GENERAL TERMS AND CONDITIONS

Last updated: 2 November 2026

These General Terms and Conditions (hereinafter the "Terms") constitute a legally binding contract ("Contract") governing the provision of services by Reskyt Online SL (hereinafter, the "MANUFACTURER") to any contracting individual and/or company (hereinafter, the "CUSTOMER"), pursuant to specific agreements entered into under special terms and conditions. These General Terms and Conditions shall apply to all services offered by the MANUFACTURER, unless expressly agreed otherwise in writing in the specific terms and conditions.

Please read these Terms carefully, as they contain important information about your rights, remedies, and obligations.

1. NATURE OF THE RELATIONSHIP

The relationship between the CUSTOMER and the MANUFACTURER is strictly commercial in nature. There is no employment, agency, partnership, or representation relationship between the parties, nor between the personnel of one party and those of the other. Each party shall assume its own tax, labor, and social security obligations in accordance with applicable law.

2. GENERAL OBLIGATIONS OF THE CUSTOMER

i. **Cooperation and provision of information:**
   - Provide the MANUFACTURER, in a truthful, complete, and timely manner, with all the information, materials, credentials, and technical or commercial documentation required for the performance of the service.
   - Keep the information provided up to date, including legal URLs (privacy policy, terms of use, etc.), as well as contact information and access to external platforms linked to the service.

ii. **Content and regulatory compliance:**
   - Ensure that all content, trademarks, text, images, or any other material provided to the MANUFACTURER does not infringe on the rights of third parties or violate applicable laws, including regulations on intellectual property, data protection, advertising, consumer protection, or competition.
   - Ensure that content published or distributed through the platform or contracted service complies with the policies and terms of use of third parties, such as the App Store, Google Play, or other technology platforms.
   - Assume responsibility for the legal consequences arising from any unlawful, inaccurate, or inappropriate content that the CUSTOMER directly or indirectly incorporates into the service provided.

iii. **Security and technical management:**
   - Have the technical accounts required to provide the service (for example, developer accounts with Apple or Google, access to Analytics or third-party tools) and provide the MANUFACTURER with the necessary access when required.
   - Ensure that its own systems, networks, or websites meet the minimum performance and compatibility requirements established by the MANUFACTURER to enable proper technical integration.

iv. **Proper use of the service:**
   - Use the contracted service in accordance with its intended purpose and terms and conditions, without manipulating, altering, duplicating, or distributing its functionality, technical components, or documentation without express authorization.

- Refrain from taking any action that could affect the stability, security, or reputation of the platform, the MANUFACTURER, or third parties.

v. **Financial obligations:**
   - Pay the agreed-upon fees on time, within the deadlines set forth in the specific terms and conditions.
   - Accept any surcharges, penalties, or service interruptions that may result from delays or nonpayment, in accordance with the provisions of these General Terms and Conditions and/or the specific terms and conditions.

vi. **Data protection:**
   - In cases where the CUSTOMER acts as the data controller for personal data related to the service, it must ensure compliance with applicable data protection regulations (GDPR, LOPDGDD, or others) and provide the MANUFACTURER with the legal texts and terms and conditions required for the proper use of such data in the provision of the service.
   - Sign, when applicable, the corresponding data processing agreement with the MANUFACTURER.

3. GENERAL OBLIGATIONS OF THE MANUFACTURER

i. **Service provision:**
   - Provide access to the platform and the features included in the contracted service, as defined in the specific terms and conditions.
   - Take reasonable measures to ensure the availability, stability, and proper functioning of the platform, except in cases of force majeure or incidents attributable to third parties beyond its control.

ii. **Technical support:**
   - Provide technical and functional support to the CUSTOMER through the designated channels during regular business hours.
   - Address and resolve, within a reasonable timeframe, any issues reported by the CUSTOMER in accordance with the established priority levels.

iii. **Security and confidentiality:**
   - Implement appropriate technical and organizational measures to protect the integrity, availability, and confidentiality of the CUSTOMER's data, in accordance with the sensitivity level of such data.
   - Ensure the confidentiality of the information provided by the CUSTOMER and not disclose or use it for any purpose other than those necessary for the performance of the contract.

iv. **Regulatory compliance:**
   - Comply with applicable laws in the course of providing its services, particularly with regard to data protection, intellectual property rights, and consumer protection regulations.
   - Facilitate, where applicable, the CUSTOMER’s signing of the necessary data processing agreements in compliance with the GDPR.

4. AUTHORIZATION TO USE INFORMATION

The CUSTOMER authorizes the MANUFACTURER to use the logos, images, and testimonials for marketing and promotional activities.

5. PUBLISHING ON THIRD-PARTY STORES (APP STORE AND GOOGLE PLAY)

The publication of the app on third-party platforms such as the App Store and Google Play (the “Third-Party Platforms”) is subject to the terms, conditions, and policies of those platforms. The MANUFACTURER does not guarantee that the app will be approved by the Third-Party Platforms.

If the application is not approved during the review process, or is subsequently removed due to content violations or other reasons attributable to the CUSTOMER, the MANUFACTURER shall not be liable for any delays or damages that may result.

The CUSTOMER is responsible for notifying the MANUFACTURER in writing of any changes to the URL of its privacy policy or other links required by Third-Party Platforms. Failure to provide such notification may result in the rejection or removal of the application, without any liability on the part of the MANUFACTURER.

The time required to resolve issues related to the approval or removal of the application by Third-Party Platforms is beyond the MANUFACTURER's control; the MANUFACTURER will cooperate in resolving these issues to the greatest extent possible but does not guarantee specific timeframes.

6. ANNUAL PRICE REVIEW (CPI) AND NON-REIMBURSEMENT

The annual price set forth in the specific terms and conditions may be adjusted by the MANUFACTURER at the beginning of each annual renewal period, applying the positive change in the general Consumer Price Index (CPI) published by the National Institute of Statistics (INE) for the previous fiscal year, using as a reference the latest official figure published in December of the year prior to renewal. The adjustment will be applied automatically unless otherwise agreed and will not be considered a substantial contractual modification, but rather an economic adjustment intended to maintain the real value of the service.

Under no circumstances—including cases in which the application is not approved or is removed from Third-Party Platforms—will there be a full or partial refund of the amount paid by the CUSTOMER.

7. TERM, RENEWAL, AND CANCELLATION

The minimum term for individual contracts is 1 year.

The CUSTOMER must provide written notice of its intention not to renew the contract at least 2 months prior to the annual renewal date. If such notice is not received within the established timeframe, the contract will be automatically extended for successive 1-year periods under the same terms and conditions.

The CUSTOMER may notify the MANUFACTURER of its intention not to renew the contract at any time. However, such notice will not take effect until the end of the contract period, and under no circumstances will it give rise to a refund, either full or partial, of the amount paid. Early termination will be valid only if there are justifiable grounds in accordance with the provisions of the General Terms and Conditions.

The CUSTOMER acknowledges that the MANUFACTURER may terminate this contract for reasons not attributable to it and due to force majeure, in accordance with the provisions of Reskyt's General Terms of Service.

8. SUSPENSION OF SERVICE AND TERMINATION OF THIS AGREEMENT

i. **Service suspension:**

   If the CUSTOMER fails to pay any invoice within one month of its due date, the MANUFACTURER shall have the right to suspend the provision of services until the outstanding debt is paid in full. The CUSTOMER will be notified in advance of such suspension.

   The suspension of service shall not relieve the CUSTOMER of its payment obligation nor shall it constitute grounds for termination of the contract, unless the conditions set forth in Section 8.2 are met.

ii. **Termination of the contract:**

   The agreement shall be deemed terminated for the following reasons:

   - Delays in paying fees or bills that exceed 3 months.

- Inclusion of content that is illegal, criminal, racist, xenophobic, incites terrorism, or violates human rights, as well as content that is defamatory, pornographic, misleading, or fraudulent to its recipients, or that in any way violates applicable laws or regulations or infringes upon the rights of the MANUFACTURER, distributors, or third parties.
- The MANUFACTURER may terminate this contract for reasons not attributable to it and due to force majeure, such as the removal of the product by Google Play or the App Store in the case of apps, or by other partners essential to the operation of the service provided by Reskyt.
- Termination of this agreement for any of the reasons mentioned above shall not entitle either party to any compensation.

9. SUPPORT AND AVAILABILITY

The MANUFACTURER agrees to provide support and customer service to the CUSTOMER during current business hours through the designated communication channels, such as email, telephone, or videoconference, as appropriate. Updated information on available hours and channels may be provided upon the CUSTOMER's request.

i. **Incident management:**

Requests and issues will be handled by the technical team according to priority criteria, with the goal of minimizing the impact on the CUSTOMER's operations and ensuring service continuity. To that end, two categories are established:

- Normal incidents: Those that do not result in a critical service interruption or compromise data security. They are handled during regular business hours, with response times appropriate to their nature.
- Critical incidents: Those that involve a total or partial service interruption, or that may affect the integrity, availability, or confidentiality of data. These incidents are prioritized for immediate attention, regardless of the time of day, through the alert system and continuous monitoring.

ii. **Business continuity:**

The technical environment that supports the MANUFACTURER's services is hosted on a highly available cloud infrastructure, with systems that actively monitor it 24/7. Any critical anomaly will be automatically reported to the technical staff on duty, who will take the necessary steps to ensure that service is restored as quickly as possible.

iii. **Scope of support:**

The support provided includes:

- Answering questions about the use and configuration of the contracted services.
- Technical support for changes or updates to the platform.
- Management of functional and technical issues related to the proper operation of the service.

The following are not included within the scope of support:

- Customized services not expressly contracted.
- Interference with systems, platforms, or data outside the MANUFACTURER's infrastructure.
- Direct support for the CUSTOMER's end users.

10. INFRASTRUCTURE AND SUBCONTRACTING

All services are provided using infrastructure hosted in secure data centers, currently provided by Amazon Web Services (AWS) in the European Union. The CUSTOMER expressly authorizes the subcontracting of technical services and infrastructure to the extent that it does not affect the confidentiality or scope of the contracted service. The subprocessors that process personal data on behalf of the CUSTOMER, and the conditions for engaging them, are governed by clause 11.

11. DATA PROTECTION POLICY

The personal data of the parties who enter into and sign this contract will be processed by both parties for the sole purpose of managing its performance and complying with the legal obligations arising therefrom. This data will be retained for as long as a contractual relationship exists between the parties and, thereafter, will be blocked for the periods required by law, with appropriate technical and organizational measures adopted to ensure, where applicable, the pseudonymization or permanent deletion of such data. No transfer of data to third parties is anticipated, except where required by law or in cases where it is necessary to engage service providers acting as Data Processors, duly authorized by each of the parties.

The parties and signatories are hereby informed that they may exercise their rights of access, rectification, erasure, objection, restriction of processing, and data portability, in accordance with the provisions of applicable regulations, by submitting a written request accompanied by a valid form of identification to the addresses listed in this contract. Likewise, they may file a complaint with the Spanish Data Protection Agency (www.aepd.es) if they believe their rights have been violated. For any questions regarding the processing of personal data, the Data Protection Officer of RESKYT ONLINE S.L. is available at dpo@reskyt.com.

In the event that the provision of the contracted services involves the processing by RESKYT ONLINE S.L. of personal data for which the CUSTOMER is the DATA CONTROLLER, such processing shall be carried out in accordance with the provisions of Article 28 of Regulation (EU) 2016/679, as well as the provisions of Organic Law 3/2018, with RESKYT ONLINE S.L. acting for this purpose as the DATA PROCESSOR.

The engagement will have the same duration as the main service contract. The following sets forth the terms and conditions governing the rights and obligations of both parties with respect to data protection, including the MANUFACTURER's obligations as a DATA PROCESSOR:

Specifications for the App or Platform Development Service

i. **Description:**

Processing of data generated by the devices of users who download and use the CUSTOMER's app for the purpose of:

- Managing push notifications.
- Providing technical and functional support to the CUSTOMER.
- Offering advanced features based on the configuration and the selected module: segmentation, customer loyalty, database creation, statistics, and integration with the CUSTOMER's CMS (Content Management System).

ii. **Categories of data subjects:**

Users who download and use the CUSTOMER's app.

iii. **Types of data processed:**

- Installation identifier and push notification token.
- Operating system, device model and App version.
- Geolocation data (subject to the user's consent).
- Connection data (IP address and user agent) in technical logs, which are retained for ninety (90) days, and in the App's statistics.
- Language, country, zone and dates of access to the app.
- Notifications sent and opened, their status in the App inbox (read or dismissed) and delivery errors.
- Browsing statistics within the App.
- Only if the CUSTOMER activates the User Journal module and the user consents: purchase events (products, amounts, order and searches).

- Only if the CUSTOMER activates them: App usage and error data collected by Firebase Analytics, Firebase Crashlytics and New Relic.
- User identification data: first name, last name, email address, mailing address, and phone number. This data will only be processed in cases where the CUSTOMER has activated specific features that require it, such as loyalty programs, advanced segmentation, or synchronization with its content management system (CMS).

iv. **Hosting:**

The personal data processed through the platform is hosted on servers provided by Amazon Web Services (AWS), located in data centers within the European Economic Area (EEA), thereby ensuring compliance with applicable data protection regulations. In addition to AWS, the following act as subprocessors: Apple and Google, to deliver push notifications; Anthropic, for the AI assistant in the admin panel; and GitHub, to build and publish the App. If the CUSTOMER activates those features, Cloudflare, for videos; New Relic, for App monitoring; and Google, for Firebase Analytics and Firebase Crashlytics, are also involved. The PROCESSOR shall inform the CUSTOMER of any addition or replacement before it takes place, so that the CUSTOMER may object.

v. **Retention period:**

At the CUSTOMER's request, the CUSTOMER's app data is deleted from the platform 30 days after the contract is terminated.

Obligations of the MANUFACTURER as DATA PROCESSOR

i. Process the data solely in accordance with the CUSTOMER's documented instructions. If the PROCESSOR considers that an instruction infringes data protection regulations, it shall immediately inform the CUSTOMER.

ii. Ensure that individuals authorized to process personal data have agreed to maintain confidentiality.

iii. Adopt appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including data protection by design and by default (Article 25 of the GDPR).

iv. Subcontracting: The CUSTOMER expressly authorizes the MANUFACTURER to engage Amazon Web Services, Inc. (AWS) as a subprocessor, exclusively for the hosting and processing of personal data on the cloud services used by the Reskyt platform, as well as the other subprocessors listed in the “Hosting” section of the Specifications. AWS provides its services from data centers located in the European Union (Ireland) and complies with the provisions of the GDPR regarding data security and protection. The DATA PROCESSOR shall ensure that AWS and the other subprocessors assume the same obligations set forth in this contract. Any subsequent change or addition of new subprocessors shall require the prior authorization—whether specific or general—of the CUSTOMER.

v. The PROCESSOR must, whenever possible and taking into account the nature of the processing, establish the technical and organizational measures necessary to assist the CONTROLLER in fulfilling its obligation to respond to requests regarding the data subject’s rights. If the DATA PROCESSOR receives a request to exercise these rights, it must notify the DATA CONTROLLER immediately and in no case later than the next business day following the day the request was received, along with any other information that may be relevant to resolving the request.

vi. Report any breach of personal data security without undue delay so that the CUSTOMER may be made aware of it and take measures to remedy the situation and mitigate its effects.

vii. Work with the CUSTOMER to conduct impact assessments and prior consultations with the supervisory authority when necessary.

viii. Provide the CUSTOMER with the information necessary to demonstrate compliance with its obligations, and allow and assist in the conduct of audits or inspections by the CUSTOMER or an authorized auditor.

ix. The CONTROLLER authorizes the PROCESSOR to carry out international data transfers provided that the PROCESSOR can demonstrate that the data transfer is based on adequacy decisions adopted by the EU Commission (Article 45 of the GDPR), on appropriate safeguards for data protection (Article 46 of the GDPR), or on one of the exceptions for specific situations (Article 49 of the GDPR). The DATA PROCESSOR shall be solely responsible for demonstrating that the data transfer provides the adequate or appropriate safeguards permitted by the GDPR and shall provide the DATA CONTROLLER with sufficient information to demonstrate that such safeguards are in place, or the means to obtain a copy of them or confirmation that they have been provided.

x. Coordination between data processors: Where the CUSTOMER orders push notifications to be sent through the MANUFACTURER's API from a third-party platform it has contracted directly (for example, CONNECTIF), the CUSTOMER authorizes and acknowledges the coordinated involvement of the MANUFACTURER and that platform, which may communicate with each other and exchange the personal data strictly necessary for the proper provision of the services, in particular for the management and sending of push notifications through the CONTROLLER's mobile application. Such communications shall be carried out exclusively for the purposes authorized by the CONTROLLER and in accordance with this contract, and each processor shall ensure compliance with the obligations incumbent upon it under Article 28 of the GDPR.

Obligations and Rights of the DATA CONTROLLER

i. The DATA CONTROLLER guarantees that the data provided to the DATA PROCESSOR has been lawfully obtained and that it is adequate, relevant, and limited to the purposes of the processing.

ii. The CONTROLLER shall provide the PROCESSOR with all the information necessary to perform the services covered by the agreement.

iii. The CONTROLLER advises the PROCESSOR that, if the PROCESSOR independently determines the purposes and means of the processing, it will be considered the controller and will be subject to compliance with the applicable provisions of current regulations in that capacity.

Security Measures

The DATA PROCESSOR undertakes to implement, at all stages of the App's development, deployment, and maintenance, appropriate technical and organizational measures to ensure that the processing of personal data is carried out in accordance with the principles of the GDPR, particularly those of data minimization, purpose limitation, confidentiality, integrity, and security. These measures will take into account the state of the art, the costs of implementation, the nature of the data, the context and purposes of the processing, as well as the risks to the rights and freedoms of individuals.

Among other things, the following specific measures will be implemented:

i. **Data minimization and pseudonymization:**
   - Data collection is limited to what is strictly necessary for each feature of the App.
   - Use of pseudonymization techniques or the replacement of personal identifiers when it is not essential to retain the direct identity.
   - Avoid collecting unnecessary information by using closed-ended forms and avoiding open-ended fields whenever possible.

ii. **Logical separation of environments and data:**
   - Isolation between development, testing, and production environments, with no use of real data in test environments unless it has been anonymized.
   - Segregated storage with restricted access for records containing personal identifiers.
   - Differentiated data management by functionality or project.

iii. **Restricted and controlled access:**
- A role-based access control (RBAC) model, based on the principle of least privilege.
- Traceability of access through logging and periodic audits.
- Records must be retained for at least two years for access to special-category data.

iv. **Privacy-focused default settings:**
- Any feature that involves the processing of non-essential data (e.g., geolocation) will be disabled by default and will require explicit activation by the user or the DATA CONTROLLER.
- Implementation of the "privacy by default" principle, configuring the system to provide the highest possible level of privacy from the moment of initial installation.

v. **Additional security measures:**
- Access control through robust authentication.
- Encryption of communications and, where applicable, of data at rest.
- Activity monitoring and incident alerts.
- Regular software updates and the application of security patches.
- Periodic technical tests to check for vulnerabilities.

vi. **Resilience, continuity, and verification:**
- Mechanisms for restoring data availability and access in the event of physical or technical incidents.
- Automatic backups and recovery policies.

vii. **Ongoing evaluation and cooperation:**
- Collaboration with the DATA CONTROLLER to conduct data protection impact assessments (DPIAs), when appropriate.
- Analysis and reporting to the DATA CONTROLLER of emerging risks that may affect data security.

Disposition of Data Upon Termination of the Contract

Upon termination, at the CUSTOMER's choice, the PROCESSOR shall return the personal data to the CUSTOMER in a structured, commonly used format or delete it, together with any copies, within thirty (30) days of the termination of the contract, unless retention is required by law.

12. CONFIDENTIALITY

The parties agree to maintain the strictest confidentiality with respect to all information exchanged that is of a confidential nature. This obligation shall remain in effect even after the termination of the contract. Disclosure to third parties shall require the prior written consent of the affected party.

13. LIMITATION OF LIABILITY

The MANUFACTURER shall not be liable for:

i. Issues caused by third-party services (Google Play, App Store, AWS, etc.).

ii. Content provided by the CUSTOMER.

iii. Loss of profits or indirect business interruptions.

In any case, the MANUFACTURER's maximum liability shall be limited to the annual amount paid by the CUSTOMER. The exclusion in point i does not extend to the providers that the PROCESSOR uses to process personal data on behalf of the CUSTOMER, for which it is liable in accordance with Article 28.4 of the GDPR.

14. INTELLECTUAL PROPERTY

All rights to the source code, designs, tools, and developments of the Reskyt platform belong exclusively to the MANUFACTURER. The CUSTOMER acquires only a limited and non-exclusive right of use, under the terms defined in the specific terms and conditions.

15. AMENDMENTS

Any amendment to these General Terms and Conditions must be made in writing and shall be notified to the CUSTOMER with reasonable advance notice. In the event of any discrepancy, the specific terms and conditions agreed upon shall prevail over the provisions set forth herein.

16. APPLICABLE JURISDICTION

The parties agree that this document shall be governed by and interpreted in accordance with Spanish law. For any controversy or dispute that may arise in connection with the interpretation, performance, or validity of this document, the parties expressly submit to the jurisdiction of the courts of the city of Barcelona, expressly waiving any other jurisdiction to which they may be entitled.