RAUVA TERMS AND CONDITIONS

Contents

Section A – General Terms.

- **Introduction**. These terms and conditions (the "**Terms**") govern your use of Rauva.com and Rauva mobile application and any related services, features, content, or communications provided by Rauva Technology, Unipessoal Lda. (collectively, the "**Rauva App**"). Rauva is a technology services provider that offers you, through the Rauva App, an interface which seamlessly enables and aggregates your access to certain financial and business-related services of its partners, via APIs, to give to you a "one-shop" digital solution for starting and managing your business, while also offering you additional business-related tools (collectively, "**Services**").

  For the avoidance of doubt, **RAUVA IS NOT REGULATED BY ANY FINANCIAL SUPERVISORY AUTHORITY**, and it does not provide, by itself, any regulated services to the public. ALL SERVICES WHICH REQUIRE AN AUTHORISATION, LICENCE, REGISTRATION, OR CERTIFICATION ARE PROVIDED BY **THE PARTNERS OF RAUVA WHICH ARE DULY AUTHORISED, LICENSED, REGISTERED OR CERTIFIED BY THE RELEVANT COMPETENT PUBLIC OR PRIVATE AUTHORITY, AGENCY, OR BODY**. Please refer to "**Rauva's Partners**" and "**Partners' Services**" sections to check the full identification, regulatory status, or certifications, as well as the relevant terms and conditions of service of our partners.

- **Rauva's Partners**. Rauva is partnering up with other entities for the provision of certain services published on the Rauva App. At present, Rauva Partners are:
  - Payment Services Provider.
  - Legal Partners.
  - Accounting Partners.
  - Virtual Address Providers.

  Rauva may, at any time, add new partners to increase the scope of Third-Party Services in the Rauva App, replace existing Partners or cease its cooperation with any Partner or the availability of one or more Third-Party Services. Rauva will give you notice if and before

any such changes take place. Please refer to the "**Amendments**" section and "**Termination of Third-Party Services**" section.

- **Entire Agreement**. These Terms, together with the data protection agreement provided in Addendum 1 to these Terms ("**DPA**"), and, when applicable, for the Supercharged Plan, the Acceptance Terms, form an agreement ("**Agreement**") between Rauva Technology, Unipessoal Lda. ("**Rauva**"), with registered office at Rua Avenida Duque de Loulé, No. 12 1050-090, Lisbon, Portugal, with sole commercial registration and taxpayer number 516903519, and € 1.000,00 share capital, and legal or natural persons acting in their professional capacity who complete a user account registration and comply with the eligibility criteria ("**you**", or "**User**"). The legal documents forming the Agreement constitute the entire agreement between you and Rauva regarding the use of the Services, and supersede all prior and contemporaneous communications, agreements, and understandings, whether written or oral. Any legal document forming the Agreement, including these Terms may be modified by Rauva at any time as provided in the "**Amendments**" section below.
- **Valid and binding Agreement**. By signing up and accepting our Terms, DPA, Subscription Plans and Price List (and for Supercharged Plan, the Acceptance Terms), and thereafter by accessing or using the Services, you signify that you have read, understood, and agree to be bound by this Agreement. A pdf version of the legal documents forming the Agreement can be downloaded from our website.
- **Other contracts**. Notwithstanding "**Entire Agreement**" and "**Valid and binding Agreement**" sections, you acknowledge that other contractual documents will apply in the context of Third-Party Services publicised in the Rauva App, as described in the "**Third-Party Services**" section. Rauva's Partners' terms will apply to the relevant third-party services, and you must read, understand, and agree with them to be able to use such third-party services.
- **Language**. You agree that all communications shall be made in English or Portuguese. Rauva is not obligated to communicate in another language.
- **Services eligibility**. The Services are available to legal and natural persons acting in their professional capacity and within the scope of an economic activity (including, but not limited to, companies and independent professionals registered as such, business owners and independent professionals), whose location and registered office is in Portugal, and which would not qualify as consumers under any laws. In the case of natural persons, the Services are intended for use by persons who are at least 18 years old. Additional requirements are applicable to the Supercharged Plan, in the terms described in the Supercharged Plan Acceptance Agreement.
- **Account Registration**. In order to use the Services, you must create an account with Rauva and provide certain information about yourself. You agree to provide true, correct, complete and up-to-date information about yourself as prompted by the registration process, and to maintain and update your information to keep it true, correct, complete and up to date at all times. Please refer to **Privacy Notice**, available on our website (https://rauva.com/legal-pages), which details how your personal data is processed by Rauva. Additional requirements are applicable to the Supercharged Plan, in the terms described in the Supercharged Plan Acceptance Agreement.
- **Representations**. You represent and warrant to us that by registering in the Rauva website and/or app, and using the Rauva App:

- you are acting in your professional capacity and not for personal use;
- where you are a natural person, you are at least 18 years old and have the legal capacity to enter into a binding agreement;
- where you register a company, that you have powers to lawfully represent that company;
- all information provided by you is true, correct, complete and up to date.

Rauva may at any time request you to provide evidence that you comply with the criteria above.

- **User rights**. Subject to these Terms, Rauva grants you a limited, personal, non-exclusive, non-transferable, non-customizable, non-assignable, non-sublicensable and revocable right to use the Rauva App, solely for your internal business purposes. You may not modify, alter, or create derivative works based on our software, or reverse engineer, decompile, or disassemble our software in any way. You may not use the Rauva App for any other purpose or in any other manner without Rauva's prior written consent. Rauva retains all rights, title, and interest in and to the Rauva App, including any modifications or improvements performed therein, and all intellectual property rights therein. By using the Rauva App, you agree to respect the intellectual property rights of Rauva, and to refrain from any unauthorised use of the Rauva App or its content or materials.
- **Intellectual property**. All intellectual property rights in and to the Rauva mobile application, APIs and website, including but not limited to the app's design, user interface, text, graphics, logos, images, names, domain, other distinctive signs and any other content or materials, are exclusively owned by Rauva. "Rauva" is a registered trademark of Rauva. The Rauva App is protected by copyright and other intellectual property laws.

  If you choose to provide comments or feedback to Rauva in relation to the Services, you hereby grant to Rauva a worldwide, non-exclusive, royalty-free, transferable, sublicensable, perpetual and irrevocable licence to use and otherwise exploit such feedback for quality assessment, training, and promotion of Rauva's Services.

  For the purposes of this Agreement, intellectual property shall mean all patents (including supplementary protection certificates), rights to inventions (i.e., invention, technical development, improvement or innovation, whether or not patentable or capable of registration, and whether or not recorded in any medium), copyrights or related rights, trademarks, trade names and domain names, service marks, utility model rights, registered designs, design rights, rights in databases, rights in computer software, topography rights, rights in trade secrets, rights in get-up, goodwill and the right to sue for passing off, Confidential Information, know-how, trade or business names.
- **Service availability and disclaimer on warranties**. Subject to the "**Amendments**" section, Rauva may change, suspend or discontinue any of its Services, as well as modify its prices. THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT ANY WARRANTIES OF ANY KIND. RAUVA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE AVAILABILITY, ACCURACY, RELIABILITY,

COMPLETENESS, OR TIMELINESS OF THE SERVICES OR ANY THIRD-PARTY SERVICES ACCESSED OR USED THROUGH THE RAUVA APP. RAUVA DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, NOR IT GRANTS THAT IT WILL MEET YOUR EXPECTATIONS. To the fullest extent permitted under applicable law, Rauva disclaims any implied or statutory warranty.

- **Obligations of the User**. In addition to any other User obligations established in these Terms, you agree that:
    - You are solely responsible for the activity that occurs on your account, and you must keep your account login credentials (including, without limitation, your password) secure. You agree to use a strong password and keep it confidential;
    - You must notify Rauva immediately of any breach of security or unauthorised use of your account;
    - You must comply with the Terms and any applicable laws or regulations;
    - You must pay the subscription fee when due in the manner selected by you in Subscription Plans and Price List.
- **Suspension**. Rauva may, at any time, suspend your access and use of the Rauva App if:
    a. You breach any obligation applicable to you under these Terms and you fail to remedy such breach within a reasonable period granted by Rauva, when Rauva considers such breach as remediable; or
    b. You breach any obligation applicable to you under these Terms and such breach causes or its likely to cause serious harm to Rauva's app or website or Rauva considers that such breach cannot be remedied, in which case suspension may be determined with immediate effects.
- **Force Majeure**. Force Majeure means an incident beyond a person's reasonable control, including but not limited to industrial disturbances, lockouts, internet outages, systemic electrical, telecommunications, or utility failures, earthquake, storms, or other elements of nature or acts of God, blockages, embargoes, sanctions, civil unrest, riots, acts or orders of government, war or military hostilities, criminal acts of third parties that could not reasonably be prevented or minimised by that person, hosting (or similar) outages, denial of service other than for Rauva's breach (such as third party web services outages or denial of service), worms, bots, malware or cyber-attacks. In case of a force Majeure event, Rauva may suspend the services as set forth in the "**Suspension**" section.
- **Taxes.** You are solely responsible for the payment of taxes that arise from your use of the Services. Unless otherwise stated, all amounts referred to in these Terms and in Rauva App or website, including any fees, are stated on a tax exclusive basis.
- **Privacy.** Each Party shall comply with the applicable data protection laws. If you provide personal data other than your representatives' personal data to Rauva, including, without limitation, data from your customers and employees, Rauva will act as a data processor in relation to such personal data, in which case Rauva undertakes to process such data in accordance with the DPA.

- **Selection of Plans.** When creating a Rauva User Account, the User will automatically start on a free trial of the Charged plan. While using the trial version of the Rauva App, the client may select to begin the next 30 days on the free Starter plan.
- **Pricing and Subscription Plans**. The Rauva Price List applicable to each Subscription Plan shall be displayed and confirmed by the User in Rauva App before subscribing the selected plan or by any other document provided to the User by Rauva to this effect.
- **Non-refundable fees.** The price charged in respect of the Rauva App subscription plan selected by the User is non-refundable, even if the User cancels its Rauva User Account soon after the stipulated debit date, as a month started is a month paid.
- **Subscription Plans**. Rauva's App Subscription Plans are the following:
  - Starter Plan.
  - Charged Plan (the Starter Plan and the Charged Plan jointly referred to as the "**Rauva App Basic Plans**").
  - Supercharged Plan (available only upon prior assessment of Rauva).

Section B – Rauva App Plans

- **Starter Plan.** The Starter plan will involve no monthly subscription for the customer, within the respective set limits. If the limits are exceeded, the User will have to pay the corresponding fees. For further information, please refer to the pricing list available on Rauva's website.
- **Charged Plan.** The Charged Plan will increase the limits permitted to the User in terms of SEPA payments, invoices and virtual cards. It will also enable the User to access certain features that are unavailable in the Starter Plan. For further information, please refer to the pricing list available on Rauva's website.
- **Supercharged Plan.** Supercharged Plan is a combination of the Charged Plan, Virtual Address Services and the Accounting Services, governed specifically by Addendum 1 and Addendum 2 to the Supercharged Plan Acceptance Agreement, respectively. For this particular plan, Users have a 60-day notice period before termination and no free trial period is given. During this notice period, the User will be charged for two billing cycles based on the same price of the last billing before the termination notice. The user acknowledges that they cannot terminate the agreement without cause during the last three months of the tax year.

  24.1. Virtual Address Services: Under the Supercharged Plan, you may also choose to have access to Virtual Address Services, provided by Rauva's Partner, under a different payment plan (for more information, please refer to the pricing list available in Rauva's website). These are "virtual office" services, including the allocation of a registered address/office in Portugal and the reception and expedition of correspondence to the company's accountant. For more information, please refer to the terms and conditions of the Virtual Address Provider available in the Supercharged Preparatory Services Acceptance Agreement and the Supercharged Plan Acceptance Agreement.

  24.2. Legal Services: Under the Supercharged Plan, you may also choose to have access to our available Legal Partners, under a different payment plan (for more information, please refer to the pricing list available in Rauva's website). The Legal Services shall be invoiced directly by the Legal Partners to the User.

If the accounting services are terminated for any cause, regardless if terminated by the User or the Accounting Partner under the terms set in the Supercharged Agreement, the User will be downgraded to the Charge Plan within 60 (sixty) days upon the date of notice of termination of the accounting services.

- **Trial version.** The trial version of the Rauva App Charged Plan is free for a period of 30 days. The client will be able to use the limits allowed on the Charged plan during the trial. If the client exceeds these limits, they will pay the Additional Fees (as referenced in section 27 below) at the end of the trial period. The trial version can be cancelled at any time. While using the trial version of the Rauva App, the client may select to begin the next 30 days on the free Starter plan. At the end of the trial, if the client has the funds to pay for Charged and has not downgraded to Starter, the client will start the next month on the Charged plan.
- **First Payment.** The amount relating to the first payment owed for the use of the Rauva User Account, regarding both Rauva App Basic Plans and Additional Fees, will be debited automatically on the same day of the next month following the creation of the Rauva User Account. When the payment is respective to a month that does not allow for the debit in the aforementioned day, the debit in question will be carried out on the last day of that month.
- **Additional Fees.** Additional Fees pertain to all services provided by Rauva that exceed those described for each specific subscription plan, which include, but are not limited to, execution of SEPA Payments, the provision of physical or digital cards and the dispatching of Rauva Bills not foreseen in the respective subscription plans.
- **Subsequent Payments.** The amounts relating to all subsequent payments owed for the use of the Rauva User Account, regarding both Monthly Subscriptions and Additional Fees, shall be debited from the Rauva User Account, in full, every month and on the same day on which the Rauva User Account was created ("Original Billing Date"). When the payment is respective to a month that does not allow for the debit on the aforementioned day, the debit in question will be carried out on the last day of that month, and Subsequent Payments will be charged on the Original Billing Date. Subscription fees for Rauva Plans are charged in advance of the upcoming month, while Additional Fees are charged in arrears, for the previous month.
- **Insufficient Funds.** If at the stipulated billing day, the User does not have enough funds to pay for the amounts owed, relating to both the Monthly Subscription and Additional Fees, the User will be notified of the need of contributing sufficient funds to its Rauva User Account within one month.
- **Notifications.** The User will be notified by e-mail and by push notifications of the amounts owed before the billing date and immediately after the failure of payment of amounts owed. The User will receive such notifications until the account is credited with sufficient funds or until the Rauva User Account is terminated.
- **Rauva User Account Suspension.** If after one month of receiving the notification of Insufficient Funds, the Rauva User Account remains without sufficient funds to settle the respective amounts owed, the Rauva User Account will be immediately suspended. After one month of the Rauva User Account being suspended, it will be deactivated and follow Deactivation Data procedures.

- **Rauva Bills.** Rauva Bills will be accessible in the Plans section of the App on a monthly basis to the User after the respective Rauva User Account has been debited for all amounts owed.
- **Deactivation:** One month after the Rauva User Account has been suspended and remains in such a state, the Rauva User Account will be deactivated.
- **Term and termination**. The Agreement shall remain in effect until terminated by either party, in accordance with these Terms. Either party may terminate the Agreement at any time at its sole discretion, provided that all outstanding obligations and liabilities have been fulfilled. The Agreement may be terminated by sending an e-mail to support@rauva.com. On termination, you lose the right to access or use the Rauva App.
- **Termination of Third-Party Services**. Please note that upon termination of your Rauva User Account and removal of the Rauva App, you will no longer have access to any Third-Party Services through the App. The terms and conditions for the Third-Party Services may establish other provisions and / or procedures for termination of those Third-Party Services. You should consult the terms and conditions of the relevant Third-Party Services when wishing to terminate your use of the Rauva App.
- **Deactivation Data Procedures.** User Data will be held by Rauva for 60 days after deactivation of the Rauva User Account, before being permanently deleted. During these 60 days, Rauva will send the User notifications via e-mail on day 15, 30 and 45 from the date of Deactivation of the Rauva User Account, regarding User data right of retrieval. During these 60 days, should the User wish to retrieve such data, an e-mail to support@rauva.com must be sent. After this e-mail has been received by Rauva, the data in question will be sent to the User, via an encrypted e-mail, within an estimated period of 48 business hours.
- **Termination Data Procedures.** User data will be held by Rauva for 60 days after Termination before being permanently deleted. During these 60 days, Rauva will send the User notifications via e-mail on day 15, 30 and 45 from the date of Termination of the Rauva User Account, regarding User data right of retrieval. During these 60 days, should the User wish to retrieve such data, an e-mail to support@rauva.com must be sent. After this e-mail has been received by Rauva, the data in question will be sent to the User, via an encrypted e-mail, within an estimated period of 48 business hours.
- **Funds on Deactivation:** If upon Rauva User Account Deactivation the User has a positive balance, such funds will be debited by Rauva, to pay towards the amounts owed by the User to Rauva.

Section C - Partner's Services

- **Third-Party Services**. Partner's services are third-party services provided to you directly by our Partners through the Rauva App. Currently these services include virtual address services, payment services, legal services, and accounting services. Rauva may, however, establish new partnerships for adding new services at any time.
- **Exclusion of liability of Third-Party Services**. While providing the Third-Party Services, Rauva acts as a mere aggregator and intermediator platform which gathers and discloses to you such Third-Party's services. Other than as provided in these Terms, Rauva does not control, ensure, or assumes responsibility for any Third-Party Services, and you agree that Rauva will not be liable for any losses or damages that you may incur

as a result of your use of any Third-Party Services or the failure of a Partner to fulfil its obligations to you as provided for in the relevant Partner's terms and conditions. You should read the terms and conditions and privacy policy of any Third-Party Services that you access or use through the Rauva App.

- **Intellectual property of Third-Party Service Providers**. Trademarks and logos used in connection with the Third-Party Services are the trademarks of their respective owners.
- **Payment Services Provider**. All payment services are exclusively provided by Swan, a simplified joint-stock company (*société par actions simplifiée*) with a capital of €22,840.20, having its registered office at 95 avenue du président Wilson, 93108, Montreuil – RCS 853827103. Swan is an electronic money institution, approved under number 17328 by the *Autorité de Contrôle Prudentiel et de Résolution* (French Prudential Supervision and Resolution Authority or ACPR), with registered office at 4 place de Budapest, CS92459 - 75436 Paris, Cedex 09, France, and subject to the supervision of ACPR. You can check ACPR's list of authorised entities, here. Swan is registered with Banco de Portugal, under number 7893, to provide services in Portugal, pursuant to the rules on freedom to provide services. You can check Swan's status with Banco de Portugal, here.
- **Payment Services Provider TnC**. Swan offers you access to a payment account where your funds will be safeguarded, issuance of e-money and payment instruments, including cards and payment instructions, such as transfers and direct debit orders, and provides other services required to manage, deposit, or withdraw funds from the payment account and issue or cancel payment instruments. The provision and your use of the payment services is subject to Swan's terms and conditions ("**Swan's TnC**"), which you can find [here]. By accepting these Terms, you acknowledge having read, understood and accepted Swan's TnCs. FOR THE AVOIDANCE OF DOUBT, BY ACCEPTING SWAN'S TNC AND ANY OTHER RELEVANT LEGAL NOTICES OF SWAN, YOU ARE ENTERING INTO A DIRECT BINDING PAYMENT SERVICES FRAMEWORK CONTRACT WITH SWAN, AND SWAN IS EXCLUSIVELY RESPONSIBLE FOR THE PROVISION OF THE PAYMENT SERVICES TO YOU. Further, you should note that the payment services provided by Swan and Swan's TnC are governed by French law, as established in Swan's TnC.
- **Information on the payment account**. Swan's payment account is held with custodian bank, BNP Paribas. Swan will issue e-money against any deposits made into the payment account by you. Please note that a payment account is not a bank account. Please refer to Swan's explanation on how your funds are protected, here.
- **Rauva's support**. Without prejudice to Swan's TnC, you acknowledge and accept that, although Rauva is not a party to the payment services framework contract between you and Swan, Rauva may enable and have access to certain information and data (including personal data) related to the payment services of Swan, as required for the operation of the Rauva App. Rauva's access to any personal/payment data in this context is further subject to our Privacy Notice. In case of suspension, deactivation or termination of your use of the Services, for whatever reason, you acknowledge that you will cease to have access to the payment services through the Rauva App. Please refer to Swan's TnC for the procedures to follow in respect of the payment services in case of termination of your relationship with Rauva. Rauva's role in support of the payment services is further described below:

- **Card orders:** you may submit virtual or physical card orders to Swan through the Rauva App, and you consent that Swan informs Rauva whenever a physical card is dispatched to you.
- **Card payments and withdrawals:** all transactions, including withdrawals are authorised and executed by Swan. Please note that Swan will notify Rauva before final acceptance of any transaction, and, in case there has been an infringement to these Terms, Rauva may invalidate such transaction.
- **Issue of SEPA transfers:** you can submit SEPA transfer orders to Swan using online forms provided in the Rauva App. Please note that Swan will notify Rauva before the transaction is carried out, and, in case there has been an infringement to these Terms, Rauva may invalidate such transaction.
- **Issue of foreign currency transfers:** you can send and receive payments in foreign currencies with Swan, through the Rauva App. Please note that Swan will notify Rauva before final acceptance of any transaction, and, in case there has been an infringement to these Terms, Rauva may invalidate such transaction.
- **SEPA direct debits set-up:** you can set-up SEPA direct debit orders with Swan using online forms provided in the Rauva App. Please note that Swan will notify Rauva before the transaction is carried out, and, in case there has been an infringement to these Terms, Rauva may invalidate such transaction.
- **Loading the Swan Account:** you can load your payment card with Swan by using online forms provided in the Rauva App.
- **Transactions to and from the electronic money account:** you can instruct Swan to send or receive electronic money transfers from the electronic money account with Swan by using online forms provided in the Rauva App.
- **Reimbursement of the balance of the electronic money account:** you can instruct Swan to reimburse the balance of the electronic money account with Swan by using online forms provided in the Rauva App.
- **Internal Direct Debit Mandate:** you can set-up internal direct debit orders with Swan, where both creditor and beneficiary are Swan's customers, by using online forms provided in the Rauva App. The conditions applicable to Swan's internal direct debit scheme are described in Swan's TnC.
- **Complaints regarding payment transactions:** In case you have any complaint regarding Swan's payment services or in case of non-authorised or incorrect payment transactions you shall submit your complaint through the Rauva email support@rauva.com , which will forward your request to Swan.
- **Reporting on payment transactions:** the User will receive monthly periodic statements including a schedule of all payment transactions. These will be made available in the Rauva App.

- **Rauva's App connection to the Payment Services Provider**. Subject to your acceptance of Swan's TnC, Swan's Privacy Notice and Rauva's Privacy Notice, Rauva App connects you directly to Swan through API. Any personal and / or payment data populated into the online forms which are visible to you on the Rauva App's interface will be securely transmitted to Swan. Swan will execute all payment instructions and / or orders, in accordance with Swan's TnC.

- **Personal data and professional secrecy**. Please refer to Privacy Notice which details how your personal data is processed by Rauva. Information provided by you for the purposes of the provision of payment services by Swan is subject to professional secrecy.

Section D – Liability and Indemnities.

- **Exclusion of liability.** TO THE FULLEST EXTENT PERMITTED BY LAW (AND UNLESS OTHERWISE AGREED WITH YOU IN WRITING), RAUVA WILL NOT BE LIABLE IN CONNECTION WITH THE AGREEMENT FOR DAMAGES, INCLUDING LOST PROFITS OR LOST BUSINESS OPPORTUNITIES, OTHER THAN AS A RESULT OF ITS OWN WILFUL MISCONDUCT OR FRAUD. RAUVA WILL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES. IN ANY EVENT, RAUVA'S LIABILITY IN CONNECTION WITH THE AGREEMENT WILL NOT EXCEED AN AMOUNT CORRESPONDING TO THE TOTAL FEES PAID OR PAYABLE BY YOU TO RAUVA FOR THE SERVICES DURING THE PREVIOUS 12 MONTHS OR THE TERM OF THE AGREEMENT IF LESS THAN 12 MONTHS.
- **Indemnities**. To the extent permitted by applicable law, you shall defend, hold harmless and indemnify Rauva from and against any loss suffered or incurred by it arising out of or in connection with claims presented by any person (including a User or third-party) because of:
    - any data (including personal data) being wrongfully or unlawfully used or disclosed by you while using the Services;
    - information used by you, while using the Rauva App, infringes any intellectual property or other right (including privacy rights) of such person.
    - Any use which may pose risks to the integrity, security and/or availability of the App or of any dataset contained therein.

Section E – Miscellaneous.

- **Data Protection**. By accepting these Terms, you acknowledge having read, understood and accepted our Privacy Policy, accessible at any time on our website.
- **Amendments**. Rauva reserves the right to modify these Terms and any legal document forming the Agreement at any time. If the changes materially affect the rights or obligations of the user or of Rauva, changes will become effective after giving 1 (one) month prior notice by email to user. After that period, or if otherwise in the meantime accepted by the user, such modifications will become immediately effective. Your continued use of the Services after the effective date of any modifications will constitute your acceptance of the modified terms. If you do not agree with the modified terms, you must notify Rauva to terminate the Services, in accordance with the **"Deactivation, Term and Termination"** section.
- **Severability**. If any provision of the Agreement, or the application thereof to any party or circumstance, shall be held to be illegal, invalid or unenforceable (in whole or in part) for any reason, the remaining provisions hereof shall continue in full force and effect as if the Agreement had been executed with the illegal, invalid or unenforceable portion eliminated, so long as the Agreement as so modified continues to express, without

material change, the original intentions of the parties as to the subject matter of this Agreement and the deletion of such portion of this Agreement will not substantially impair the respective benefits or expectations of the parties of this Agreement.

- **No waiver**. No failure or delay by Rauva in exercising any right, power, or privilege under this Agreement shall operate as a waiver thereof, nor shall any single or partial exercise of any right, power, or privilege by Rauva preclude any other or further exercise thereof or the exercise of any other right, power, or privilege.
- **Assignment**. You may not assign or transfer the Agreement (or use of Services) to anyone without our consent. However, you agree that Rauva may assign the Agreement to its affiliates or to a third-party that buys it without your consent.
- **Subcontracting.** You acknowledge and accept that Rauva may use the services of third-party contractors, including data-enrichers, infrastructure and/or hosting environment provider(s) for the provisioning of the Services.
- **Survival of Terms**. The following terms shall survive termination of the Agreement:
  - Rauva's rights to use and disclose your feedback;
  - Exclusion of liability and Exclusion of liability of Third-Party Services sections;
  - Indemnities section;
  - Governing law and Jurisdiction sections;
  - Legal notices section;
  - Severability section;
  - Intellectual property sections;
  - Any amounts owed by either party prior to termination remain owed after termination.

Section F – Notices and communications.

- **Communications to the User**. Rauva may send you notices and communications through the Rauva App, and any other means elected by you, including push notifications, email, SMS, and phone. You may change the type and means of communication made by Rauva in Preferences.
- **Contact Rauva**. For general inquiries and help services, you may contact us through support@rauva.com.
- **Legal notices.** For legal notices or service of process, you may write to us at support@rauva.com. Please note that the only way to provide us legal notice is at the addresses provided in this Section.

Section G – Governing Law and Jurisdiction.

- **Governing law**. The Agreement is governed by and construed in accordance with Portuguese law.
- **Jurisdiction**. Any disputes arising out of or in connection with the Agreement shall be subject to the exclusive jurisdiction of the competent Judicial Courts of Lisbon.

ADDENDUM 1 - DATA PROCESSING AGREEMENT

This document sets out the Data Processing Agreement ("**DPA**") for the processing of personal data during the execution and after the termination of the Terms and Conditions of Use of RAUVA's Services ("**Agreement**"), as required by article 28, no. 3 of GDPR. Where, while performing RAUVA's Services ("Services") under the Agreement, RAUVA processes "personal data" or "personal information" under applicable data protection laws on behalf of the User as Controller, which are not personal to the User's representatives , RAUVA is qualified as a Processor (as defined below) and this DPA shall apply.

1. Definitions

1.1. In addition to the terms defined in the Agreement, in this DPA all the definitions set forth in article 4 of GDPR shall be adopted, namely the terms "**Personal Data**", "**Data Subjects**", "**Processing**", "**Personal Data Breach**", "**Pseudonymization**", "**Controller**" and "**Processor**".

1.2. In addition to the above, the following definitions shall be adopted:

"**Data Protection Law**"	means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, commonly known as the "**General Data Protection Regulation**" or "**GDPR**" as well as any other applicable national rule and legislation on the protection of personal data in the European Union or locally that is already in force or that will come into force during the term of this DPA, including any measure, guideline and opinion issued by the European data protection authorities or by the European Data Protection Board ("**EDPB**").
"**Persons in Charge of Data Processing**"	means the employees and any natural persons who, authorized by the Processor and/ or its sub-processors, if any, can process the Processed Data;
"**Platform**"	means the relevant web, online platform or other software service or application developed by RAUVA, and shall include any modifications, customizations and derivatives of the same;
"Processed Data"	all the personal data processed by the Processor on behalf of the Controller under the Services, as better defined in **Appendix I – Description of Processed Data**
"**Security Measures**"	means the security measures and any other obligations under the Data Protection Law for the purposes of guaranteeing the security and confidentiality of the Processed Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures, as well as procedures and activities to be performed in case of a personal data breach to prevent and reduce the adverse effects of the breach on the affected data subjects, in particular, those identified in **Appendix II – Security Measures**;
"**Sub-Processor**"	means the legal person, company or independent professional who, authorized by the Controller and engaged by the Processor, is allowed to carry out activities entailing the process of the Processed Data, as permitted under Data Protection Law and this DPA. Authorized sub-Processors are detailed in **Appendix III – General Authorization for Sub-processing**

2. Scope

2.1. RAUVA shall act as the Processor ("**Processor**") in relation to the processing of Processed Data on behalf of the User which is qualified as the Controller ("**Controller**"), exclusively for the purposes of executing the Agreement or as required by law, according to the terms and conditions of this DPA and of the Data Protection Law.

2.2. The type of personal data and processing activities to be handled by the Processor are described in Appendix I – Description of Processed Data. Any amendment to this list must be previously approved in writing by the User, and a copy of said updated list will be stored in the most updated version of this DPA.

2.3. In relation to any processing of Processed Data carried out by the Processor or by a Sub-processor, directly or through the respective Persons in Charge of Data Processing, for purposes other than those within the scope of this DPA and the Service engaged, and on the basis of different relationships with data subjects, the Processor or its subsequent Subcontractors shall not act as processors of the Controller in relation to the Processed Data, but as independent data controllers, or processors of entities other than the Controller, as the case may be.

3. Term

3.1. This DPA shall be effective from the Effective Date of the Agreement up to the end of the transitional period of 15 (fifteen) days granted after the termination of such Agreement or its related services.

3.2. During the transitional period the Controller will be able to delete, remove or transfer the Processed Data resulting from the Services. After such transitional period, the Processor will permanently delete all the Processed Data from the Platform and all

the existing copies, unless any applicable law requires storage of the Processed Data.

3.3. The Processor shall ensure that all Persons in Charge of Data Processing, its Sub-Processors, if any, and their Persons in Charge of Data Processing, comply with the obligations laid down in this DPA, as applicable, in the manner and in accordance with the timing indicated thereunder.

4. Obligations of the Controller

4.1. The Controller undertakes to:

4.1.1. Ensure that the collection and further processing of all Processed Data is done in a lawful manner;

4.1.2. Provide clear and timely written instructions to the Processor regarding the Processed Data;

4.1.3. Assist and cooperate, within a reasonable manner, with the Processor whenever required under the processing of the Processed Data, namely if it suspects of any data breach that could undermine the availability, integrity, privacy and/or security of the Processed Data;

4.1.4. Inform the Processor of any restriction required to the processing of any Processed Data, regardless if required by a Data Subject or instructed by a relevant data protection supervisory authority;

4.1.5. Keep the Processor up to date about the Processed Data or any other relevant information for its processing by the Processor or by its Sub-processors, namely about any notification or request for information from a relevant data supervisory authority.

5. Obligations of the Processor

5.1. The Processor undertakes to:

5.1.1. Process the Processed Data for the sole purpose of performing the Services, subject to the limits and in the manner provided for by the Agreement between Controller and Processor for the provision of such Services, this DPA and the Data Protection Law, and in strict compliance with the written instructions given by the Controller, and shall immediately inform in writing the Controller should it deem that any of the aforesaid instructions is in breach of the Data Protection Law or, in general, of any applicable law;

5.1.2. Process exclusively the Processed Data that is strictly necessary for correctly and fully performing the Service or meeting the obligations provided for by Data Protection Law or other applicable law;

5.1.3. Process the Processed Data lawfully, fairly and in full compliance with the principles applicable to data processing, with the requirements laid down by the Data Protection Law and the information on the processing of the Processed Data provided to the relevant data subjects by the Controller;

5.1.4. Assist and cooperate, within a reasonable manner, with the Controller whenever required under the processing of the Processed Data, namely if it suspects of any data breach that could undermine the availability, integrity, privacy and/or security of the Processed Data;

5.1.5. Inform the Controller of any restriction required to the processing of any Processed Data, regardless if required by a Data Subject or instructed by a relevant data protection supervisory authority, unless if prohibited by law;

5.1.6. Keep the Controller up to date about the Processed Data or any other relevant information, namely about any notification or request for information from a relevant data supervisory authority;

5.1.7. Cooperate with and assist the Controller in the response to any notifications from a supervisory authority in connection with the Processed Data, including, without limitation, the provision of supporting documentation to be submitted to the relevant supervisory authority as evidence that the Processor is legally bound by the terms of this DPA;

5.1.8. Provide to the Controller, upon request, all the information in its possession or control referring to the processing of the Processed Data under this DPA, namely for the latter to assess whether such processing is carried out in accordance with this DPA.

5.1.9. Disclose the information reasonably required by the Controller for the performance of privacy impact assessments concerning the processing activities and cooperate on the implementation of mitigation actions agreed by the Parties to address privacy risks which may have been identified.

5.1.10. Permit, provide information for and cooperate with the Controller regarding audits, including any inspections conducted by the Controller or another auditor mandated by the Controller.

5.2. With regard to the Persons in Charge of Data Processing, the Processor further undertakes to:

5.2.1. guarantee that the Persons in Charge of Data Processing can access and process only the Processed Data that is strictly necessary for correctly and fully performing the Services or meeting the legal requirements, in each case, subject to the limits and in accordance with the conditions of this DPA, the principal agreement between Controller and Processor for the provision of the Services and the Data Protection Law;

5.2.2. guarantee that the Persons in Charge of Data Processing are subject to confidentiality undertakings or professional or statutory obligations of confidentiality;

5.2.3. consent that the Processed Data are processed only by the Persons in Charge of Data Processing who

(i) on the basis of their experience, capabilities and training, can ensure compliance with the Data Protection Law and need to access the data for the purpose of performing the Service;

(ii) attended periodically training courses on the obligations prescribed by the Data Protection Law.

5.2.4. adopt any physical, technical and organizational measure aimed at enabling:

5.2.4.1. each Person in Charge of Data Processing to access exclusively the Processed Data that he/she is authorized to process, by taking into account the activity that he/she is required to carry out to perform the Service;

5.2.4.2. any processing of the Processed Data that is in breach of the DPA and/or the Data Protection Law to be promptly identified and reported to the Controller; and

5.2.4.3. upon termination of the Services and, with respect to each Person in Charge of Data Processing, upon termination of the appointment of such Person in Charge of Data Processing, including, without limitation, when the employment or collaboration relationship between the Person in Charge of Data Processing and the relevant Processor or Sub-Processor is terminated, ensure total confidentiality, availability and integrity of the Processed Data.

6. Sub-processors

6.1. Regarding the Processed Data, the Processor undertakes to engage and work only with sub-processors to which the Controller did not reasonably oppose in writing to said collaboration.

6.2. Sub-Processors identified in Appendix III – General Authorization for Sub-processing are hereby authorized by the Controller to process Processed Data provided that said Sub-Processor:

6.2.1. has committed to confidentiality obligations and enters into a written agreement providing the same data protection obligations as set out in this DPA and other obligations as may be required by the Controller under the instructions of the Processor.

6.2.2. acts exclusively on behalf of the Controller or the Processor instructions;

6.2.3. provides adequate guarantees with reference to the technical and organizational measures adopted for the processing of the Processed Data, including, without limitation, ensuring that the Sub-Processor immediately ceases the processing of the Processed Data should such guarantee be no longer available.

6.3. In case of any intended changes concerning the addition or replacement of any of the Sub-Processors identified in Appendix III] – General Authorization for Sub-processing, the Processor undertakes to notify the Controller, giving the Controller the opportunity to reasonable object to such change within 30 (thirty) days counting from said notification. If the Controller notifies the Processor of any objection to the proposed appointment, the Parties shall work together to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed sub-processor. Costs related to his change, if any, will be borne by the Controller.

6.4. The Processor shall correctly and completely adopt all the Security Measures in compliance with the Data Protection Law and this DPA.

7. Security measures

7.1. Without limiting the foregoing, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing of the Processed Data, and the likelihood and severity of the risk to the rights and freedoms of natural persons, Processor shall implement appropriate technical and organizational measures to ensure a level of security that is proportionate to the risk associated with the processing of the Processed Data, including, without limitation, the measures provided for by Article 32, paragraph 1 of the GDPR, and in particularly including, but not limited to, the measures identified in Appendix II – Security Measures.

8. Processed Data Breach

8.1. In the event of a Personal Data Breach or any other incidents that may compromise the security of the Processed Data (such as loss, damage or destruction of the Processed Data in an electronic or hard copy format, third party unauthorized access to the Processed Data or any other breach of the Processed Data) including, without limitation, any breach or other incident resulting from the conduct of, if any, the Processor's Sub-Processors and/or its Persons in Charge of Data Processing, the Processor shall:

8.1.1. immediately and without undue delay inform the Controller by email which shall include at least information regarding the type and description of the Personal Data Breach, identification of the Processed Data and of the Data Subjects affected and potential consequences of said breach, as well as any remedies already put in place (if any). Where and insofar is not possible to provide all the relevant information at the same time, the information may be provided in phases without undue delay;

8.1.2. in collaboration with the Controller, adopt immediately, and in any case without undue delay, all necessary measures to minimize any type of risk that may derive for the Data Subjects from such breach or incident, remedy such breach or incident and mitigate any possible adverse effect.

8.2. The Controller is fully liable, whenever required, for notifying such Personal Data Breach to the relevant data protection supervisory authority and to the Data Subjects, if applicable.

9. Data Subjects' Rights

9.1. The Controller shall ensure that the rights granted to the Data Subjects by the Data Protection Law are effectively executed. The Processor undertakes to notify the Controller in writing within 5 (five) Business Days of receipt of any request made in this respect by the Data Subjects.

9.2. The Processor shall cooperate with the Controller to ensure that all requests by Data Subjects exercising their rights under the Data Protection Law (including, without limitation, the right to object to the processing and the right to the Processed Data portability) are complied with within the time period and in accordance with all other requirements provided for by the Data Protection Law.

10. Audits

10.1. The Processor acknowledges and accepts that the Controller may assess the organizational, technical and security measures adopted by the Processor in the processing of the Processed Data by way of audit no more frequent than annually (unless if in the context of a Processed Data Breach). To this end, upon no less than ten (10) Business Days' prior written notice (except if there is a reasonable urgency of the Controller for an earlier prior notice), the Controller will be entitled to access, directly or through any authorized third-party, the premises, computers and any other IT system/file of the Processor and its

Sub-Processors, if, at its sole discretion, Controller deems it necessary to verify compliance by the Processor and/or one of its Sub-Processors with this DPA and the Data Protection Law or to ascertain any breach of the Processed Data.

11. Transfers of Processed Data outside the EEA

11.1. The Processor will carry out the processing only in the European Economic Area ("**EEA**") and agrees not to transfer the Processed Data outside the EEA, without the Controller's prior written consent or unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

11.2. When the Processor transfers personal data with the Controller's consent, as provided for in clause 11.1 above, such transfer is made in accordance with the provided for in Chapter V of the GDPR and with the instructions given by the Controller in relation to such transfer.

11.3. In case the Processor transfers data outside the EEA, the Processor, acting as data exporter, shall ensure that whenever there is no adequacy decision in place as set forth in article 45 of the GDPR, it will execute additional, including but not limited to, the Standard Contractual Clauses as timely approved by the European Commission or any other Standard Contractual clauses approved by any EU data protection supervisory authority.

11.4. If any of the Sub-Processors engaged by the Processor is based out of the EEA or transfers Processed Data to any country out of the EEA, the Processor will execute with such Sub-Processor the equivalent Standard Contractual Clauses model as required by law.

Appendix I - Description of Processed Data

Personal Data collected	Brief description of the processing activities
NIF	Rauva Customers will send Invoices, Invoice Receipts, Credit Notes and Debit Notes to their Customers, for this process we need to know and record the Name, NIF, Email and Address of the The Clients of our Customers and the The Suppliers of our Customers.
Email	
Address	
Name	

Appendix II – Security Measures

Processor shall maintain and enforce various policies, standards and processes designed to secure personal data and other data to which Processor employees are provided access, and updates such policies, standards, and processes from time to time consistent with industry standards. Without prejudice to the rules contained within Clause 6 (Security Measures) of the Data Processing Agreement, the Processor shall implement appropriate technical and organizational measures to ensure a level of security adequate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of the data subjects. These measures shall ensure full compliance with Article 32 of the GDPR. Following is a description of some of the core technical and organizational security measures implemented by Processor as of the date of signature:

1. General Security Procedures

1.1 Processor shall be responsible for establishing and maintaining an information security program that is designed to: (i) protect the security and confidentiality of Personal Data; (ii) protect against anticipated threats or hazards to the security or integrity of the Personal Data; (iii) protect against unauthorized access to or use of the Personal Data; (iv) ensure the proper disposal of Personal Data, as further defined herein; and, (v) ensure that all employees and subcontractors of Processor, if any, comply with all of the foregoing. Processor will designate an individual to be responsible for the information security program. Such individual shall respond to Controller inquiries regarding computer security and to be responsible for notifying Controller-designated contact(s) if a breach or an incident occurs, as further described herein.

1.2 Processor shall conduct formal privacy and security awareness training for all personnel and contractors as soon as reasonably practicable after the time of hiring and/or prior to being appointed to work on Personal Data and annually recertified thereafter. Documentation of security awareness training shall be retained by Processor, confirming that this training and subsequent annual recertification process have been completed.

1.3 Controller shall have the right to review an overview of Processor's information security program prior to the commencement of Service and annually thereafter upon Controller request.

1.4 In the event of any apparent or actual theft, unauthorized use or disclosure of any Personal Data, Processor shall immediately commence all reasonable efforts to investigate and correct the causes and remediate the results thereof, and within 2 business days following confirmation of any such event, provide Controller notice thereof, and such further information and assistance as may be reasonably requested. Upon Controller's request, remediation actions and reasonable assurance of resolution of discovered issues shall be provided to Controller.

1.5 Processor will not transmit any unencrypted Personal Data over the internet or any unsecured network, and will not store any Personal Data on any mobile computing device, such as a laptop computer, USB drive or portable data device, except where there is a business necessity and then only if the mobile computing device is protected by industry-standard encryption software. Processor shall encrypt Personal Data in transit into and out of the Services over public networks using industry standard protocols.

2. Network and Communications Security

2.1 All Processor connectivity to Controller computing systems and/or networks and all attempts at same shall be only through Controller's security gateways/firewalls and only through Controller-approved security procedures.

2.2 Processor will not access, and will endeavor its best efforts to prevent unauthorized persons or entities to access,Controller computing systems and/or networks without Controller's express written authorization and any such actual or attempted access shall be consistent with any such authorization.

2.3 Processor will take appropriate measures to ensure that Processor's systems connecting to Controller's systems and anything provided to Controller through such systems does not contain any computer code, programs, mechanisms or programming devices designed to, or that would enable, the disruption, modification, deletion, damage, deactivation, disabling, harm or otherwise be an impediment, in any manner, to the operation of Controller's systems.

2.4 Processor will maintain technical and organizational measures for data protection including: (i) firewalls and threat detections systems to identify malicious connection attempts, to block spam, viruses and unauthorized intrusion; (ii) physical networking technology designed to resist attacks by malicious users or malicious code; and (iii) encrypted data in transit over public networks using industry standard protocols.

3. Personal Data Handling Procedures

3.1 Disposal of Personal Data on paper shall be done in a secure manner, to include shredders or secure shredding bins within Processor space from which Personal Data is handled or accessed ("Controller Work Area"). Shredding must take place within the Controller Work Area before disposal or transit outside of the Controller Work Area or be performed offsite by a reputable third party under contract with Processor.

3.2 Erasure of Information and Destruction of Electronic Storage Media. All electronic storage media containing Personal Data must be wiped or degaussed for physical destruction or disposal, in a manner meeting forensic industry standards such as the NIST SP800-88 Guidelines for Media Sanitization, prior to departing Controller Work Area(s), with the exception of encrypted Personal Data residing on portable media for the express purpose of providing service to the Controller. Processor shall maintain commercially reasonable documented evidence of data erasure and destruction for infrastructure level resources. This evidence must be available for review at the request of Controller.

3.3 Processor shall maintain authorization and authentication technologies and processes to ensure that only authorized persons access Personal Data, including: (i) granting access rights on the basis of the need-to-know-principle; (ii) reviewing and maintaining records of employees who have been authorized or who can grant, alter or cancel authorized access to systems; (iii) requiring personalized, individual access accounts to use passwords that meet complexity, length and duration requirements; (iv) storing passwords in a manner that makes them undecipherable if used incorrectly or recovered in isolation; (v) encrypting, logging and auditing all access sessions to systems containing Personal Data; and (vi) instructing employees on safe administration methods when computers may be unattended such as use of password protected screen savers and session time limits.

3.4 Processor shall maintain logical controls to segregate Personal Data from other data, including the data of other Clients.

3.5 Processor shall maintain measures to provide for separate processing of data for different purposes including: (i) provisioning Controller within its own application-level security domain, which creates logical separation and isolation of security principles between Clients; and (ii) isolating test or development environments from live or production environments.

4. Physical Security

4.1 All backup and archival media containing Personal Data must be contained in secure, environmentally controlled storage areas owned, operated, or contracted for by Processor. All backup and archival media containing Personal Data must be encrypted.

4.2 Technical and organizational measures to control access to data center premises and facilities are in place and include: (i) staffed reception desks or security officers to restrict access to identified, authorized individuals; (ii) visitor screening on arrival to verify identity; (iii) all access doors, including equipment cages, secured with automatic door locking systems with access control systems that record and retain access histories; (iv) monitoring and recording of all areas using CCTV digital camera coverage, motion detecting alarm systems and detailed surveillance and audit logs; (v) intruder alarms present on all external emergency doors with one-way internal exit doors; and (vi) segregation of shipping and receiving areas with equipment checks upon arrival.

4.3 Processor shall maintain measures to protect against accidental destruction or loss of Personal Data including: (i) fire detection and suppression, including a multi-zoned, dry-pipe, double-interlock, pre-action fire suppression system and a Very Early Smoke Detection and Alarm (VESDA); (ii) redundant on-site electricity generators with adequate supply of generator fuel and contracts with multiple fuel providers; (iii) heating, ventilation, and air conditioning (HVAC) systems that provide stable airflow, temperature and humidity, with minimum N+1 redundancy for all major equipment and N+2 redundancy for chillers and thermal energy storage; and (iv) physical systems used for the storage and transport of data utilizing fault tolerant designs with multiple levels of redundancy.

5. Security Testing

5.1 During the performance of services under the Agreement, Processor shall engage periodically a Third-Party ("Testing Company") to perform penetration and vulnerability testing ("Security Tests") with respect to Processor's systems containing and/or storing Personal Data.

5.2 The objective of such Security Tests shall be to identify design and/or functionality issues in applications or infrastructure of the Processor systems containing and/or storing Personal Data, which could expose Controller's assets to risks from malicious activities. Security Tests shall probe for weaknesses in applications, network perimeters or other infrastructure elements as well as weaknesses in process or technical countermeasures relating to the Processor systems containing and/or storing Personal Data that could be exploited by a malicious party.

5.3 Security Tests shall identify, at a minimum, the following security vulnerabilities: invalidated or un-sanitized input; broken or excessive access controls; broken authentication and session management; cross-site scripting (XSS) flaws; buffer overflows; injection flaws; improper error handling; insecure storage; common denial of service vulnerabilities; insecure or inconsistent configuration management; improper use of SSL/TLS; proper use of encryption; and anti-virus reliability and testing.

5.4 Within a reasonable period after the Security Test has been performed, Processor shall notify Controller in writing of any critical security issues that were revealed during such Security Test which have not been remediated. To the extent that critical security issues were revealed during a particular Security Test, Processor shall subsequently engage, at its own expense, the Testing Company to perform an additional Security Test to ensure resolution of identified security issues. Results thereof shall be made available to the Controller upon request.

6. Security Audit

Processor, and all subcontracted entities (as appropriate) will perform whenever convenient detailed security and vulnerability tests and assessments against all systems processing Personal Data conducted by independent third-party security experts that include a thorough code analysis and a comprehensive security audit, and shall perform regular (i.e. at least bi-annually) penetration tests (for exploits including, but not limited to, XSS, SQL injection, access controls, and CSRF) against any Internet-facing systems used in connection with the Services. Processor further agrees to perform regular risk assessments of the physical and logical security measures and safeguards it maintains applicable to its protection of Personal Data. Processor will provide Controller, upon request, a summary report of such tests and assessments, including a description of any significant (i.e. moderate or greater) risks identified and an overview of the remediation effort(s) undertaken to address such risks, and attest to Controller the date of the most recent security and vulnerability assessment at Controller reasonable request.

7. Anonymisation and Pseudonymisation of personal data

7.1 When possible, the Processor should ensure that data is anonymised or pseudonymised before data processing operations.

7.2 When pseudonymising data, the key for reverting the process should be protected and stored in an adequate manner and according to industry standards.

7.3 Anonymisation should be preferred to pseudonymisation.

7.4 The Processor should guarantee the anonymisation is not reversible, in accordance with the technological state of the art.

8. Other technical and organizational measures

8.1 A Data Protection Officer should be appointed when the applicable legislation or good practices requires it.

8.2 When available for the Processor's industry, the Processor should acquire/adhere to Codes of Conduct and/or independent Certification regarding the processing of Personal Data and in accordance with the GDPR.

8.3 The Processor should keep itself updated of any developments to legislation, case-law or opinions from supervisory authorities regarding subjects that are relevant for the provision of services and inform the Controller if it considers that any of the above may have an impact on the services the Processor provides.

Appendix III – General Authorization for Sub-processing

Sub-Processor	**Purpose**	**Entity Country**	**Appropriate safeguards** *(Only applicable to transfers of data outside the EEA)*	**Onward Transfers** *(Y/N)*
Amazon AWS	Data storage for Rauva Technology	Spain	NA	NA
Invoicexpress	Sending of invoices	Portugal	NA	NA