PRIVACY POLICY

Bootyn.com digital content provider platform

Effective: April 7, 2026 | Version 1.1

Table of Contents

1. Introductory provisions

1.1 Purpose of the Privacy Policy

The purpose of this Privacy Policy is to provide detailed information to users of the Bootyn.com website (hereinafter: "Website" or "Platform") operated by SPONDEX LTD regarding our practices concerning the processing of personal data. This Privacy Policy defines what types of data we collect, how we use them, with whom we share them, and what rights users have regarding their personal data. The Platform operates on a marketplace model through the intermediation of adult-oriented, age-restricted digital content uploaded by independent content providers.

This Privacy Policy is to be read together with the General Terms and Conditions, the Cookie Policy, the 18 U.S.C. §§ 2257 and 2257A Compliance Declaration, and, for content providers, the Content Creator Agreement. In case of inconsistency between this Privacy Policy and any other Platform document concerning the processing of personal data, this Privacy Policy prevails.

1.2 Applicable legislation

We take into account the following legislation in our data processing:

- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR);
- Cypriot Law 125(I)/2018 on the Protection of Natural Persons with regard to the Processing of Personal Data;
- Cypriot Law on Certain Aspects of Information Society Services, in particular Electronic Commerce (L.156(I)/2004);
- Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act, DSA), to the extent it imposes obligations on us as a hosting service provider and online platform;
- Council Directive (EU) 2021/514 (DAC7) on the automatic exchange of information reported by digital platforms, as transposed into Cypriot law;
- Directive (EU) 2015/849 (as amended) on anti-money-laundering and counter-terrorist-financing, as transposed into Cypriot law;
- Directive 2002/58/EC (ePrivacy Directive), as amended, in respect of cookies and similar technologies;
- United States 18 U.S.C. § 2257 and 28 C.F.R. Part 75 record-keeping rules, in respect of records collected from content providers and depicted performers;
- other local data protection laws applicable according to the User's place of residence.

1.3 Definitions

For the purposes of this Privacy Policy, the following terms shall have the following meanings:

- Personal Data: any information relating to an identified or identifiable natural person.
- Special-category personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation (Article 9(1) GDPR).
- Data Processing: any operation or set of operations performed on personal data or sets of data, whether or not by automated means.
- Data Controller: the natural or legal person who, alone or jointly with others, determines the purposes and means of data processing. In this case, SPONDEX LTD.
- Data Processor: a natural or legal person who processes personal data on behalf of the controller.
- Data Subject Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes.
- Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- Standard User: a registered user who uses the basic functions of the Website.
- Premium User: a registered user who uses the expanded functions of the Website through subscription or other payment.
- Content Provider or Model: a user with special permissions who publishes digital content on the Website for which they may receive compensation.

1.4 Data Controller information

Controller name: SPONDEX LTD

Company registration number: HE 490894

Registered office: Voukourestiou 25, NEPTUNE HOUSE, 1st floor, Flat/Office 11, Zakaki, 3045 Limassol, Cyprus

Director and legal representative: Charalampos Lafazanis

Privacy contact / Data Protection Officer contact: legal@bootyn.com

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

2. Principles of data processing

2.1 Lawfulness, fairness and transparency

We are committed to processing personal data lawfully, fairly and in a transparent manner in relation to the data subject. In all data processing operations, we ensure that users receive clear information about who processes their personal data, for what purpose, on what legal basis, and for how long.

2.2 Purpose limitation

We collect personal data only for specified, explicit and legitimate purposes and do not process them in a manner incompatible with those purposes. If the purpose of data processing changes, we inform users in advance and request new consent if necessary.

2.3 Data minimization

We collect only personal data that is necessary and relevant for achieving the purpose of processing. We strive to process the minimum amount of personal data and use anonymous or pseudonymized data where possible.

2.4 Accuracy

We take all reasonable steps to ensure that the personal data we process is accurate and, where necessary, kept up to date. Inaccurate personal data is immediately deleted or rectified upon user request.

2.5 Storage limitation

We store personal data only for as long as necessary to achieve the purpose of processing or as required by legal obligations. After this, data is deleted or anonymized.

2.6 Integrity and confidentiality

We apply appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing, accidental loss, destruction or damage.

2.7 Accountability

We take responsibility for compliance with data protection principles and are able to demonstrate this. We regularly review our data processing practices, document processing operations, and conduct data protection impact assessments when necessary.

3. Scope of data processed and purpose of processing

3.1 Registration and user account

Data processed:

- Username; email address; password (stored as a salted hash, never in plaintext); registration date; IP address used at registration; optional profile picture, introduction text, and indicated interests.

Purpose of processing:

- Creating and managing user accounts; providing Platform services; user identification and authentication; communication with users.

Legal basis: performance of contract (Article 6(1)(b) GDPR) for mandatory account data; consent (Article 6(1)(a) GDPR) for optional profile data.

3.2 User authentication and age verification

Data processed:

- Verification result and timestamp returned by Shufti Pro; data extracted from the government-issued ID document (name, date of birth, document number, document type, issuing country); biometric facial-recognition match result. Biometric raw data and document images are processed by Shufti Pro as a sub-processor and are not stored on our servers.

Purpose of processing:

- Verifying that the User has reached the applicable age of majority (eighteen years, or such higher age as is required by applicable local law); identity confirmation; preventing abuse, fraud, and access by minors; complying with anti-money-laundering legal obligations and with the United States 18 U.S.C. § 2257 record-keeping requirements where applicable.

Legal basis: legal obligation (Article 6(1)(c) GDPR) for age verification, anti-money-laundering and 2257 record-keeping; legitimate interest (Article 6(1)(f) GDPR) in fraud prevention. The processing of biometric data through Shufti Pro is carried out on the basis of the User's explicit consent (Article 9(2)(a) GDPR), which is requested separately at the start of the verification flow.

3.3 Payment data

Data processed:

- Last four digits of the card number, card brand, card expiration date; billing address; payment history and transaction data; token balance and token usage history; chargeback and dispute records. Full card numbers (PAN) and CVV codes are processed exclusively by our PCI DSS certified payment processors and are not stored on our systems.

Purpose of processing:

- Processing payment transactions; managing subscriptions; preventing and detecting fraud; meeting accounting and tax obligations; investigating chargebacks and disputes.

Legal basis: performance of contract (Article 6(1)(b) GDPR); legal obligation in respect of accounting and tax records (Article 6(1)(c) GDPR); legitimate interest in fraud prevention (Article 6(1)(f) GDPR).

3.4 User interactions and communication

Data processed:

- Direct messages exchanged through the Platform's built-in messaging system; recordings of paid live-stream sessions where applicable; interaction timestamps and types; follows, likes, comments; token-spending events.

Purpose of processing:

- Providing core Platform services (messaging, live streaming, social features); fraud prevention and anti-circumvention checks; content moderation; dispute resolution; investigation of reports of illegal content and harassment.

Legal basis: performance of contract (Article 6(1)(b) GDPR) for delivery of the messaging and live-stream features; legitimate interest (Article 6(1)(f) GDPR) for moderation, fraud-prevention and anti-circumvention scanning of messages, balanced against the User's reasonable expectations and supported by clear up-front notice; explicit consent (Article 6(1)(a) and, where the recording reveals special-category data, Article 9(2)(a) GDPR) collected through a dedicated checkbox before the start of any User-initiated recording of a paid live-stream session.

3.5 Content Provider data

Data processed:

- Bank account number, IBAN/SWIFT or other payout-account information; tax identification number, VAT number where applicable, country of tax residence; gross revenue, payout history; performance metrics (number of followers, gross revenue, content interactions);

KYC and 2257 documentation collected via Shufti Pro and via the Content Creator Agreement, including signed performer release forms; copies of any documentation provided by the Content Provider relating to performers depicted in their content.

Purpose of processing:

- Settling and paying out earnings within the marketplace model; complying with accounting, tax, anti-money-laundering and DAC7 reporting obligations; complying with United States 18 U.S.C. § 2257 and 28 C.F.R. Part 75 record-keeping requirements as a primary or secondary producer where applicable; measuring and evaluating Content Provider performance for product analytics; investigating disputes and abuse.

Legal basis: performance of contract (Article 6(1)(b) GDPR) for payout and analytics; legal obligation (Article 6(1)(c) GDPR) for accounting, tax, AML, DAC7 and 2257 record-keeping; legitimate interest (Article 6(1)(f) GDPR) for fraud and abuse investigation.

DAC7 reporting threshold: under Council Directive (EU) 2021/514, we report Content Providers who, in a calendar year, are paid for more than thirty (30) relevant activities or receive total consideration exceeding two thousand euros (€2,000) for relevant activities, to the competent Cypriot tax authority, which then exchanges the information with the tax authority of the Content Provider's country of residence.

3.6 Automatically collected data

Data processed:

- IP address; browser type and version; operating system; device type and identifier; coarse geolocation derived from IP address; Platform usage data (pages visited, clicks, session duration); error reports and crash logs.

Purpose of processing:

- Ensuring technical operation, security and stability of the Platform; statistical analysis; product development and optimization; detection of security events, fraud and abuse; geo-blocking enforcement.

Legal basis: legitimate interest (Article 6(1)(f) GDPR) for security, fraud prevention and product analytics; legal obligation (Article 6(1)(c) GDPR) where logs are required for security or law-enforcement compliance.

3.7 Cookies and similar technologies

Data processed:

- Strictly necessary, functional, analytical and (where applicable) marketing cookie data, as detailed in our separate Cookie Policy.

Purpose of processing:

- Ensuring proper Platform functionality; remembering user preferences; improving user experience; producing aggregated analytics; displaying relevant advertising where the User has consented.

Legal basis: legitimate interest (Article 6(1)(f) GDPR) and Article 5(3) of the ePrivacy Directive for strictly necessary cookies; consent (Article 6(1)(a) GDPR and Article 5(3) of the ePrivacy Directive) for all non-essential cookies, given through the cookie banner displayed on first visit.

Detailed information about each cookie used, its provider, its purpose and its storage duration, together with instructions for managing or withdrawing consent, can be found in our separate Cookie Policy, accessible from the Platform footer.

3.8 Uploaded content (images, videos, live streams)

Data processed:

- Photos, videos and live-stream recordings uploaded or generated by Content Providers; content metadata (upload timestamp, file size, format, resolution); technical derivatives (resized versions, thumbnails, watermarked versions, CDN cache copies); content descriptions and tags; images and likenesses of persons depicted in content.

Purpose of processing:

- Providing Platform services; displaying and streaming content to authorized Buyers; technical optimization for different devices; copyright protection (watermarking and content fingerprinting); automated and human moderation; filtering of illegal content; backups and disaster recovery; CDN distribution.

Legal basis: performance of contract (Article 6(1)(b) GDPR) with the Content Provider; legitimate interest (Article 6(1)(f) GDPR) in moderation, abuse prevention and intellectual-property protection; legal obligation (Article 6(1)(c) GDPR) where moderation is required by the DSA, by anti-CSAM rules or by 18 U.S.C. § 2257.

Where uploaded content reveals special-category data within the meaning of Article 9(1) GDPR (in particular, data concerning sex life or sexual orientation), the additional legal basis for processing on our side is the explicit consent of the depicted person, collected by the Content Provider through a signed performer release form, made available to us under the Content Creator Agreement; and, where applicable, processing is necessary for the establishment, exercise or defence of legal claims (Article 9(2)(f) GDPR).

Special provisions for uploaded content:

- Content Providers are independent controllers in respect of the personal data of persons depicted in their content; they warrant in the Content Creator Agreement that they have collected all necessary consents and 18 U.S.C. § 2257 records before upload.
- The Platform performs automated and human moderation to filter illegal or violating content.

- Technical copies of content (different resolutions, CDN cache, backups) are necessary for service provision and are kept under the same security and access controls as the original content.

3.9 Buyer content-viewing data

Data processed:

- Records of which Content Providers a Buyer follows or subscribes to, which albums or live streams a Buyer purchases or accesses, search queries, and content recommendations served to the Buyer.

Purpose of processing:

- Granting access to purchased content; populating the Buyer's personal library; producing personalized recommendations; preventing fraud and chargeback abuse; producing aggregated, non-attributable analytics.

Legal basis: performance of contract (Article 6(1)(b) GDPR) for access management; legitimate interest (Article 6(1)(f) GDPR) for security and analytics. Because such viewing data may reveal information about a Buyer's sex life or sexual orientation, processing is also based on the Buyer's explicit consent (Article 9(2)(a) GDPR), which is built into the act of registering on an adult-content platform after a clear notice; this consent may be withdrawn at any time by closing the account.

3.10 Notice-and-action and DSA compliance data

Data processed:

- Notices received under Article 16 of the DSA, including the notifier's identity and contact details, content of the notice, attached evidence; Statements of Reasons issued under Article 17 of the DSA; internal complaint-handling records under Article 20 of the DSA; orders received from authorities under Articles 9 and 10 of the DSA.

Purpose of processing:

- Handling notices and complaints; complying with DSA transparency obligations; communicating with affected Users; cooperating with authorities; defending against legal claims.

Legal basis: legal obligation under the DSA (Article 6(1)(c) GDPR); legitimate interest in legal-claims management (Article 6(1)(f) GDPR).

4. Legal basis for data processing

This section summarizes, in one place, the legal bases on which we rely. The specific legal basis applicable to each processing operation is also stated in Section 3.

4.1 Consent (Article 6(1)(a) GDPR)

For certain data processing operations, the legal basis is the data subject's prior, voluntary, specific and informed consent. In such cases, Users may withdraw their consent at any time, which does not affect the lawfulness of processing based on consent before its withdrawal. Withdrawal is made as easy as giving consent.

Data processed based on consent particularly includes:

- sending marketing communications;
- non-essential cookies;
- optional profile data;
- recording of paid live-stream sessions initiated by a User.

4.2 Performance of contract (Article 6(1)(b) GDPR)

Many data processing operations are necessary to perform the contract with the User (the General Terms and Conditions and, for Content Providers, the Content Creator Agreement) or to take steps at the data subject's request prior to entering into a contract.

Data processed on this basis includes data necessary for registration and account management, payment data and transaction records, interaction data necessary for service delivery, payout data for Content Providers, and the storage and intermediation of uploaded content.

4.3 Legal obligation (Article 6(1)(c) GDPR)

In certain cases, the legal basis for processing is the fulfilment of a legal obligation to which we are subject.

Data processed on this basis includes:

- data retained for accounting and tax purposes (eight to ten years);
- data necessary for fulfilling DAC7 reporting obligations;
- identification and verification data related to anti-money-laundering;
- 18 U.S.C. § 2257 record-keeping data, where applicable;
- data transferred upon valid order from law enforcement or judicial authorities; and
- data we are required to process under the DSA (notice-and-action records, statements of reasons, internal complaints, transparency-report data).

4.4 Legitimate interest (Article 6(1)(f) GDPR)

In some cases, the legal basis for processing may be the legitimate interest of the Controller or a third party, provided that the interests, fundamental rights and freedoms of the data subject do not override those interests. We perform and document a balancing test for every legitimate-interest based processing operation; the result of those tests is available on request to legal@bootyn.com.

Data processed on this basis includes:

- fraud and abuse prevention and detection;
- information-security measures;
- scanning of in-platform messages for circumvention, fraud and harassment patterns;
- dispute resolution;
- aggregated, non-attributable analytics for product development;
- content moderation in addition to legally required moderation.

5. Special-category personal data (Article 9 GDPR)

Because the Platform makes available adult-oriented digital content, certain processing operations may relate to special-category personal data within the meaning of Article 9(1) GDPR — in particular, data concerning a natural person's sex life or sexual orientation, and biometric data processed for the purpose of uniquely identifying a natural person.

We process special-category personal data only on one or more of the following Article 9(2) GDPR conditions, in combination with the corresponding Article 6(1) basis:

- the explicit consent of the data subject (Article 9(2)(a) GDPR), in particular for the biometric component of Shufti Pro identity verification, for User-initiated recording of paid live-stream sessions, and for the Buyer's use of an adult-content platform that records content-viewing patterns;
- processing relates to personal data which are manifestly made public by the data subject (Article 9(2)(e) GDPR), in respect of content that the Content Provider voluntarily uploads and chooses to make publicly available on the Platform;
- processing is necessary for the establishment, exercise or defence of legal claims (Article 9(2)(f) GDPR), in particular for evidence preservation in dispute, fraud or law-enforcement contexts.

Withdrawal of explicit consent: an Article 9(2)(a) consent can be withdrawn at any time, with effect for the future, by writing to legal@bootyn.com or by closing the User account. Where withdrawal of consent makes the continued provision of the service impossible (for example, withdrawing consent to identity verification), the corresponding service feature will cease.

6. Data retention and deletion

6.1 Data retention periods

We store personal data only for as long as necessary to achieve the purpose for which the data was originally collected, or as required by law. The retention periods for the main data categories are as follows:

- Registration and user-account data: during the existence of the account, and for up to ninety (90) days after account deletion, except where a longer retention is required by law or by a pending dispute.
- Shufti Pro verification result and metadata: for the duration of the User account, and for an additional five (5) years after account deletion where required by anti-money-laundering legislation. Biometric raw data and document images are not retained by us; they are processed by Shufti Pro and deleted in accordance with Shufti Pro's data-protection commitments.
- Payment and transaction data: eight to ten (8–10) years from transaction completion for accounting and tax obligations under Cypriot law.
- Direct messages and live-stream recordings: during the existence of the account and for up to twelve (12) months after account deletion, for dispute resolution and legal-defence purposes. User-initiated recordings of paid live-stream sessions remain in the recording User's personal library subject to the rules in the General Terms and Conditions.
- Content Provider financial data: during the existence of the relationship and for eight to ten (8–10) years after termination for tax and accounting obligations.
- 18 U.S.C. § 2257 records: for the period required by 28 C.F.R. Part 75.
- Uploaded content: during the existence of the Content Provider account, and — in accordance with Section 5.6 of the General Terms and Conditions — also after account closure, to the extent necessary to preserve access to the content for Buyers who have already purchased it, except where the content must be removed for legal, safety or rights-infringement reasons.
- DAC7 reporting data: for the period required by Cypriot tax law transposing Council Directive (EU) 2021/514, generally five (5) years.
- Automatically collected technical and security log data: up to twelve (12) months.
- Support-ticket data: up to five (5) years.
- Notice-and-action and DSA records: for as long as required by Article 24 DSA transparency obligations and applicable record-keeping rules.
- Cookie data: as detailed in the Cookie Policy, with retention varying by cookie type.

6.2 Management of inactive accounts

If a User does not log in for six (6) months, the account is considered inactive. We follow this procedure for inactive accounts:

- we send a notification of inactive status to the registered email address;
- the User has thirty (30) days to reactivate by simply logging in;
- if no reactivation occurs, the account is suspended and remains in this state for a further one hundred and fifty (150) days;

- after a total of one hundred and eighty (180) days of inactivity, the account may be deleted, with prior notification to the User. Deletion is subject to the retention rules in Section 6.1 above.

6.3 Data deletion procedures

Data deletion may occur in different ways depending on the type of data:

- Automatic deletion: certain data categories are deleted automatically when they reach the end of the retention period.
- User-initiated deletion: Users may request deletion of their personal data through the Platform settings or by writing to legal@bootyn.com.
- Partial deletion: in certain cases, only part of the data is deleted while other data is retained to comply with legal obligations or to defend legitimate interests (for example, accounting records, 2257 records, AML records).

We process deletion requests within thirty (30) days, with the deadline extendable by an additional two (2) months for complex requests, and notify the User of the outcome.

6.4 Anonymization and pseudonymization

We anonymize or pseudonymize certain data instead of deleting it. Anonymized data no longer qualifies as personal data and is no longer subject to GDPR. Pseudonymized data is processed in such a way that it can no longer be attributed to a specific data subject without additional information, which is stored separately and securely. We use these techniques primarily for statistical analyses, research, and product-development decisions.

7. Data transfer and data processors

7.1 Data transfer within the Controller

Personal data within the SPONDEX LTD organization may only be accessed by persons who need it to perform their job duties. All employees and contributors are bound by written confidentiality obligations.

7.2 Data processors

We use third-party data processors for certain processing operations. We make data available to processors only to the extent and for the duration necessary, and ensure by data-processing agreement under Article 28 GDPR that they process data only on our documented instructions and with appropriate technical and organizational security measures.

Categories of data processors used:

- payment service providers: processing of payment transactions, fraud screening;
- payout service providers: settlement of payouts to Content Providers;

- hosting, cloud and CDN providers: storage and delivery of data and content;
- Shufti Pro: identity and age verification, including biometric verification;
- customer-service tooling providers: handling of User inquiries;
- analytics providers: aggregated Platform usage statistics;
- email and communication providers: transactional and marketing communications;
- security and anti-fraud providers: detection and mitigation of attacks and abuse.

An up-to-date list of named processors, including the country of processing, is available on request to legal@bootyn.com and is also published in the Cookie Policy where the processor sets cookies.

7.3 Data transfer to third parties other than processors

We transfer personal data to third parties other than processors only in the following cases:

- with the User's express prior consent;
- to comply with legal obligations (in particular DAC7 reporting to the Cypriot tax authority, AML reporting to MOKAS, 2257 inspections, DSA reporting);
- based on a valid order from a court or competent authority;
- for the establishment, exercise or defence of legal claims.

We do not sell, rent or otherwise make personal data available to third parties for their own commercial purposes.

7.4 International data transfer

Because SPONDEX LTD is established in the Republic of Cyprus and provides services globally, personal data may be transferred to countries outside the European Economic Area (EEA). For all such transfers, we ensure that one of the following safeguards is in place:

- transfer to a country covered by an adequacy decision of the European Commission under Article 45 GDPR;
- transfer under the EU–US Data Privacy Framework (DPF) where the recipient is self-certified under the DPF, in accordance with the European Commission's adequacy decision of 10 July 2023;
- transfer under Standard Contractual Clauses (SCCs) adopted by the European Commission, with supplementary measures where necessary on the basis of a transfer impact assessment;
- transfer based on one of the derogations set out in Article 49 GDPR, only in exceptional cases.

A copy of the relevant safeguards (excluding any commercially sensitive information) is available on request to legal@bootyn.com.

7.5 Data transfer based on official request

We may disclose personal data upon valid request from law-enforcement, regulatory or judicial authorities. In such cases:

- we examine the legal validity of every request;
- we transfer only the minimum amount of data necessary to comply with the request;
- we strive to notify the data subject if and when this is permitted by law and by the requesting authority;
- we document the fact and the circumstances of every transfer, and report aggregated figures in our annual transparency report.

8. Data security

8.1 Technical measures

We apply, among others, the following technical measures:

- Encryption: passwords are stored as salted hashes; payment data is encrypted in line with PCI DSS; data in transit is protected by TLS 1.3; data at rest is protected by AES-256 where applicable.
- Firewalls and intrusion detection: layered firewalls and intrusion-detection systems.
- Logging and monitoring: continuous logging and monitoring of system access to detect and prevent security events.
- Backups: regular encrypted backups stored separately from production systems.
- Patch management: timely application of security patches.
- Network segmentation: isolation of systems storing different categories of data.
- Multi-factor authentication for staff system access.
- DDoS protection.
- Content protection: watermarking and access-control measures on uploaded content.

8.2 Organizational measures

We apply, among others, the following organizational measures:

- documented data-protection and information-security policies;
- role-based access control on a least-privilege basis;
- regular data-protection and information-security training for staff;
- written confidentiality obligations for employees and processors;
- regular review and testing of security controls;
- documentation of processing activities under Article 30 GDPR;
- a designated Data Protection Officer reachable at legal@bootyn.com.

8.3 Personal data breach management

In the event of a personal-data breach, we follow the procedure below:

- Detection and reporting: all employees and processors must report any detected or suspected data breach without delay.
- Assessment: we assess the nature, severity and likely consequences of the incident.
- Containment and mitigation: we take measures to contain the incident and limit damage.
- Notification: we notify the Office of the Commissioner for Personal Data Protection of the Republic of Cyprus within seventy-two (72) hours of becoming aware, where the breach is likely to result in a risk to the rights and freedoms of natural persons (Article 33 GDPR), and notify affected data subjects where the risk is likely to be high (Article 34 GDPR).
- Documentation: we document every incident, including circumstances, impact and measures taken.
- Lessons learned: we update our security controls based on incident analysis.

8.4 Data Protection Impact Assessments

We carry out Data Protection Impact Assessments (Article 35 GDPR) where required, in particular before introducing new technologies (such as new AI-based moderation systems), where automated decision-making with significant effects is involved, where special-category personal data is processed on a large scale, and where processing is otherwise likely to result in a high risk to data subjects.

9. Data subject rights

9.1 Right to be informed

You have the right to receive clear, transparent and easily understandable information about how we process your personal data. This Privacy Policy is our principal instrument for satisfying that right.

9.2 Right of access (Article 15 GDPR)

You have the right to confirm whether personal data concerning you is being processed, and if so, to access the personal data and receive a copy. Access requests can be submitted to legal@bootyn.com or through the privacy settings in your account.

9.3 Right to rectification (Article 16 GDPR)

You have the right to request rectification of inaccurate personal data or completion of incomplete data. Most personal data can be modified directly through user-account settings; for everything else, contact legal@bootyn.com.

9.4 Right to erasure / right to be forgotten (Article 17 GDPR)

Under certain circumstances, you have the right to request erasure of your personal data. The right to erasure is not absolute, and we may refuse where processing is necessary for compliance with a legal obligation (for example, accounting retention, AML, DAC7, 2257 record-keeping) or for the establishment, exercise or defence of legal claims.

9.5 Right to restriction of processing (Article 18 GDPR)

You have the right to request restriction of processing where: you contest the accuracy of the data, processing is unlawful, we no longer need the data but you require it for legal claims, or you have objected to processing pending verification.

9.6 Right to data portability (Article 20 GDPR)

Where processing is based on consent or contract and is carried out by automated means, you have the right to receive your personal data in a structured, commonly used, machine-readable format and to have that data transmitted to another controller where technically feasible.

9.7 Right to object (Article 21 GDPR)

You have the right to object to processing of your personal data based on legitimate interest or on the public interest, including profiling. You have an absolute right to object to processing for direct-marketing purposes.

9.8 Rights related to automated decision-making and profiling (Article 22 GDPR)

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you, except where the decision is necessary for entering into or performing a contract, is authorized by law, or is based on your explicit consent. Where automated tools are used in content moderation that significantly affects you, the decision is reviewed on request by qualified human staff in accordance with Article 20 of the DSA, and a Statement of Reasons is issued in accordance with Article 17 of the DSA, as further described in the General Terms and Conditions.

9.9 Right to withdraw consent

Where processing is based on consent, you have the right to withdraw that consent at any time, with effect for the future. Withdrawing consent does not affect the lawfulness of processing based on consent before its withdrawal.

9.10 How to exercise your rights

You can exercise your rights by writing to legal@bootyn.com from the email address associated with your account, or by using the privacy settings in your account. We will respond within thirty (30) days, with the deadline extendable by a further two (2) months for complex requests. Exercise of these rights is free of charge, except for repeated or manifestly unfounded requests, where we may either charge a reasonable fee or refuse the request, in line with Article 12(5) GDPR.

10. Special data processing rules by user category

10.1 Standard Users

For Standard Users, we collect only the data necessary for basic Platform use, store data about interactions with followed Content Providers and other Users, and collect statistical data about the categories of content viewed.

10.2 Premium Users

For Premium Users, in addition to Standard User data processing, we process additional data necessary for managing subscriptions, store more detailed data about subscribed content and token usage, and apply enhanced security measures to protect Premium Users' data.

10.3 Content Providers

For Content Providers, we apply the additional rules below:

- detailed identification for legal compliance (KYC via Shufti Pro);
- processing of bank-account or payout-account information;
- processing of tax information for DAC7 reporting and Cypriot tax compliance;
- processing of 18 U.S.C. § 2257 record-keeping documentation, where applicable, including signed performer release forms and copies of performer government-issued ID;
- maintenance of detailed statistics on content performance and revenue;
- processing of documents related to the Content Creator Agreement;
- retention of data for the period required by applicable tax, accounting, AML and 2257 rules.

Content Providers acknowledge that they are independent controllers in respect of the personal data of persons depicted in their content, and that they bear the responsibility for collecting all necessary consents and records before upload.

10.4 Protection of minors

The Platform may be used only by adults (eighteen years of age or such higher age as is required by applicable local law). To this end:

- we apply an age-verification system at registration using Shufti Pro;
- we require government-issued ID documents for verification;
- we perform automated and human moderation;
- we operate an in-product reporting system;
- we check uploaded content to ensure it does not contain depictions of minors.

If we become aware that a User has not reached the applicable age of majority, we immediately delete their account and all associated personal data, except data that we must retain to fulfil legal

obligations (for example, evidence preservation in connection with a referral to law enforcement or NCMEC).

11. Remedies

11.1 Complaint handling

If you believe we have violated applicable laws in processing your personal data, please contact us by email at legal@bootyn.com (data protection), at support@bootyn.com (general customer service), or at finance@bootyn.com (financial matters). We investigate complaints within thirty (30) days and respond in writing.

11.2 Right to lodge a complaint with a supervisory authority

If you have not received a satisfactory response, you have the right to lodge a complaint with the competent data-protection authority.

In Cyprus:

- Office of the Commissioner for Personal Data Protection
- Address: Iasonos 1, 1082 Nicosia, Cyprus
- Website: www.dataprotection.gov.cy

In the European Union:

- the data-protection authority of the Member State of your habitual residence, place of work, or place of alleged infringement.

11.3 Judicial remedies

In addition to or instead of administrative remedies, you may seek judicial remedies. Proceedings may be brought:

- in Cyprus: before the Limassol District Court;
- in the European Union: before the courts of the Member State where the controller has an establishment, or before the courts of the Member State of your habitual residence.

12. International compliance

12.1 GDPR compliance

We make our services available to persons living in the European Union, and therefore we comply with the requirements of the GDPR: lawfulness, fairness and transparency of processing; lawful processing on one of the Article 6 GDPR bases; processing of special-category data only on one of the Article 9 GDPR bases; effective exercise of data subject rights; data-protection impact assessments

where necessary; the seventy-two-hour breach-notification procedure; appropriate safeguards for international transfers; and a record of processing activities under Article 30 GDPR.

12.2 Cypriot data protection law compliance

As a Cypriot company, we comply with Cypriot Law 125(I)/2018 on the Protection of Natural Persons with regard to the Processing of Personal Data and we cooperate with the Office of the Commissioner for Personal Data Protection of the Republic of Cyprus.

12.3 Compliance with other regional laws

We monitor relevant data-protection laws in jurisdictions where the Platform is available and update our practices accordingly. Specific regional notices, where applicable, may be published as appendices to this Privacy Policy.

13. Transparency and reporting

13.1 Data Protection Officer

We have appointed a Data Protection Officer (DPO) under Article 37 GDPR, on the basis that our core activities include the processing of special-category data on a large scale and the regular and systematic monitoring of data subjects. The DPO oversees compliance with data-protection rules, serves as the contact point for data subjects and supervisory authorities, provides regular training, coordinates DPIAs, and oversees breach management. The DPO can be reached at legal@bootyn.com.

13.2 Transparency reports

We are committed to transparency. We publish an annual transparency report covering: the number and type of valid notices received under Article 16 of the DSA; statements of reasons issued under Article 17 of the DSA; outcomes of internal complaints under Article 20 of the DSA; orders received from authorities under Articles 9 and 10 of the DSA; aggregated statistics on data-protection requests; and aggregated statistics on data breaches.

13.3 Public data-protection commitment

We commit to a high level of data protection: we regularly review and improve our practices, are open to user feedback, proactively adapt to the changing regulatory environment, and cooperate with industry initiatives in data protection.

14. Final provisions

14.1 Modification of the Privacy Policy

We reserve the right to modify this Privacy Policy. Modifications take effect upon publication on the Platform. For substantive changes:

- we notify registered Users by email;
- we display prominent notifications on the Platform;
- we make previous versions available on request;
- we provide a thirty (30) day transition period for material changes.

14.2 Contact

For data-protection matters, you may contact us at:

- Data protection / DPO: legal@bootyn.com
- General customer service: support@bootyn.com
- Financial matters: finance@bootyn.com
- Postal: SPONDEX LTD — Privacy, Voukourestiou 25, NEPTUNE HOUSE, 1st floor, Flat/Office 11, Zakaki, 3045 Limassol, Cyprus

We respond to all inquiries within thirty (30) days.

14.3 Effective date

This Privacy Policy enters into force on April 7, 2026 and remains in force until revoked or replaced. From the effective date, all previous versions cease to apply.

Bootyn.com Platform Privacy Policy

Last updated: April 28, 2026 | Version 1.1