GENERAL TERMS AND CONDITIONS

Bootyn.com digital content provider platform

Effective: April 7, 2026 | Version 1.4

Detailed Table of Contents

1. Introductory provisions

1.1 Website Operator and subject of the agreement

These General Terms and Conditions (hereinafter: "GTC") govern the conditions of use of the digital content provider platform operating under the domain name Bootyn.com (hereinafter: "Website", "Platform" or "Service") and define the legal relationship between the Service Provider and Users. The Website is operated by SPONDEX LTD, a private company limited by shares incorporated under the laws of the Republic of Cyprus, with company registration number HE 490894. The company's registered office is: Voukourestiou 25, NEPTUNE HOUSE, 1st floor, Flat/Office 11, Zakaki, 3045 Limassol, Cyprus. The company is represented by Charalampos Lafazanis, Director.

SPONDEX LTD operates in accordance with Cypriot company law (the Companies Law, Cap. 113) and relevant European Union legislation, with particular regard to the General Data Protection Regulation (GDPR), the Digital Services Act (Regulation (EU) 2022/2065), directives on digital content (Directive (EU) 2019/770) and consumer protection regulations. The Platform's primary activity is the intermediation of adult-oriented, age-restricted digital content on a marketplace model, where the Platform provides online marketplace services between independent content providers and buyers.

1.2 Acceptance and scope of the GTC

By starting to use the Website, completing the registration process, or using any service, the User expressly accepts all provisions of these GTC and acknowledges them as binding. Platform services cannot be used without accepting the GTC. These GTC constitute an electronically concluded agreement between the Service Provider and the User, which is not filed on paper but is electronically recorded and archived in the Service Provider's IT system, making it retrievable and accessible at any time.

The scope of the GTC extends to all functions and services of the Platform, as well as all legal relationships arising between the Service Provider and the User in connection with the use of the Platform. This includes browsing, registration, content viewing, token purchases, subscriptions, content provider activities, and all other activities performed on the Platform.

1.3 Modification of the GTC

The Service Provider reserves the right to unilaterally modify these GTC at any time to reflect technological developments, legislative changes, business model improvements, or other justified circumstances. The modified GTC shall enter into force on the date of publication on the Platform, except where the modification contains substantial changes to Users' rights or obligations, in which case the Service Provider shall provide at least fifteen (15) days' notice before the effective date.

The Service Provider shall notify registered Users of modifications via email and through prominent notifications appearing on the Platform. Continued use of the Platform following modifications constitutes express acceptance of the modified GTC. If the User does not accept the modifications, they are entitled to terminate the agreement with immediate effect and delete their user account.

1.4 Definitions

For the purposes of these GTC, the following terms shall have the following meanings:

- "User" means any natural person who registers on, browses, or uses the Platform's services in any way, regardless of whether they use free or paid services.
- "Content Provider" or "Model" means a User with special permissions who publishes digital content for sale through the Platform and may receive compensation for it. Content Providers operate as independent contractors, are not employees of the Service Provider, and conduct their activities under a separate Content Creator Agreement.
- "Buyer" means a User who purchases tokens, subscribes, or otherwise spends money on the Platform to access content.
- "Content" means any digital data, information, image, video, audio material, text, live stream, or other intellectual creation that Users or Content Providers publish, share, or make available on the Platform.
- "Token" means the Platform's virtual payment instrument that enables access to certain services and exclusive content. Tokens do not qualify as money, securities, electronic money, or cryptocurrency, and can only be used within the Platform.

- "Marketplace Model" means a business structure in which the Platform provides a digital marketplace, acting as an intermediary between content providers and buyers, enabling them to sell and purchase digital content.
- "DSA" means Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act).

1.5 Platform operating model

The Bootyn.com platform operates as a digital marketplace service connecting content providers (models) and buyers. The Platform applies a marketplace model in which it acts as an intermediary between parties. The Service Provider provides the technical infrastructure, payment system, moderation, and customer service, for which it charges a commission or platform usage fee.

The legal nature of access to digital content is not a transfer of ownership but the provision of usage rights in the form of a limited, personal, non-exclusive license for a specified period or under specified conditions. The time of service performance is the moment of successful payment and technical opening of access to the content. In accordance with European Union consumer protection directives, the right of withdrawal for digital content expires upon commencement of performance, provided the buyer has expressly consented to this.

2. Eligibility and age requirements

2.1 Age of majority requirement

The Platform and all its services are available exclusively to adults. To use the Platform, the User must have reached eighteen (18) years of age, or, if the laws of their place of residence or domicile prescribe a higher age limit (such as nineteen (19) years in U.S. states like Alabama or Nebraska, or twenty-one (21) years in Mississippi or Puerto Rico), they must have reached that higher age. The Platform provides access to adult-oriented, age-restricted digital content uploaded by independent content providers and is available exclusively to users who have reached the applicable age of majority.

By registering and using the Platform, the User expressly declares and warrants that they have reached the above age limit, have full legal capacity, and are entitled to enter into binding contracts. The Service Provider accepts no responsibility if a User makes false statements about their age, provides false data, or otherwise misleads the Service Provider regarding their age.

2.2 Protection of minors

The Service Provider is committed to protecting minors and applies zero tolerance to all content and activities that affect or endanger minors.

The Platform applies strict technical and organizational measures to ensure that minors cannot access services and content. Users are required to provide real and accurate data and to declare during registration that they have reached the applicable age of majority in their country.

The Platform makes all reasonable efforts to exclude minors; however, ultimate responsibility lies with the user. If a user provides false age data or circumvents the system in any way, the Platform accepts no responsibility for this.

It is strictly prohibited on the Platform to publish, share, or distribute any content that depicts minors in a sexual or erotic context, aims to sexualize or encourage the sexualization of minors, contains adult content imitating minors, or could be harmful to minors in any way. It is also prohibited to publish content that targets or is aimed at minors, or that constitutes or is suspected of constituting child sexual abuse material.

If the Service Provider becomes aware that abuse involving minors has occurred or is suspected, it will immediately take the following measures: immediate removal and preservation of the objectionable content as evidence; immediate and permanent deletion of the affected User's account; reporting to the competent law enforcement authorities and to the National Center for Missing & Exploited Children (NCMEC) where applicable; full cooperation in official investigations; and transfer of all necessary data and information to investigating authorities.

2.3 Legal capacity and legal restrictions

In addition to having reached the applicable age of majority, full legal capacity is required to use the Platform. By registering and using the Platform, the User expressly declares and warrants that they have full legal capacity, are not under guardianship, supported decision-making, or other measures restricting or excluding legal capacity, are entitled to enter into binding contracts, are not subject to legal restrictions that would prevent use of the Platform, are not listed on international sanctions lists or other restrictive registers, and have not been permanently banned from the Platform previously.

The Service Provider reserves the right to refuse or terminate access for persons who do not meet the above requirements or who are reasonably suspected of having made false statements regarding their legal capacity.

2.4 Regional eligibility and geo-blocking

Although the Platform operates as a global service, in certain countries or regions, services may be limited or completely unavailable due to local laws, international sanctions, business considerations, or technical reasons. The Service Provider may apply geographic access restrictions (geo-blocking) to ensure that Platform use complies with applicable local and international laws.

It is the User's responsibility to ensure that use of the Platform does not violate the laws of their residence, domicile, or place where the service is used. The use of VPN, proxy, or other technology to circumvent geographic restrictions is strictly prohibited and constitutes a serious violation of the GTC, resulting in immediate account deletion. The Service Provider accepts no responsibility for legal consequences arising from unauthorized or illegal use of the Platform by the User.

2.5 Age verification procedure

To protect minors and ensure legal compliance, the Service Provider operates a comprehensive age verification system using the Shufti Pro artificial intelligence-based identity verification platform. Age verification is mandatory for all Users during registration and before using certain services.

During the age verification process, the User must present an official government-issued photo ID to the Shufti Pro system, which automatically verifies the document's authenticity, reads and verifies the date of birth, and uses biometric facial recognition technology to compare the photo on the document with a live selfie taken by the User. The entire verification process is automated, occurs without human intervention, and ensures compliance with data protection regulations.

2.6 18 U.S.C. § 2257 record-keeping compliance statement

The Service Provider is committed to full compliance with United States federal record-keeping requirements applicable to producers and certain service providers of sexually explicit content under 18 U.S.C. § 2257 and 28 C.F.R. Part 75.

All content depicting actual sexually explicit conduct made available through the Platform is subject to the following requirements:

- Each Content Provider, as the primary producer of their own content, is responsible for collecting, maintaining, and making available the records required under 18 U.S.C. § 2257 and 28 C.F.R. Part 75 for all performers depicted in their content. By accepting the Content Creator Agreement, Content Providers expressly acknowledge their status as producers under these provisions.
- As a secondary producer where applicable, the Service Provider maintains records demonstrating that, for each piece of content, the depicted performers were over the age of eighteen (18) at the time of production, verified through Shufti Pro government-issued ID checks and signed performer release documentation submitted by the Content Provider.
- Records required under 18 U.S.C. § 2257 are maintained by the designated Custodian of Records and are available for inspection during normal business hours at the address set forth in the 18 U.S.C. §§ 2257 and 2257A Compliance Declaration.

Custodian of Records:

The contact details of the designated Custodian of Records are published in a separate 18 U.S.C. §§ 2257 and 2257A Compliance Declaration accessible from the footer of the Platform. The Custodian of Records is appointed in accordance with 28 C.F.R. § 75.6 and maintains all required documentation for the statutory retention period.

Content Providers warrant that all records required under 18 U.S.C. § 2257 and any equivalent local legislation in their jurisdiction have been collected and are kept in their direct custody as primary producer. Failure to comply with these record-keeping obligations constitutes a material breach of the Content Creator Agreement and these GTC.

3. User accounts and registration

3.1 Creating a user account

Creating a user account is required for full use of the Platform and is available exclusively to natural persons. Legal entities, businesses, or organizations may not create accounts on the Platform. Registration is fundamentally free, but certain services and features are subject to fees.

During registration, the User must provide real, accurate, and up-to-date information. Required data includes a valid email address to which the User has exclusive access, a unique username between three and twenty characters that may not contain obscene, offensive, or copyrighted expressions, and a secure password of at least eight characters containing lowercase and uppercase letters, numbers, and special characters. Additionally, the date of birth must be provided for age verification, as well as country and region to determine service availability.

A natural person may create and maintain only one user account. Creating and using multiple accounts is strictly prohibited, regardless of whether they are registered with the same or different email addresses. Creating multiple accounts to circumvent the system or for abuse purposes will result in immediate and permanent deletion of all related accounts and permanent banning of the User from the Platform.

3.2 User authentication and permissions

Access to certain Platform functions and services requires enhanced identity verification, known as Know Your Customer (KYC) procedures. This particularly applies to becoming a Content Provider (Model), conducting financial transactions, and accessing premium services.

The identity verification process is entirely performed by the Shufti Pro AI-based platform, which uses state-of-the-art artificial intelligence and machine learning technologies for secure and reliable identification. The Shufti Pro system automatically verifies the authenticity of submitted documents against a database of official documents from more than two hundred countries, detects forged or modified documents, and uses biometric facial recognition technology to compare the photo on the document with a live video or selfie taken by the User.

During the authentication process, the User must submit a valid government-issued photo ID (identity card, passport, or driver’s license), take a live selfie or short video according to Shufti Pro instructions, and for Content Providers, submit additional documents such as proof of address and tax information. The complete verification process typically takes only a few minutes, and the User receives real-time notification of the result.

3.3 User account security

User account security is fundamental to the proper functioning of the Platform and the protection of Users. Each User bears full responsibility for their account security and all activities performed with it. The User must take all reasonable measures to protect their account, including using a strong, unique password, changing the password regularly at least every ninety days, keeping the password

confidential and never sharing it with third parties, and immediately changing the password if account compromise is suspected.

The Service Provider strongly recommends and may require the use of two-factor authentication (2FA) for certain services, which significantly increases account security. Two-factor authentication can be set up as SMS-based codes, authenticator apps, or biometric identification. The User must regularly monitor their account activity and immediately notify the Service Provider at legal@bootyn.com if any suspicious activity or unauthorized access is detected.

3.4 Account suspension and termination

The Service Provider reserves the right to suspend or permanently delete accounts that violate these GTC, engage in abusive activity, or participate in illegal conduct, at its sole discretion, with or without prior notice. Serious violations resulting in immediate and permanent account deletion include particularly violation of rules regarding the protection of minors, publication of illegal or prohibited content, use of false identity or identity theft, attacks or attempted attacks on the Platform's technical infrastructure, fraudulent payment activity or money laundering, repeated or serious copyright infringement, and extortion, threats, harassment, or violent behavior against other Users.

For less serious violations, the Service Provider applies a graduated sanction system that provides the User with an opportunity to correct their behavior. For the first violation, a written warning is sent detailing the problematic behavior and its consequences. On the second occasion, a 24- to 72-hour temporary suspension follows. For a third violation, a 7- to 30-day suspension may be applied. For a fourth or subsequent violation, the account is permanently deleted.

In accordance with Article 17 of the DSA, where the Service Provider imposes a content restriction or account-level sanction, the affected User shall receive a clear and specific Statement of Reasons setting out the factual and legal grounds for the decision and the available redress mechanisms, including the internal complaint-handling system referred to in Article 20 of the DSA and out-of-court dispute settlement under Article 21 of the DSA.

3.5 User categories and permission levels

The Platform distinguishes between different user categories with different permissions and features. Standard Users have basic browsing and interaction capabilities, can view public content, purchase tokens, and subscribe to Content Providers' exclusive content. Premium Users have all Standard permissions, plus access to expanded interaction options, special search and filter functions, and discounted token packages.

Content Providers (Models) have a special status that allows them to publish and sell exclusive content, generate revenue through the Platform, configure custom subscription models and token-based access, view detailed analytics and statistics, and use marketing tools to grow their follower base. Obtaining Content Provider status requires successful Shufti Pro identity verification, provision of valid tax and banking information, acceptance of the Content Creator Agreement, and approval by the Service Provider.

3.6 Communication on the Platform

The Platform provides a built-in messaging system for direct communication between Users, which may be used exclusively for interactions within the Platform framework. To prevent circumvention of the Platform and protect Users from off-platform abuse, it is prohibited to share personal contact information, including real names, email addresses, phone numbers, physical addresses, or social media profiles. It is also prohibited to encourage circumvention of the Platform, attempt to redirect to external payment platforms or services, send spam or unsolicited promotional messages, harass, threaten or intimidate, and organize or call for illegal activities.

The Service Provider reserves the right to apply automated filtering and human moderation of messages to prevent violations, on the legal basis of legitimate interest in fraud prevention, anti-circumvention, and User protection (GDPR Article 6(1)(f)). Violation of communication rules may result in warnings, temporary or permanent suspension of communication privileges, and in serious cases, account deletion.

4. Identity verification and Shufti Pro

4.1 Verification obligation

To guarantee the security and reliability of the Platform and ensure legal compliance, all Users and Content Providers (Models) must undergo the identity verification process. This verification is mandatory for completing registration, obtaining Content Provider status, conducting financial transactions, and accessing certain premium services.

The primary purpose of identity verification is to ensure that all Users register with their real identity, that everyone has reached the required age, to prevent fraud and abuse, to comply with anti-money laundering regulations, and to protect the Platform community from fake profiles and malicious actors.

4.2 Application of the Shufti Pro system

The Service Provider uses the Shufti Pro AI-based identity verification platform as its exclusive technology partner for all identification processes. Shufti Pro uses state-of-the-art artificial intelligence and machine learning technologies capable of performing the complete verification process in real-time without human intervention while guaranteeing maximum data security and GDPR compliance.

Shufti Pro system capabilities include recognition and verification of official documents from more than two hundred countries, advanced document authentication technologies to detect forgeries, biometric facial recognition and liveness detection, automatic data extraction and validation, and instant result reporting and risk assessment.

4.3 Steps in the verification process

The verification process takes place entirely online through the User's device and typically takes only a few minutes. In the first step, the User uploads or photographs their official document. Shufti Pro automatically recognizes the document type and country of origin, verifying its validity and authenticity. The system examines more than thirty security features, including holograms, watermarks, microprinting, and other security characteristics.

In the second step, the User takes a live selfie or short video according to Shufti Pro instructions. The system's biometric facial recognition algorithm compares the live capture with the photo on the document while performing liveness detection to ensure it is a real person and not a photo or video. In the third step, Shufti Pro automatically reads and verifies the data on the document, including name, date of birth, and other relevant information.

4.4 Data security during verification

The Shufti Pro system applies the highest data security standards. All data is encrypted during transmission and storage, biometric data is immediately deleted after verification is complete, and only the result is retained. Shufti Pro complies with GDPR, PCI DSS, and other international data protection standards, undergoes regular security audits, and holds ISO 27001 certification.

The Service Provider stores only the verification result provided by Shufti Pro and age confirmation, not actual document images or biometric data. This ensures that Users' personal data receives maximum protection while the Platform meets all legal requirements.

4.5 Consequences of refusing verification

If a User refuses Shufti Pro identity verification or the verification concludes with an unsuccessful result, certain consequences must be expected. Without verification, the User cannot become a Content Provider (Model), cannot conduct financial transactions on the Platform, cannot access certain premium services, and can only use the Platform with limited functionality.

If verification reveals that the User has not reached the required age, attempted to use false or forged documents, or attempted to register with another person's identity, their account will be immediately and permanently deleted, and the Service Provider reserves the right to take legal action and notify the competent authorities.

5. Content rules

5.1 User content and restrictions

The uploading User or Content Provider (Model) bears full legal and moral responsibility for all content published on the Platform. By publishing content, the User expressly declares and warrants that the content is their own intellectual creation or they have all necessary rights, permissions, and authorizations to publish it, all persons appearing in the content are adults and have expressly consented to display and distribution, the content does not infringe third parties' copyrights,

trademarks, personality rights, or other intellectual property rights, and the content complies with all applicable local, national, and international laws.

The User further warrants that the published content is real and not misleading, does not contain viruses, malicious code, or other harmful elements, complies with the Platform's community guidelines and quality expectations, and is not intended to circumvent the Platform's business model or payment system. Content Providers further warrant that all 18 U.S.C. § 2257 records and any equivalent local performer documentation have been collected and are maintained as set out in Section 2.6 above.

5.2 Prohibited content

It is strictly prohibited to publish any content on the Platform that violates the law, infringes third party rights, or violates the Platform's community standards. Prohibited content includes but is not limited to:

sexual or erotic content depicting, targeting, or imitating minors, regardless of whether it is real or artificially generated material; real footage depicting violence, torture, death, serious bodily injury, or animal cruelty; hate speech, discrimination, harassment, or intimidation against any person or group based on race, ethnicity, religion, gender, sexual orientation, disability, or other protected characteristic; revenge porn, non-consensual intimate recordings, or any content published without the express consent of the person depicted.

Deepfake or other artificial-intelligence-generated or manipulated content that may be misleading or harmful; content promoting, encouraging, or instructing illegal activities, including drug trafficking, arms trafficking, human trafficking, or terrorism; unauthorized use or distribution of copyrighted materials; unauthorized publication of personal data such as phone numbers, addresses, credit card information, or identification numbers.

5.3 Rights and licenses to content

The Content Provider (Model) retains full copyright and intellectual property rights to content they create and upload. However, by uploading content to the Platform, the Content Provider automatically grants the Service Provider a non-exclusive, worldwide, royalty-free, transferable, and sublicensable license to store, copy, modify for technical purposes, display and distribute content through the Platform, create previews and thumbnails, and use for promotional purposes with the Content Provider's prior consent.

This license remains in effect until the content is deleted or the Content Provider account is terminated; however, for content already sold or licensed, the license remains valid to the extent necessary to ensure buyers' acquired rights. By purchasing content or subscribing, buyers acquire limited, non-exclusive, non-transferable, personal use rights that authorize them solely to view the content through the Platform.

5.4 Content supervision and moderation

The Service Provider operates a comprehensive content moderation system to ensure Platform security and compliance with community standards. The moderation system applies a multi-tiered approach combining automated technologies and human review.

Automated pre-screening uses artificial intelligence and machine learning algorithms to identify potentially problematic content. This includes image recognition technologies to detect prohibited visual elements, text analysis to filter hate speech and other prohibited text content, and hash-matching technology to prevent re-uploading of previously removed content.

Trained human moderators review content flagged by the automated system and conduct random checks. Moderators receive special training in recognizing different types of problematic content and consider context and cultural specificities in their decisions.

Moderation decisions are generally made within seventy-two hours. In accordance with Article 17 of the DSA, where a Content Provider's content is restricted, removed, demonetized, or otherwise affected by a moderation decision, the Content Provider receives a Statement of Reasons specifying the type of restriction, the territorial scope, the underlying facts, the legal or contractual ground (referencing the specific clause of these GTC), the use of automated means in the decision, and information on internal complaint mechanisms and out-of-court dispute settlement options.

Content Providers may appeal decisions through the Platform's internal complaint-handling system within six months of the decision, in which case independent human review occurs free of charge.

5.5 Content quality expectations

The Platform maintains high quality standards for exclusive content, especially for paid content. Visual content (images and videos) must have appropriate resolution, with minimum 1080p HD quality recommended for videos and minimum 1920×1080 pixel resolution for images. Content must be sharp, well-lit, and of professional or near-professional quality.

Audio content must have clear, understandable sound quality with minimal background noise. Content descriptions must be accurate and truthful, avoiding misleading titles or clickbait techniques. Content Providers must properly categorize and tag their content so buyers can easily find materials matching their interests.

5.6 Continued buyer access in case of Content Provider account closure

Where a Content Provider account is voluntarily closed, deleted at the request of the Content Provider, or permanently terminated by the Service Provider for breach of these GTC or the Content Creator Agreement, the personal data of the Content Provider is removed and their public profile is deactivated in accordance with applicable data protection laws.

However, content previously purchased by Buyers prior to account closure shall, to the extent technically feasible, remain accessible to those Buyers within their personal library on the Platform under a "Deleted Creator" label, in order to preserve the limited usage rights acquired by the Buyer at the time of purchase. The Buyer's right to access purchased content survives the closure of the

Content Provider's account but ceases automatically where the content is required to be removed for legal, safety, or rights-infringement reasons.

Where access cannot be preserved due to legal, safety, or technical reasons (including but not limited to confirmed unlawful content, valid takedown notices, or successful third-party rights claims), affected Buyers shall not be entitled to a refund of tokens already spent on access, except where mandatory consumer protection law requires otherwise or where the Service Provider, in its discretion, decides to grant a goodwill credit.

5.7 Custom content orders and escrow

The Platform supports custom content orders whereby Buyers may commission personalized content from Content Providers. Custom content orders are subject to the following rules:

- The minimum order value is ten (10) tokens; there is no maximum cap on order value, except that custom content orders exceeding two hundred (200) tokens are subject to administrative review and approval by the Service Provider prior to execution, in line with the anti-money-laundering controls described in Section 8.6.
- Tokens spent by the Buyer on a custom content order are placed in escrow at the moment of order placement and are not credited to the Content Provider until the order is accepted by the Buyer or until the auto-acceptance period expires.
- Once the Content Provider has delivered the agreed content, the Buyer has forty-eight (48) hours to either accept delivery or raise a dispute. In the absence of any action by the Buyer within forty-eight (48) hours, the order is automatically deemed accepted and tokens are released from escrow to the Content Provider, subject to the payout holding rules in Section 8.7.
- In case of dispute, the Service Provider reviews the order, the agreed specifications, and the delivered content, and decides whether to release the escrowed tokens to the Content Provider, refund the Buyer in tokens, or apply a partial split. The decision of the Service Provider is final, subject to the dispute resolution procedures in Section 13.

6. Services and liability limitation

6.1 Service description and performance

The Bootyn.com platform provides digital content intermediation services on a marketplace model, connecting content providers (models) and buyers in a secure, reliable online environment. The Platform acts as an intermediary, where SPONDEX LTD provides the technical infrastructure, payment system, and necessary services for selling digital content.

The time of service performance is the moment of successful payment processing and technical opening of access to digital content. It is important to emphasize that the service does not constitute a transfer of ownership but provision of usage rights in the form of a limited, personal, non-exclusive

license. This license authorizes solely viewing of content through the Platform and does not include rights to download, copy, transfer, or commercial use.

6.2 "As is" provision

The Platform and all related services are provided on an "as is" and "as available" basis, without any express or implied warranty, save for warranties that cannot lawfully be excluded. The Service Provider does not guarantee that the Platform will operate without interruption, error-free, or virus-free, that the Platform will be compatible with all hardware and software, that the service will always be available, or that all errors will be corrected.

The Service Provider accepts no responsibility for the accuracy, completeness, reliability, or quality of content published by Users or Content Providers, except where mandatory consumer protection law (including Directive (EU) 2019/770 on contracts for the supply of digital content) imposes liability for non-conformity. Each User uses the Platform and accesses content at their own risk.

6.3 Limitation of liability

The Service Provider, its owners, officers, employees, subcontractors, and other contributors shall under no circumstances be liable for indirect, consequential, punitive, or exemplary damages, including but not limited to lost profits, data loss, business loss, damage to reputation, or other pecuniary or non-pecuniary damages arising from use or inability to use the Platform.

The Service Provider’s maximum liability shall in no case exceed the amount paid by the respective User for Platform services in the three months preceding the occurrence of the damage event. Nothing in these GTC excludes or limits liability for intentional misconduct, gross negligence, personal injury or death caused by negligence, fraud or fraudulent misrepresentation, or any other liability that cannot be lawfully excluded under the applicable law of the User’s residence.

6.4 Technical limitations of the Website

Platform operation is subject to various technical limitations that Users acknowledge and accept. These include geographic access restrictions (geo-blocking) in certain countries or regions, bandwidth and data traffic limitations to ensure service stability, limits on the number of concurrent connections per user, and security measures such as rate limiting and CAPTCHA systems to prevent abuse.

A modern web browser is required for optimal Platform operation, and certain features may not be available in older browsers or devices. The Service Provider reserves the right to perform technical maintenance during which the service may be temporarily unavailable or limited.

6.5 Service modification and termination

The Service Provider reserves the right to modify, suspend, or terminate any Platform feature or service at any time, with or without prior notice. This includes introducing new features, removing or modifying existing features, changing pricing or fee structure, and terminating the entire service.

For significant changes, the Service Provider strives to provide Users with at least thirty days' advance notice. In case of complete service termination, the Service Provider will make reasonable efforts to allow Users and Content Providers to access their data and content, and to find an equitable solution regarding unused tokens or subscriptions.

6.6 Availability guarantee

While the Service Provider strives to ensure high Platform availability, aiming to achieve 99% annual availability, it makes no legal commitment or guarantee of continuous availability. The Service Provider announces planned maintenance in advance, performs it during low-traffic periods when possible, and strives to ensure that duration does not exceed four hours per month.

In cases of force majeure events such as natural disasters, war, strikes, internet service provider failures, or DDoS attacks, the Service Provider is not responsible for service outages or limited availability. In such cases, the Service Provider makes all reasonable efforts to restore service as soon as possible.

7. Payments and fees

7.1 Payment methods

The Platform accepts various payment methods for User convenience. Accepted payment instruments include major credit and debit cards such as Visa and Mastercard, as well as certain digital wallets and alternative payment methods that may vary by region. All payment transactions occur in a secure, PCI DSS compliant environment with SSL/TLS encryption.

Incoming payment processing is performed by reliable international payment processor partners specializing in handling payment transactions for digital content and adult services. Settlements to content providers are made through dedicated payout service providers ensuring fast and reliable money transfers worldwide. The current list of payment processors and payout providers used by the Platform is disclosed in the Privacy Policy as data processors and may be updated from time to time.

7.2 Prices and fees

Prices displayed on the Platform appear exclusively in US dollars (USD) and are always gross prices including applicable taxes, including VAT where applicable. For Buyers paying with non-USD payment instruments, the actual amount charged is converted to USD at the exchange rate applied by the Buyer's payment provider at the moment of the transaction. The Service Provider fulfills tax obligations in accordance with applicable European Union and national legislation, including VAT reporting and payment through the OSS system.

The Service Provider reserves the right to modify prices and fees, providing Users with at least thirty days' advance notice of such modifications. Already purchased tokens or active subscriptions are not affected by the modification; however, for renewing subscriptions, new prices apply from the next billing cycle.

7.3 Subscriptions and recurring payments

Subscriptions automatically renew at the end of the selected billing cycle unless canceled by the User. Cancellation can be made at any time in user account settings and takes effect from the next billing cycle. The Service Provider sends a reminder notification to the User three days before renewal.

In case of failed payment, the Service Provider attempts to collect the fee multiple times within a specified period. If payment remains unsuccessful, the subscription automatically terminates, and access to subscription content ceases. Pro-rata refunds are generally not possible unless required by law or the Service Provider decides otherwise on equitable grounds.

7.4 Billing and VAT

SPONDEX LTD issues electronic invoices for all transactions in the buyer's name. Invoices are automatically generated in PDF format and sent to the User's registered email address. Billing occurs according to the marketplace model, where the Service Provider acts as an intermediary and handles transactions.

For B2C sales within the European Union, the Service Provider fulfills VAT obligations through the One-Stop-Shop (OSS) system in accordance with applicable laws. For B2B settlements with Content Providers acting as independent contractors, reverse-charge or local invoicing rules apply depending on the Content Provider's tax residence. Content Providers are solely responsible for declaring and paying their own income tax and any applicable local VAT or sales tax in their jurisdiction of residence.

7.5 Fraud and abuse prevention

The Service Provider operates a comprehensive fraud prevention system to protect the Platform and Users. This includes real-time transaction monitoring to detect suspicious activities, artificial-intelligence-based pattern recognition to identify fraudulent transactions, detection of multiple account abuse, and verification of payment data with card issuers.

In cases of suspected fraud or abuse, the Service Provider is entitled to suspend transactions, initiate further verification, temporarily or permanently suspend the User's account, and notify competent authorities. Users are required to cooperate in fraud prevention investigations.

7.6 Right of withdrawal for digital content

In accordance with European Union consumer protection directives, consumers generally have a fourteen-day right of withdrawal for online purchases. However, for digital content, this right of withdrawal expires once performance begins, provided the consumer has expressly consented to this and acknowledged the loss of the right of withdrawal.

On the Platform, before finalizing a purchase, the User must expressly accept that they request immediate performance of digital content and acknowledge that they thereby lose their right of withdrawal. This consent is given by checking a checkbox during the payment process, and the choice is recorded in the system.

7.7 Platform usage fee structure

For operating the Platform, providing technical infrastructure, and related services, the Service Provider charges a commission or platform usage fee deducted from Content Providers' gross revenue. This fee covers server costs and hosting services, payment system operation and transaction fees, content moderation and customer service, Shufti Pro identity verification service, marketing and promotional activities, and fulfillment of tax obligations.

Settlement to content providers occurs after commission deduction. The exact fee structure is detailed in the Content Creator Agreement, and the fee amount may depend on revenue size, content provider activity, and other factors.

8. Token-based access system

8.1 General description of the token system

The Platform uses its own virtual payment instrument called tokens, which facilitate and provide flexibility for accessing digital content. Tokens do not qualify as money, securities, electronic money, or cryptocurrency within the meaning of Regulation (EU) 2023/1114 (MiCA), Directive 2009/110/EC (E-Money Directive), or equivalent national legislation. They can only be used within the Platform to access specific services and content.

Advantages of the token system include flexible pricing options for Content Providers, simplified transactions within the Platform, better cost control for Users, and simplification of international payments through a unified internal settlement system. Token value is fixed at the time of purchase and does not change due to market rates or other external factors.

8.2 Token packages and pricing

The Platform offers various token packages that may include volume discounts. Purchasing larger packages generally results in a more favorable unit price. Token package prices and composition may change from time to time due to promotions, campaigns, or business considerations; however, the value and usability of already purchased tokens do not change.

Token purchases constitute final transactions and are generally non-refundable. Purchases are made using the selected payment method, and tokens are immediately credited to the user account.

8.3 Token usage options

Tokens can be widely used on the Platform for various purposes. They primarily serve to unlock exclusive content, where Content Providers can determine how many tokens are required for specific content. They can also be used for accessing live streams, requesting custom content or personalized videos in accordance with Section 5.7, sending tips to favorite Content Providers, activating premium features, and opening special communication options.

Token usage is final, and used tokens cannot be refunded, even if the User is dissatisfied with the acquired content. Exceptions include cases where content is unavailable due to technical error, or when the Service Provider determines that content significantly differs from its description or was sold fraudulently.

8.4 Token expiration and validity

Purchased tokens are valid for twenty-four (24) months from the date of purchase by default. After eighteen (18) months of inactivity, the Service Provider sends a warning notification to the User about approaching token expiration and provides an opportunity to use them. During temporary account suspension, tokens do not expire; however, all unused tokens are lost upon permanent account deletion.

The Service Provider reserves the right to issue tokens with shorter or longer validity periods as part of special promotions, clearly informing Users before purchase. Expired tokens cannot be used and cannot be converted to money.

8.5 Token refund rules

Token purchases are generally final and non-refundable, consistent with consumer protection rules for digital content. However, in exceptional cases, the Service Provider may provide refunds at its discretion on equitable grounds. Such cases may include double charging due to technical error, system error preventing token crediting, becoming a victim of fraud, or force majeure events.

Refund requests must be submitted to legal@bootyn.com within fourteen days of the problem arising, with detailed description and evidence. The Service Provider investigates the request within thirty days and notifies the User of its decision.

8.6 Anti-money-laundering controls and token purchase limits

In line with applicable anti-money-laundering and counter-terrorist-financing legislation, including Directive (EU) 2015/849 as amended and the implementing Cypriot legislation, and to manage exposure to fraud and chargeback risk, the Service Provider applies tiered daily token-purchase limits depending on the verification status of the User:

- Unverified Users (registered but without confirmed email): up to USD 500 per twenty-four-hour rolling window.
- Email-verified Users (no Shufti Pro KYC completed): up to USD 1,000 per twenty-four-hour rolling window.
- KYC-verified Users (Shufti Pro identity verification successfully completed): up to USD 5,000 per twenty-four-hour rolling window.

The Service Provider may temporarily lower these limits or require additional verification where transaction patterns indicate elevated risk, including but not limited to use of multiple payment instruments in a short period, IP-address mismatches, the same device or IP being shared between a Content Provider and a Buyer engaging in transactions with each other, the concentration of revenue

of a Content Provider on a single Buyer, the placement of unusually high custom-content orders by a newly created account, or any other pattern indicating possible structuring, fraud, or money laundering.

Custom-content orders exceeding two hundred (200) tokens, as well as token purchases above the applicable per-window limit, are subject to administrative review and may be rejected at the sole discretion of the Service Provider. Where required by Cypriot anti-money-laundering legislation transposing Directive (EU) 2015/849 (as amended), the Service Provider files Suspicious Transaction Reports (STRs) with the Unit for Combating Money Laundering (MOKAS) of the Republic of Cyprus, without notification to the affected User where such notification is prohibited under tipping-off rules.

8.7 Content Provider payouts and onboarding controls

To manage fraud risk during onboarding and to ensure compliance with payout-provider requirements, the following controls apply to Content Provider payouts:

- The first payout requested by any newly onboarded Content Provider is subject to a manual review by the Service Provider before release.
- During the first thirty (30) days following the activation of Content Provider status, total payouts are capped at five hundred US dollars (USD 500), with any excess balance carried over to subsequent payout periods after the cap no longer applies.
- Earnings from custom-content orders are subject to a fourteen-day (14) holding period, calculated from the moment the order is accepted by the Buyer or auto-accepted under Section 5.7, before being eligible for payout. This holding period is intended to absorb chargeback and dispute risk.
- The Service Provider reserves the right to extend holding periods, withhold individual payouts, or apply additional verification where elevated fraud, chargeback, or compliance risk is identified.

8.8 Prohibition of token transfer

Tokens are strictly personal and cannot be transferred to other Users or third parties in any form. It is prohibited to sell, exchange, gift, or transfer tokens in any way. Tokens cannot be exported outside the Platform and cannot be converted to other virtual or real payment instruments.

Violation of the token transfer prohibition constitutes a serious violation and has immediate consequences, including immediate and permanent deletion of all affected accounts, invalidation of tokens, and the Service Provider reserves the right to take legal action. The Platform uses automated systems to detect and prevent such abuse.

9. Intellectual property rights and protection

9.1 Website content and ownership

The Platform's entire infrastructure, including the website's source code, software, algorithms, database structure, user interface, design, graphics, logo, trademarks, and all other intellectual creations, is the exclusive property of SPONDEX LTD or its licensors. These elements are protected by copyright, trademark, and other intellectual property rights under European Union and international conventions.

The Platform's technological solutions, business model, and operational processes constitute trade secrets and enjoy strict protection. Copying, modifying, reverse engineering, decompiling, or creating derivative works from the Platform or any part thereof without the Service Provider's prior written permission is prohibited.

9.2 Trademarks and service marks

The names "Bootyn," "Bootyn.com," the Platform logo, and other related trademarks are registered or common law protected trademarks of SPONDEX LTD. Use of these trademarks is only possible with the Service Provider's prior written permission. Unauthorized use of trademarks constitutes trademark infringement and has legal consequences.

Factual mention of the Platform's name in news reports, opinions, or nominative use is permitted, provided it does not create the appearance that the Service Provider endorses or approves the content or activity. Content Providers may use descriptive expressions such as "Available on Bootyn.com" for their marketing purposes but may not use the Platform's logo or trademarks without the Service Provider's permission.

9.3 Copyright infringement and complaint handling

The Platform is committed to respecting intellectual property rights and applies zero tolerance to copyright infringement. Copyright complaints, including from rightsholders located in the United States, are processed under the Article 16 DSA notice-and-action mechanism described in Section 11. The Service Provider does not maintain a Designated Agent registered with the United States Copyright Office under 17 U.S.C. § 512(c)(2) and does not invoke the safe-harbor protections of the United States Digital Millennium Copyright Act (DMCA); the Article 16 DSA procedure provides substantively equivalent protection for rightsholders. Notices alleging copyright infringement may be sent to legal@bootyn.com.

To submit a copyright complaint, the rights holder or authorized representative must provide the following information in a notice sent to legal@bootyn.com: identification of the protected work, exact location (URL) of the allegedly infringing content, contact information, good faith statement about the infringement, statement about the notice's authenticity under penalty of perjury, and electronic or physical signature.

The Service Provider promptly investigates the matter upon receipt of the notice and removes or makes inaccessible the objectionable content in case of a valid complaint. The uploader receives notice of the complaint and has the opportunity to submit a counter-notice.

9.4 Limited license to users

By using the Platform, Users receive a limited, non-exclusive, non-transferable, revocable license to use the Platform and its services for personal, non-commercial use. This license only authorizes proper use of the Platform within the framework of the GTC.

The license does not include the right to commercially use, modify, copy, distribute, or resell the Platform or its content, automated downloading or data mining of Platform content, embedding or framing the Platform on other websites, or creating derivative works. Any use exceeding the license framework requires the Service Provider's prior written permission.

9.5 Users' intellectual property rights

Content Providers (Models) retain full copyright and intellectual property rights to original content they create and upload to the Platform. However, by uploading content, they automatically grant the Service Provider a license to use the content within the Platform framework, which includes storage, display, streaming, technical modifications (resizing, compression, format conversion), creating previews and index images, and promotional use with the Content Provider's consent.

By purchasing content or subscribing, buyers acquire only personal viewing rights, which do not include downloading, copying, distributing, or any other use of the content. Acquired usage rights can be exercised within the Platform framework and, subject to Section 5.6, cease upon deletion of the Content Provider's account or removal of the content.

10. Data protection

10.1 Privacy Policy

The Service Provider fully complies with the European Union General Data Protection Regulation (GDPR) requirements and applicable national data protection laws when processing personal data. Data processing principles include lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality.

Detailed data processing information — including the identity of the data controller, the contact details of the Data Protection Officer where designated, the legal bases for each processing operation, the list of data processors (including Shufti Pro, hosting providers, payment processors, and payout providers), retention periods, the supervisory authority (Office of the Commissioner for Personal Data Protection of the Republic of Cyprus), and the procedure for exercising data-subject rights — can be found in the Platform's separate Privacy Policy.

10.2 Confidential handling and security

The Service Provider pays special attention to personal data security. Technical measures include data encryption at rest and in transit (AES-256 and TLS 1.3), application of multi-level firewalls and intrusion detection systems, regular security audits and penetration tests, and automatic security backups.

As organizational measures, the Service Provider applies strict access control, provides regular data protection training for staff, enters into confidentiality agreements, and operates developed incident handling protocols. Use of the Shufti Pro system provides an additional security layer during identity verification.

10.3 Data retention period

Personal data retention period depends on the purpose of processing and legal obligations. Active user account data is retained during the contractual relationship, deleted accounts for ninety days, financial and billing data for eight to ten years in accordance with applicable laws, Shufti Pro verification results for the duration of the account, and system log files for twelve months.

After data retention periods expire, data is automatically deleted or anonymized unless longer retention is required by law or justified by ongoing legal disputes.

10.4 Recording of interactions

The Platform records and retains certain interactions on the Platform, including private messages exchanged through the built-in messaging system and live-stream sessions, for the purposes of fraud prevention, anti-circumvention, content-moderation, dispute resolution, and compliance with legal obligations. The legal basis for this processing is the legitimate interest of the Service Provider and other Users in preventing fraud, abuse, and circumvention of the Platform (GDPR Article 6(1)(f)), supplemented, where the recording is initiated by an individual User (e.g. recording of a paid live session for the User's own library), by the explicit consent of the participants given through a dedicated checkbox prior to the start of the session (GDPR Article 6(1)(a)).

Users are informed of recording in advance through these GTC, the Privacy Policy, and contextual notices on the Platform. Recorded data is accessible only to authorized employees under strict access protocols and is not shared with third parties except where required by law, court order, valid law-enforcement request, or in accordance with the data-processor list set out in the Privacy Policy. Users may exercise their data-subject rights, including access, rectification, erasure, and objection, in accordance with Section 10.5 and the Privacy Policy.

10.5 Data subject rights

Under GDPR, Users have the right to access their personal data, rectification of inaccurate data, erasure under certain conditions, restriction of processing, data portability, and objection to certain processing, including the right to lodge a complaint with the Office of the Commissioner for Personal Data Protection of the Republic of Cyprus or with the supervisory authority of the User's habitual residence.

Requests to exercise these rights can be submitted to legal@bootyn.com. The Service Provider responds to requests within thirty days, with the deadline extendable by an additional two months for complex requests. Request fulfillment is generally free, except for repeated or manifestly unfounded requests.

10.6 Data transfer to third parties

The Service Provider only shares personal data with third parties to the extent absolutely necessary for Platform operation. Such partners may include the Shufti Pro identity verification service, payment processors, payout service providers, hosting and cloud providers, email providers, and analytics tool providers. The full list of recipients is published and kept up to date in the Privacy Policy.

Strict data processing agreements are concluded with all data processor partners guaranteeing appropriate data protection. Where personal data is transferred outside the European Economic Area, the Service Provider relies on appropriate safeguards such as adequacy decisions or Standard Contractual Clauses adopted by the European Commission. The Service Provider does not sell Users' personal data and does not use it for marketing purposes without User consent.

11. Reporting illegal content and DSA compliance

11.1 Reporting mechanism (Article 16 DSA notice-and-action)

In accordance with Article 16 of the DSA, the Platform operates an electronic notice-and-action mechanism that allows any individual or entity to notify the Service Provider of the presence on the Platform of specific items of information considered to be illegal content. Reports can be submitted directly through the "Report" button on the Platform interface, by email to legal@bootyn.com, through the support ticket system, or by letter sent to the Service Provider's registered office.

A valid notice must be sufficiently precise and adequately substantiated, and shall include the exact electronic location of the content (URL or other identifier), a sufficiently detailed explanation of the reasons why the notifier considers the content to be illegal, the name and email address of the notifier (except where the content concerns offences referred to in Articles 3 to 7 of Directive 2011/93/EU on combating sexual abuse of children), and a statement confirming the good-faith belief of the notifier that the information and allegations contained in the notice are accurate and complete.

Notices submitted in accordance with the above shall give rise to actual knowledge or awareness for the purposes of Article 6 of the DSA in respect of the specific item of information concerned, where they allow the Service Provider to identify the illegality of the content without a detailed legal examination.

11.2 Actions upon a valid notice

Upon receipt of a valid notice, the Service Provider acts in a timely, diligent, non-arbitrary, and objective manner. As a first step, content may be temporarily restricted during investigation. Investigations generally conclude within seventy-two hours, during which the moderation team evaluates the content and the notice.

In case of a valid complaint, content is permanently removed or disabled, the uploader receives notification of the decision together with a Statement of Reasons under Section 11.4, there is an opportunity to submit a counter-statement and to use the internal complaint-handling system within

ten business days, in cases of repeated or serious infringement the uploader's account is suspended or deleted, and in particularly serious cases (e.g. suspected child sexual abuse material) the Service Provider notifies competent authorities, including, where applicable, NCMEC and Europol.

11.3 Consequences of false or abusive notices

Bad-faith, knowingly false, or abusive notices have serious consequences. The Service Provider reserves the right to restrict or terminate reporting privileges of repeat false notifiers in accordance with Article 23 of the DSA, suspend or delete user accounts, take legal action for damages, and file criminal complaints for false accusation or defamation.

The Service Provider pays special attention to abusive reporting between competing Content Providers and applies appropriate sanctions against such behavior.

11.4 Statement of Reasons (Article 17 DSA)

Where the Service Provider decides to remove or disable access to content, restrict the visibility of content, suspend or terminate monetization, or suspend or terminate the affected User's account, the Service Provider shall provide the affected User with a clear and specific Statement of Reasons setting out at least:

- the type of restriction imposed and, where relevant, its territorial scope and duration;
- the facts and circumstances relied on, including, where relevant, whether the decision was taken following a notice submitted under Article 16 DSA or pursuant to a voluntary investigation by the Service Provider;
- where applicable, information on the use of automated means in taking the decision;
- the legal or contractual ground for the decision, including reference to the specific clause of these GTC where the ground is contractual;
- information on the redress mechanisms available to the User, including the internal complaint-handling system referred to in Section 11.5 and out-of-court dispute settlement under Section 11.6.

11.5 Internal complaint-handling system (Article 20 DSA)

Affected Users may, free of charge, lodge a complaint against any decision referred to in Section 11.4 through the internal complaint-handling system available in their account settings, for a period of at least six months from the date of the decision. Complaints are handled in a timely, non-discriminatory, diligent, and non-arbitrary manner, and decisions taken on the basis of complaints are reviewed by qualified human staff and not solely on the basis of automated means. Where a complaint contains sufficient grounds to consider that the original decision was unfounded, the Service Provider reverses the decision without undue delay.

11.6 Out-of-court dispute settlement (Article 21 DSA)

Affected Users have the right to select any out-of-court dispute settlement body certified under Article 21 of the DSA in order to resolve disputes relating to decisions referred to in Section 11.4, including disputes that have not been resolved through the internal complaint-handling system. The selection of an out-of-court dispute settlement body is without prejudice to the User's right to initiate, at any stage, judicial proceedings to contest the relevant decision.

11.7 Single point of contact and legal representative (Articles 11–12 DSA)

In accordance with Article 11 of the DSA, the Service Provider has designated a single point of contact for direct, electronic communication with Member-State authorities, the European Commission, and the European Board for Digital Services. The single point of contact may be reached at legal@bootyn.com, with English as the working language.

In accordance with Article 12 of the DSA, the Service Provider has designated a single point of contact for Users, also reachable at legal@bootyn.com, allowing Users to communicate directly and rapidly with the Service Provider by electronic means in a user-friendly manner.

Article 13 of the DSA, which requires non-EU intermediary service providers to designate a legal representative within the European Union, does not apply to the Service Provider, which is established in the Republic of Cyprus.

11.8 Cooperation with authorities

The Service Provider fully cooperates with law enforcement agencies and other competent authorities in detecting illegal content and identifying perpetrators. This cooperation occurs within legal frameworks with appropriate legal authorization, including pursuant to orders to act against illegal content under Article 9 of the DSA and orders to provide information under Article 10 of the DSA.

Forms of cooperation may include data provision based on court orders or official requests, preservation of objectionable content as evidence, technical assistance for investigations, and proactive reporting when particularly serious violations are detected (e.g. suspected child sexual abuse material).

12. Indemnification and exemption

12.1 User indemnification obligation

The User undertakes to fully indemnify and hold harmless SPONDEX LTD, its owners, officers, employees, subcontractors, and other contributors from all claims, losses, damages, costs, and expenses arising from the User's violation of the GTC, except to the extent that such claims arise from the Service Provider's own intentional misconduct or gross negligence, or from any liability that cannot be lawfully excluded under applicable law.

This particularly applies to claims arising from illegal or infringing content uploaded by the User, claims arising from infringement of third parties' intellectual property rights, breach of 18 U.S.C. § 2257

record-keeping obligations by Content Providers, damages arising from providing false or misleading information, losses arising from abusive use of the Platform, and consequences arising from attempts to circumvent the Shufti Pro system.

12.2 Scope of exemption

The indemnification and exemption obligation extends to all direct and indirect damages, attorney fees and legal costs, costs of judicial or arbitration proceedings, administrative fines and sanctions, settlement amounts, and costs of restoring damage to the Service Provider's reputation.

The User must immediately notify the Service Provider upon becoming aware of circumstances that may establish their indemnification obligation and must fully cooperate in the defense.

12.3 Legal defense

In case of third-party claims, the Service Provider is entitled to take over defense management, retain legal counsel of its choice at the User's expense, and enter into reasonable settlements that the User must pay.

The User may not enter into settlements affecting the Service Provider without the Service Provider's prior written consent and must provide all necessary information and documents to the Service Provider for defense.

13. Alternative dispute resolution

13.1 Principle of dispute resolution

The parties' primary goal is amicable, out-of-court settlement of all disputes. To this end, the parties undertake to conduct good faith negotiations to resolve disputes before initiating court proceedings. Negotiation is initiated in writing, and the parties provide a thirty-day period for negotiations.

During negotiations, the parties strive to find a mutually acceptable solution, considering both parties' legitimate interests and the possibility of long-term cooperation.

13.2 Mediation and arbitration

If direct negotiation does not lead to results, the parties may initiate mediation proceedings with an independent mediator. Mediation costs are borne equally by the parties, and the mediation venue is Limassol, Cyprus, or an online platform.

If mediation also fails to produce results, final dispute resolution occurs before the competent court under the laws of the Republic of Cyprus. The language of court proceedings shall be English, to the extent permitted by Cypriot procedural rules.

13.3 International and consumer dispute resolution

Consumers residing in the European Union are entitled to contact consumer protection organizations in their place of residence, to use national or sectoral alternative dispute resolution (ADR) entities certified under Directive 2013/11/EU, and to consult the European Commission's list of certified ADR bodies available at https://consumer-redress.ec.europa.eu/dispute-resolution-bodies. The European Online Dispute Resolution (ODR) Platform previously established under Regulation (EU) No 524/2013 was discontinued on 20 July 2025 by Regulation (EU) 2024/3228 and is therefore no longer available.

For disputes specifically concerning content-moderation or account-level decisions taken by the Service Provider, Users may additionally rely on the internal complaint-handling system under Section 11.5 and the out-of-court dispute settlement mechanism under Article 21 of the Digital Services Act, as described in Section 11.6.

13.4 Competent court

If the dispute is resolved through court proceedings, the parties stipulate the exclusive jurisdiction of Limassol District Court, Cyprus. Exceptions include cases where mandatory legal provisions prescribe the jurisdiction of another court, particularly in consumer disputes where consumers retain the right to bring proceedings before the courts of their place of habitual residence.

The applicable law is the law of the Republic of Cyprus in all cases, taking into account European Union legislation, excluding conflict of law rules, and without depriving consumers of the protection afforded by mandatory provisions of the law of their habitual residence.

13.5 Waiver of class action rights

To the maximum extent permitted by applicable law, by accepting these Terms and Conditions the User expressly and voluntarily waives any right to initiate or participate in a class action lawsuit against the Service Provider, and agrees to pursue any claims arising against the Service Provider solely on an individual basis. This waiver does not apply where mandatory consumer protection law in the User's jurisdiction grants a non-waivable right to participate in collective redress.

14. Final provisions

14.1 Entire agreement

These GTC, the related Privacy Policy, Content Creator Agreement, 18 U.S.C. §§ 2257 and 2257A Compliance Declaration, and other referenced documents together constitute the entire agreement between the Service Provider and the User. These documents supersede all prior oral or written agreements, offers, or communications.

Service Provider employees, representatives, or contributors are not authorized to make oral promises or statements that differ from or supplement the GTC, and the User may not rely on such statements.

14.2 Partial invalidity

If any provision of these GTC proves to be invalid, unlawful, or unenforceable, this does not affect the validity and enforceability of the remaining provisions. The invalid provision is automatically replaced by a valid provision that comes as close as possible to the economic purpose and legal effect of the original provision.

The parties undertake to cooperate in good faith in appropriately replacing the invalid provision, taking into account the general purpose and spirit of the GTC.

14.3 Waiver and assignment

The Service Provider's abstention from exercising any right or remedy does not constitute a waiver and does not prevent subsequent exercise of that right. Waiver is only valid in writing, signed by the Service Provider's authorized representative.

The User may not assign their rights or obligations under the GTC to third parties without the Service Provider's prior written consent. The Service Provider may freely assign its rights and obligations to an affiliated company or to a successor in case of Platform sale.

14.4 Jurisdiction and applicable law

The law of the Republic of Cyprus applies to these GTC and all legal relationships arising from or related to them, taking into account European Union legislation. Application of the UN Convention on Contracts for the International Sale of Goods (CISG) is expressly excluded.

The choice of law may not deprive consumers of protections provided by mandatory provisions of the law of their residence.

14.5 Modification of the GTC

The Service Provider reserves the right to unilaterally modify the GTC. Users are notified of modifications via email and through notifications appearing on the Platform interface. For substantial modifications, the Service Provider provides at least fifteen days' notice.

Modifications take effect on the date of publication or at a specified later time. Continued use of the Platform following modifications constitutes acceptance of the modified GTC.

14.6 Contact

Official contact information:

- General customer service: support@bootyn.com
- Legal, DMCA, DSA matters: legal@bootyn.com
- Financial matters: finance@bootyn.com
- Data protection matters: legal@bootyn.com
- Section 2257 Custodian of Records: see separate 18 U.S.C. §§ 2257 and 2257A Compliance Declaration

- Postal address: SPONDEX LTD, Voukourestiou 25, NEPTUNE HOUSE, 1st floor, Flat/Office 11, Zakaki, 3045 Limassol, Cyprus

Response times:

- General inquiries: 72 hours
- Urgent security matters: 48 hours
- Legal inquiries: within 5 business days
- Financial matters: within 3 business days

14.7 Effective date of Terms of Use

These General Terms and Conditions enter into force on April 7, 2026, and remain in effect until revoked or until a new version is published. From the effective date, all previous versions lose their validity.

By accepting the GTC, the User declares that they have read, understood, and acknowledged them as binding. By using the Platform, the User continuously confirms acceptance of the GTC.

© 2026 SPONDEX LTD — All rights reserved

Bootyn.com Platform General Terms and Conditions

Last updated: April 28, 2026 | Version 1.4