legal or commercial relations, or in any disputes between you and the Partner, between you and a Payer or between you and any other user of the Platform. We do not exercise any control over the compliance or characteristics of the products and services for which we process a payment. We are extraneous to the contract between you and a Payer or between you and the Partner. As a result, we cannot be held liable for the non-performance or improper performance of the obligations resulting therefrom, nor for the fault, misconduct or negligence of any Payer or Partner committed towards you. The Partner is solely responsible for the security of their Platform, and you must contact the latter concerning any dispute relating to the use of their Platform..

We shall under no circumstances be held liable (i) in the event of Mangopay Account blocking or suspension of the Mangopay Services which occurs in the cases provided for in these Terms and Conditions, (ii) in the event of unavailability of the Platform or your Interface, (iii) in the event of unauthorised access to your Interface or a security breach of the Platform, (iv) in case of interruption or disruption to our software and computer systems used to provide the Mangopay Solution, (v) in the event of non-performance or improper performance of the obligations arising from your contract with a Payer or with the Platform and (vi) in the event that a Transaction, Transfer, Top-up or Payment Operation is declined or not processed because CDD requirements have not been fulfilled or are no longer satisfied. In all cases, our liability is limited to compensation for direct damages related to our breach of any of our obligations under these Terms and Conditions, except in cases where such a limitation is prohibited by applicable law.

Section 7. Your commitments

For the entire duration of your use of the Mangopay Services, you agree to comply with the following conditions:

- Your use of Mangopay Services is not contrary to (i) public order, (ii) morality, or (iii) applicable laws and regulations and (iv) does not infringe the rights of third parties;
- Your use of Mangopay Services is exclusively for the purpose of carrying out Transactions under the Platform Agreement;
- You agree not to use Mangopay Services for activities that are prohibited. The list of prohibited activities is available on our website (<https://mangopay.com/prohibited-businesses>);
- You agree not to impersonate another person or entity, falsify or conceal your identity or age, or create a false identity.
- You agree to remain financially liable to Mangopay for the full amount of all Chargebacks, refunds, and fines that arise from your use of Mangopay Services.

In the event of a breach of these commitments, we reserve the right to take a number of measures to protect Mangopay, at any time and at our sole discretion. In particular, we may, without notice, take the following actions:

- Terminate these Terms and Conditions;
- Restrict your Mangopay Account and/or suspend Mangopay Services;
- Block your Mangopay Account;
- Refuse to provide you with Mangopay Services in the future, including on other platforms,
- Suspend your funds to the extent reasonably necessary and for as long as reasonably necessary;
- Refuse at any time any Transaction, in this case we will notify you of the refusal and reasons within the limits imposed by law.

We are entitled to take any private legal action to compensate for any damage suffered by us as a result of your breach of your obligations under these Terms and Conditions. If you observe a breach of the aforementioned obligations, you may inform us of these actions by contacting us at: compliance@Mangopay.com.

Section 8. Protection of your personal data

In connection with the provision of Mangopay Services, we process your personal data ("Data"). In accordance with European Regulation (EU) 2016/679 ("General Data Protection Regulation" or "GDPR"), only Data strictly necessary for the fulfilment of the specified purposes described in Mangopay's privacy statement is processed. For more information regarding the processing of your Data by Mangopay, please consult our privacy statement at: <https://mangopay.com/privacy-statement>. For any questions or requests relating to the processing of your Data, you can contact us at any time at: dpo.mangopay@mangopay.com.

By signing these Terms and Conditions, you: (i) declare that you have read our privacy statement available on Mangopay's commercial website at the following address: <https://mangopay.com/privacy-statement>; (ii) you agree to consult our privacy statement periodically, since you are aware that it may be adapted according to changes to our personal data processing activities or to applicable regulations, with the latest version published on the Mangopay commercial website prevailing; (iii) in the event that you act as legal representative of a legal entity or association, and that you provide us with personal data relating to a third party, you undertake to communicate our privacy statement (<https://mangopay.com/privacy-statement>) to such third party(ies).

Section 9. General Provisions

9.1. Professional secrecy

We are subject to strict professional secrecy obligations.

You agree that professional secrecy will be waived for the benefit of the service providers with which we subcontract operational functions relevant for the provision of the Mangopay Services. Service providers with whom we will share data covered by professional secrecy provide us with services related to fraud prevention, anti-money laundering and countering the financing of terrorism, as well as the hosting and security of our technical infrastructure, and customer support services. The data concerned are your Identity Data as well as data related to Transactions carried out through the use of Mangopay Services. We may also share certain technical data relating to the device you use (computer, telephone, etc.), your e-IDs, your IP address and information about your interaction with our Partner's Platform for fraud prevention purposes. Our service providers are generally located within the European Union, particularly in Luxembourg, Poland, France, Ireland, and Germany. Some of these entities are also located outside the European Union and the European Economic Area ("EEA"), among others in the United States, the United Kingdom and Canada.

You agree that professional secrecy will be lifted for the benefit of the Platform you subscribed to and which uses the Mangopay Services to allow payments related to your activities on the Platform. You authorize sharing information with the Platform(s) you subscribed to so that the Platform(s) can perform certain activities that are in your interest, including helping you when you contact their support center, supporting refund requests, contributing to fraud investigations, and carrying out audits. The data concerned are your Identity Data as well as data related to Transactions and external payments to your external bank account(s) carried out through the use of Mangopay Services. We may also share other data such as technical data (e.g., User ID) or status of some of our processes.

You also authorize Mangopay to share your Identity Data and Supporting Documents, including copies of your identity documents and other information or documents used for CDD, with the Partner you

registered with and that needs this Identity Data and Supporting Documents for its compliance activities, such as the Partner's own CDD's obligations. By requesting the data to Mangopay, the Platform aims to limit the need for the Partner to request the same data or documents that are collected by Mangopay for the compliance obligations applicable to its own Platform you registered with.

Such disclosure may take place for the duration of the contract between Mangopay and the Partner and, following its termination, only to the extent necessary to complete ongoing processes, such as migrations. You may revoke your consent at any time.

9.2. Intellectual property

We retain all intellectual property titles and rights attached to the Mangopay Services we provide to you. None of these rights is transferred to you hereunder.

You undertake not to infringe the titles and rights held by Mangopay, including the "Mangopay" trademark and logo. You also undertake not to remove or modify any indication of the "Mangopay" trademark or any other intellectual property or property right appearing on any item supplied or made available by Mangopay.

9.3. Force majeure

We cannot be held liable or considered to be in default of these Terms and Conditions, in the event of non-performance of Mangopay Services, where the cause is related to a force majeure event as defined by applicable law.

9.4. Independence of the contractual provisions

If any one of the provisions of these Terms and Conditions is held to be null and void, it shall be deemed unwritten and shall not invalidate any of the other provisions. If one or more provisions of these Terms and Conditions become obsolete or are declared as such pursuant to a law, regulation or following a final decision delivered by a competent court, the other provisions shall retain their binding force and scope.

9.5. Non-assignability

You may not transfer or assign your rights and obligations under these Terms and Conditions to a third party.

9.6. Agreement on evidence

You acknowledge that all information relating to your use of Mangopay Services and held in our IT system in an unalterable, reliable and secure manner shall be deemed authentic until proven otherwise.

9.7. Non-waiver

The fact that you or we do not avail ourselves of any provision set out in these Terms and Conditions at a given time does not constitute a waiver of a right and does not prevent the exercise of that right or any other right at a later date.

9.8. Complaints and mediation

For any request relating to the use of Mangopay Services, we invite you to first contact the Platform's customer service department. For complaints related to the Mangopay Services or your Mangopay Account, you can contact our Complaints Department at the following email address: complaint@mangopay.com.

We will provide acknowledgement of receipt of your complaint within 10 business days of receiving your complaint.

You will receive a response as soon as possible and no later than fifteen (15) business days following Mangopay's receipt of the complaint. However, for reasons beyond its control, Mangopay may not be able to respond within this fifteen (15) day period.

In this case, we will provide you with a response specifying the reasons for this additional time. In any event, you will receive a final response no later than one (1) month i.e thirty (30) days following receipt of the complaint.

Therefore, when filling your complaint, please be sure to provide us with at least the following information:

- Name and surname;
- Contact details such as your email address and/or your mobile phone number;
- The platform on which you are using Mangopay's service;
- The context of your complaint: what happened, when did the incident or problem occur and under which circumstances;
- Any documentation that could support your complaint or be useful.

We inform you that the *Commission de Surveillance du Secteur Financier* (CSSF) has jurisdiction to settle, on an extrajudicial basis, disputes relating to the implementation of these Terms and Conditions. For more information on the CSSF and the conditions of such recourse, you can consult the CSSF website (<https://www.cssf.lu/en/customer-complaints/>). We draw your attention to the fact that the CSSF cannot be engaged if the request is clearly unfounded or abusive, if the dispute has been previously examined or is in the process of being examined by another ombudsman or by a court, if the application to the ombudsman is submitted more than one year after the written complaint you have made to us, or if the dispute does not fall within the ombudsman's field of competence. If you are a consumer, you may also submit your dispute on the European Commission's Online Dispute Resolution platform at <https://webgate.ec.europa.eu/odr/>. The use of mediation is an alternative mechanism that does not constitute a precondition for taking legal action.

9.9. Language

Except in the case of public order rules (which shall only apply to the strict extent of their purpose), these Terms and Conditions are concluded in English only and you agree that we will communicate

with you in English. Any translation of these Terms and Conditions is provided solely for your convenience and is not intended to modify the terms of these Terms and Conditions.

9.10. Applicable law and jurisdiction

These Terms and Conditions are subject to Luxembourg law, except where laws of public order (such as local consumer law) are intended to apply to the relationship that binds us.

In the event of a dispute between us, you accept the exclusive jurisdiction of the Luxembourg courts. However, if you are a consumer, you may either refer the matter to the court of your place of residence, or the court of the place of Mangopay's registered office, in accordance with Regulation No. 1215/2012 of 12 December 2012.

Specific Terms and Conditions for Mangopay Services in the event of Transfers of funds and/or Top-up

Version in force from 30 June, 2026

Where relevant to you, these Specific Terms and Conditions for Mangopay Services in the event of Transfers of funds and/or Top-up apply in addition to the above Terms and Conditions. Accordingly, all provisions of the main Terms and Conditions also apply to your use of the services described in these Specific Terms.

Section 1 – Transfer of funds

This section applies when you have the option (i) to use the funds available in your Mangopay Account to transfer funds to the Mangopay Account of another user of the Platform, and (ii) to receive on your Mangopay Account transfers of funds initiated from the Mangopay Account of another Platform user. This feature is referred to as a “**Transfer**” and is only available if the Partner or Mangopay has specified that this option is available to you. A Transfer constitutes a Payment Operation per the Definitions in Section 1 of the Terms and Conditions for Mangopay Payment Services.

Transfers are only available if your CDD has been successfully completed and if you hold a Mangopay Account.

1. Transferring funds from your Mangopay Account to another Mangopay Account

You may use the funds available in your Mangopay Account to make a payment to the Mangopay Account of another user of the Platform. Before initiating your payment, you must ensure that the available balance in your Mangopay Account is sufficient to cover the Transfer amount.

In order to effectuate a Transfer to the Mangopay Account of another Platform user, you must indicate the amount, the beneficiary, and any other information requested by the Partner. Your payment instruction is irrevocable once you have confirmed your Transfer on the Platform Interface, and will be deemed to be immediate in the absence of any indication to the contrary. We will carry out your instruction as soon as possible and will record the funds in the Mangopay Account of the user who is the beneficiary of the Transfer. We may refuse to carry out the Transfer if the instruction is incomplete or erroneous. We may refuse, block or suspend a Transfer from your Mangopay Account to another Mangopay Account if we suspect fraudulent or unlawful use of your Mangopay Account, if CDD requirements are not fulfilled or are no longer satisfied, a security breach of your Mangopay Account or for AML/CFT reasons, including but not limited to asset freezing measures, sanctions or restrictions imposed against you by an administrative authority or in relation to the context of the Transfer.

Disputing a Transfer initiated from your Mangopay Account – If you wish to dispute a payment made to the Mangopay Account of another Platform user that you have not authorised or which has been carried out incorrectly, we invite you to first contact the Partner's customer service department as soon as possible or to contact Mangopay's customer service department.

If you use the Mangopay Services for non-professional purposes, you have a period of thirteen (13) months following the debit of your Mangopay Account to dispute the Transfer. If you use the Mangopay Services as a professional, your dispute period is eight (8) weeks from the debit of your Mangopay Account. If we find that the unauthorised payment is due to fraud, we will return the transaction amount to you. However, any losses related to unauthorised payments will remain your responsibility if they result from fraudulent activity carried out by you, or in the event of your negligence regarding the security of and access to your Mangopay Account.

2. Receiving a Transfer on your Mangopay Account

You can receive funds on your Mangopay Account from other Platform users that hold a Mangopay Account through a Transfer. The funds received following a Transfer will be recorded in your Mangopay Account.

3. Refunding a received Transfer

If you wish to refund a Transfer you received on your Mangopay Account, you may request the total or partial cancellation of such Transfer received in your Account in accordance with this article. Cancellation of a Transfer will only be possible if the funds corresponding to the amount to be repaid are available in your Mangopay Account.

Section 2 – Funding your Mangopay Account (Top-up)

This section applies when you have the option to perform a Top-up of your Mangopay Account.

Depending on the integration of the Partner Platform, you may be able to perform a Top-up of your Mangopay Account. A **“Top-up”** means the funds that you transfer to your Mangopay Account using a Mangopay Payment Method or an External Payment Method. You can then use the funds to perform a Transfer to another Mangopay Account of a user of the Platform. A Top-up constitutes a Transaction as per the Definitions in Section 1 of the Terms and Conditions for Mangopay Payment Services.