

YOUNITHUB.COM PRIVACY POLICY

Free Version | Platform for Creators and Communities

Version 1.0 | 17 July 2026 | Polish law and the GDPR | effective from the date of publication

IMPORTANT INFORMATION

Younithub.com is currently an entirely free-of-charge platform. It does not support purchases, sales, payments, withdrawals, wallets, tokens, NFTs or blockchain transactions; therefore, the Controller does not collect payment card, bank account, wallet or settlement data. The Platform is intended for adults. The Controller does not sell personal data. Optional analytics, marketing or other technologies that are not necessary to provide the requested service may operate only after the required consent has been obtained.

This summary does not replace the full Policy. Detailed information about the data, purposes, legal bases, recipients, retention periods and rights is provided below.

1. Data Controller and contact details

The controller of personal data processed in connection with the website <https://younithub.com/> is KAMLER Spółka z ograniczoną odpowiedzialnością, with its registered office at ul. Stanisława Wyspiańskiego 25, 87-100 Toruń, Poland, entered in the Register of Entrepreneurs of the National Court Register under KRS number 0000582381, Tax Identification Number (NIP) 9562313938 and National Business Registry Number (REGON) 362820375 (the "Controller" or the "Operator").

Contact for privacy matters and the exercise of rights: kamlerspzoo@gmail.com. Reports of security incidents: kamlerspzoo@gmail.com.

Data Protection Officer

The Controller has not appointed a Data Protection Officer. For all matters concerning the processing of personal data and the exercise of rights under the GDPR, you may contact the Controller directly by email at kamlerspzoo@gmail.com or by post at: ul. Stanisława Wyspiańskiego 25, 87-100 Toruń, Poland.

Roles of Creators, studios and teams

The Controller determines the purposes and means of processing the data required for the operation of the Platform. A Creator, studio or team may be a separate controller of data that it independently collects for its own Project, collaboration, production or activities outside the Platform. In such a case, it is responsible for establishing its own legal basis and providing the required privacy information. If the parties jointly determine the purposes and means of a specific processing activity, they will provide data subjects with the essential information about their joint-controller arrangement.

2. Scope of the Policy and definitions

This Policy applies to the personal data of visitors to the Platform, Account holders, Fans, Creators, members of studios and teams, persons identifiable in Content, persons submitting reports and persons contacting the Operator. It covers both use without an Account and functions available after registration.

Capitalised terms have the meanings assigned to them in the YounitHub.com Terms and Conditions.

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council, "EEA" means the European Economic Area, and "PKE" means the Polish Act of 12 July 2024 - Electronic

Communications Law. "Depicted Person" means a person whose image, voice, name, role, statement or other personal data appears in Content or in a Project description.

A shorter layered notice may be displayed in connection with a specific function to supplement this Policy, for example before an identity verification process begins or before consent to cookies is requested. This Policy does not cover processing by external services accessed through a link; those entities apply their own privacy rules.

3. Data processing principles

The Controller processes personal data in accordance with the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability. The scope of personal data is limited to what is appropriate for the function that is actually made available.

- privacy and visibility settings limit personal data by default to the scope required for the selected function;
- access by employees, contractors and service providers is restricted according to their role and need to perform a task;
- the Controller does not sell or rent personal data or disclose it in exchange for a share of revenue;
- the free-of-charge nature of the Platform does not mean that personal data may be treated as an unrestricted means of payment - every processing activity requires its own legal basis;
- a new purpose, a new category of data or a materially different technology requires a prior assessment and the provision of appropriate information.

4. Personal data we may process

The scope depends on how the Platform is used and may include:

- **Visitor data** - IP address, approximate region derived from the IP address, device type, operating system, browser, language, technical identifiers, referring page, request time, pages visited, and error and security logs.

- **Account data** - email address, username, cryptographic password hash, language, settings, Account status, login history, records confirming acceptance of documents, and multi-factor authentication data if that function is available.
- **Community activity** - Creators followed, reactions, comments, survey responses, searches, views, saved preferences and other interactions, if the relevant functions are available.
- **Creator application** - information about the profile, body of work, studio or team, planned Content and Projects, role, rights to materials, business status and the history of the application review.
- **Age or identity verification** - declaration of legal age, 18+ result, full name, date of birth, country, limited document data, verification photograph or recording, comparison result and verification history - only where a given method is actually used, necessary and described before the process begins.
- **Studio or team data** - name, description, members, roles, business contact details, permissions for a team Account and identification of the responsible adult.
- **User Content** - profile, avatar, description, videos, photographs, music, podcasts, texts, graphics, educational materials, Project descriptions, comments and messages, if the relevant function is available, together with file metadata, upload date and visibility setting.
- **Data of Depicted Persons** - image, voice, name, pseudonym, role, authorship or contribution to a Project and, where required, a record of consent, licence or another legal basis for publication.
- **Reports, moderation and security** - reported Content, reason for the report, evidence, reporter details, decisions and reasons, appeals, restrictions, infringement identifiers and communications with individuals and competent authorities.
- **Contact and exercise of rights** - name, organisation name, email address, correspondence, attachments, information needed to verify identity and case history.
- **Cookies and similar technologies** - session identifiers, preferences, consent status and history and, after the required consent has been obtained, analytics or marketing data described in the cookie settings panel.

No payment or blockchain data

The Platform currently does not support purchases, sales, payments, tips, funding, withdrawals, wallets, tokens, NFTs or Smart Contracts. The Controller does not request payment card numbers, bank account numbers, Wallet addresses, private keys, seed phrases, transaction signatures or settlement histories. Such information must not be included in profiles, comments, Content or correspondence.

If a person submits such data without being asked, the Controller will restrict its further processing or delete it unless the minimum necessary scope must be retained to investigate fraud, a security incident, a legal violation or a claim.

Special categories of personal data

The Platform does not require the disclosure of data concerning health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or sexual orientation. Content, a profile or activity may nevertheless indirectly reveal such information. A User should not post such information unless doing so is necessary and lawful.

Where the Controller intentionally processes special categories of personal data, it applies an appropriate condition under Article 9(2) of the GDPR, in addition to a legal basis under Article 6, and implements additional safeguards. Deliberately making specific information public does not constitute consent to the unrestricted use of other personal data. Special category data is not used for behavioural advertising or for training general-purpose models.

5. Sources of personal data

Personal data may be obtained:

- directly from the data subject when visiting, registering, publishing, applying to the Creator programme, undergoing verification or contacting the Operator;
- from the device and the way in which the Platform is used, including logs, cookies, session events and security events;
- from a Creator, studio or team when they provide the personal data of a team member, co-creator or Depicted Person, provided that they have a legal basis and provide the information required by law;
- from an external verification provider if such a service is actually implemented and the person starts the process;
- from other Users, reporters or rights holders when they report Content, an Account, a legal violation or a threat;
- from public registers or publicly available sources solely to the extent necessary to confirm a Creator's identity, rights to Content, professional status or protection against abuse;
- from technical service providers, professional advisers or competent authorities where lawful and necessary for a specific purpose.

Where personal data has not been obtained directly from the data subject, the Controller provides the information required by Article 14 of the GDPR within a reasonable period and no later than one month after obtaining the data, at the first communication or before the first disclosure, whichever occurs first, unless the person already has the information or a specific legal exception applies.

6. Purposes and legal bases of processing

Each purpose has its own legal basis. The indication of several legal bases does not mean that they are applied interchangeably; each basis applies only to the corresponding scope of a processing activity.

Purpose	Scope	Legal basis
Public part of the website and technical security	Device, connection, log and diagnostic data, protection against attacks and maintenance of availability.	Article 6(1)(f) GDPR - legitimate interest in providing a secure public part of the Platform; Article 6(1)(c) - where a specific legal security obligation applies.
Account and community functions	Registration, login, settings, Following, comments, surveys, notifications and Account closure support.	Article 6(1)(b) GDPR - entering into and performing the free-of-charge contract under the Terms and Conditions; Article 6(1)(f) - service integrity and prevention of abuse.
Creator status and verification	Assessment of the application, legal age, identity, rights to Content, role and professional status; renewed verification where justified by risk.	Article 6(1)(b) GDPR - steps before granting status and performance of publishing conditions; Article 6(1)(f) - trustworthiness and security; Article 6(1)(c) - only where a specific obligation arises from law.
Publishing and presentation of Projects	Hosting, formatting, thumbnails and display of profiles, Content, Project stages and co-creator data to the intended audience.	Article 6(1)(b) GDPR - performance of the function selected by the User; Article 6(1)(f) - provision of the public Platform and protection of rights. Consent applies where it is the appropriate basis for a specific image or item of personal data.
Moderation, reports and appeals	Detection of violations, receipt of reports, examination of evidence, reasons for decisions, appeals and cooperation with authorities.	Article 6(1)(c) GDPR - legal obligations, including those relating to digital services; Article 6(1)(b) - enforcement of the Terms and Conditions; Article 6(1)(f) - security and protection of rights.
Recommendations and personalisation	Profiles followed, interactions, language, region, recency, quality and security signals used to determine the order of Content.	Article 6(1)(b) GDPR - provision of the selected function; Article 6(1)(f) - relevance, quality and security of recommendations. Special-category personal data is not used for behavioural advertising.
Contact, complaints and data subject rights	Correspondence, case identification, proportionate identity verification, response and evidence of handling.	Article 6(1)(b), (c) or (f) GDPR - depending on whether the matter concerns a contract, legal obligation, handling of an enquiry or protection of claims.

Purpose	Scope	Legal basis
Optional cookies, analytics and marketing	Data activated only after the user's selection in the consent panel; email marketing only after separate consent if introduced.	Article 6(1)(a) GDPR - consent; Article 399(1) PKE for optional technologies; Article 398 PKE for commercial information sent by electronic means.
Claims, audit and compliance	Records of decisions, consents, incidents, requests, disputes, inspections and corporate transactions concerning the Operator's activities.	Article 6(1)(c) GDPR - legal obligation; Article 6(1)(f) - demonstration of compliance and establishment, exercise or defence of legal claims.

Is providing personal data mandatory?

Technical data necessary for connectivity and security is transmitted automatically; without it, the Platform may not operate. Providing Account data is voluntary but necessary to create an Account. Data required in the Creator application form is necessary to review the application and provide publishing tools. Refusal to provide it results in the relevant function being unavailable, not in a fee being charged.

Fields marked as optional and consents to analytics, optional technologies or marketing are voluntary. Failure to provide them or withdrawal of consent does not restrict basic functions that do not depend on that data.

7. Adults and Creator verification

User Account

The Platform is intended for persons who are at least 18 years old. At registration, the Controller may request a declaration that the person is of legal age. Additional confirmation of age or identity may be requested only where justified by security, a suspected violation, the protection of individual rights or a specific legal obligation.

Application and Creator status

Creator verification may include confirming legal age, identity, role, business status and rights to Content. Before the process begins, the Platform identifies the method actually used, the name and role of the provider, the scope of data, purpose, legal basis, retention period, any transfers outside the EEA and the method for challenging an incorrect result.

Wherever possible, the Controller retains a verification result or a limited verification token instead of a full copy of an identity document. A document, photograph or recording may not be used for advertising, unrelated facial recognition or training general-purpose models.

Biometric data and high-risk processing

A photograph or recording becomes special-category biometric data where it is subject to specific technical processing for the purpose of uniquely identifying a person. Such processing may be implemented only after necessity has been demonstrated, legal bases under Articles 6 and 9 of the GDPR have been established, appropriate safeguards have been applied and a data protection impact assessment has been carried out where required by Article 35 of the GDPR. This Policy does not itself constitute consent to biometric processing.

An incorrect result may be reported by email to: younithub@gmail.com.

If an automated result materially restricts access, the Controller provides human review or identifies an available appeal procedure offered by the provider.

8. Public visibility of Content and personal data of other persons

A username, avatar, description, Creator profile, public Content, comments, list of co-creators and Project information may be visible to an unlimited audience and indexed by search engines. Copies may remain in a search engine cache or may have been made by third parties even after the material has been removed from the Platform.

Before publishing, the User should check the intended audience and should not post personal data that they do not wish to disclose. Messages to a specified recipient, where this function is available, are not public; the Operator accesses them only to the extent necessary for delivery, security, moderation, handling a report or compliance with a legal obligation.

A Creator who publishes personal data of a Depicted Person must have an appropriate legal basis, provide the required privacy information and respect an objection, withdrawal of consent or other rights to the extent applicable to the relevant legal basis. The Controller may request proportionate evidence of authorisation or restrict the material while the matter is being clarified.

9. Recommendations, profiling, moderation and artificial intelligence

The order of Content may take account of recency, popularity, Following, interactions, language, approximate region, compliance with the Terms and Conditions and security signals. The purpose is to display useful Content and limit abuse, not to infer sensitive characteristics for advertising.

Automated tools may assist in detecting spam, fraud, impersonation, infringement of rights, dangerous Content or circumvention of safeguards. A result may flag a matter for review or support a moderation decision. The Controller does not make a decision based solely on automated processing that produces legal effects or similarly significantly affects a person unless permitted by Article 22 of the GDPR and the required safeguards, including human intervention and the ability to challenge the result, have been implemented.

The Controller does not use private messages, verification documents or User Content to train external general-purpose artificial intelligence models without prior notice and a separate valid legal basis. A tool provider may not use personal data for its own model training unless this has been expressly disclosed and properly regulated.

10. Cookies and similar technologies

The Platform does not currently use cookies, local storage, pixels or similar technologies.

11. Recipients of personal data

To the extent necessary for a specific purpose, personal data may be received by:

- **Other Users and members of the public** - to the extent resulting from the selected visibility setting for a profile, Content, comment, team or Project.
- **Service providers acting on the Controller's behalf** - hosting, cloud services, CDN, storage and delivery of Content, email, report handling, security, backups, consent management, moderation, consent-based analytics and age or identity verification, if implemented.
- **Independent controllers** - search engines indexing public pages, a verification provider to the extent that it independently determines purposes and means, professional advisers, insurers, courts, supervisory authorities and law enforcement authorities.
- **A legal successor or participant in a corporate transaction** - subject to confidentiality, minimisation and safeguards in connection with a reorganisation, merger, sale of a business or another lawful transfer of operations.

Processors act on documented instructions, under a contract and subject to confidentiality and security obligations.

The current model does not require a payment service provider, bank, crypto-asset exchange or Wallet provider. The Controller does not disclose personal data to public authorities through voluntary bulk cooperation; it responds to lawful and proportionate requests.

12. Transfers of personal data outside the EEA

The Controller aims to process personal data within the EEA. If a service provider or recipient processes personal data outside the EEA, the transfer is based on a European Commission adequacy decision or appropriate safeguards such as Standard Contractual Clauses or Binding Corporate Rules. A derogation under Article 49 of the GDPR is used only exceptionally and within the limits of the law.

13. How long we retain personal data

Personal data is retained no longer than required by the purpose, a legal obligation, security needs or the protection of claims. The applicable periods and criteria are set out below; before publication, they must reflect the actual configuration of the systems.

Category	Retention period or criterion
Visit, error and security logs	As a rule, for up to 12 months. Data connected with an incident, fraud or proceedings may be retained for longer, until the matter is concluded and the applicable limitation period for claims expires.
Account data and settings	For the lifetime of the Account. After closure, deletion or anonymisation in active systems generally takes place within 30 days; backups may be overwritten within up to 90 days. Minimal records concerning violations or claims may be retained for longer.
Creator application and verification	An unsuccessful or incomplete application - generally for up to 12 months. Data of an active Creator - for the duration of the status and up to 3 years after it ends. A copy of a document or recording is deleted earlier where the verification result is sufficient; longer retention applies only where required by an obligation, dispute or risk.
User Content and Projects	Until deletion by the User or Operator or closure of the Account. Backups may remain for up to 90 days without ordinary public access. Content preserved as evidence is retained for the period required by the matter or by law.
Community activity	Until the specific interaction is deleted, the Account is closed or the need connected with the function ceases. Effectively anonymised and aggregated data may be retained for longer.
Reports, moderation and appeals	As a rule, for 3 years after the matter is closed. Data required by an order or proceeding, or needed to prevent repeated serious abuse, may be retained for a proportionately longer period.
Correspondence and data subject requests	As a rule, for 3 years after the matter is closed in order to demonstrate that it was handled correctly, unless the law or an ongoing dispute requires a different period.
Cookies and evidence of consent	Cookies - for the period indicated in the consent panel. Evidence that consent was given or withdrawn - for the period required to demonstrate compliance, generally up to 3 years after consent expires or is withdrawn.
Marketing and suppression list	Marketing data - until consent is withdrawn or an objection is made. A minimal record of the objection may be retained for longer solely to ensure that no further communications are sent.

After the applicable period expires, personal data is deleted, anonymised or isolated until a backup is securely overwritten. The Controller documents the reason for applying an exception to the ordinary retention period.

14. Rights of the data subject

Subject to the conditions and limits set out in the GDPR, a person may request:

- access to personal data, information about its processing and a copy of the data;
- rectification of inaccurate personal data and completion of incomplete personal data;
- erasure of personal data where there is no longer a lawful basis for its processing;
- restriction of processing in the circumstances specified in the GDPR;
- portability of personal data provided to the Controller where processing is automated and based on consent or a contract;
- the right to object, on grounds relating to their particular situation, to processing based on legitimate interests;
- the unconditional right to object to direct marketing, including related profiling;
- withdrawal of consent at any time, without affecting the lawfulness of processing carried out before its withdrawal;
- the right not to be subject to a decision based solely on automated processing where it produces legal effects or similarly significantly affects the person, subject to the exceptions and safeguards in Article 22 of the GDPR;
- the right to lodge a complaint with the competent supervisory authority and to seek a judicial remedy.

These rights are not absolute. Erasure or access may be restricted, among other reasons, because of a legal obligation, the rights and freedoms of other persons, freedom of expression, security or the establishment, exercise or defence of legal claims. The Controller explains the basis for any full or partial refusal.

15. How to exercise your rights

A request may be sent to younithub@gmail.com with the subject line "PRIVACY". The request should identify the Account, profile, Content or other information necessary to locate the personal data and should describe the request precisely. If the function is available, selected personal data may be corrected or deleted directly in the Account settings.

Where there are reasonable doubts concerning identity, the Controller may request only the additional information necessary to confirm it. A full identity document should not be sent unless it has been expressly requested through a secure channel.

The Controller responds without undue delay and, as a rule, within one month. This period may be extended by a further two months due to the complexity or number of requests; information about the extension and the reasons for it is provided within the first month. Requests are handled free of charge, except in cases that are manifestly unfounded or excessive as provided by law.

16. Security and personal data breaches

The Controller applies technical and organisational measures appropriate to the risk, including role-based access controls, confidentiality, encryption in transit, secure password hashing, multi-factor authentication where appropriate, event logging, backups, vulnerability management, separation of verification documents from profiles and reviews of service providers and permissions.

No system can guarantee complete security. The User should use a unique password, protect their device, log out of shared equipment and never disclose codes, login links, private keys or seed phrases. A suspected Account compromise or disclosure of personal data should be reported to: younithub@gmail.com.

The Controller assesses every personal data breach. If a breach is likely to result in a risk to the rights or freedoms of individuals, the Controller notifies the supervisory authority without undue delay and, where feasible, no later than 72 hours after becoming aware of it. Where a high risk is likely, the Controller informs the affected person without undue delay unless a statutory exception applies.

17. Minors

Accounts, Creator status and community functions are intended for persons who are at least 18 years old. The Controller does not intend to knowingly register minors. A credible report concerning an Account held by a person under 18 may result in access restrictions, verification, deletion of personal data or another measure required to protect that person.

Creative Content may exceptionally include a minor's personal data or image only where the Creator has an appropriate legal basis, has fulfilled the applicable information obligations and has taken the best interests of the child into account. The Controller may apply additional visibility restrictions, request evidence of authorisation or remove the material if its publication creates a risk.

A parent, guardian or another person may report a concern to: younithub@gmail.com. The Controller may request proportionate evidence of authority and will not disclose Account data to the reporting person without a proper legal basis.

18. Complaint to a supervisory authority

A person may lodge a complaint with the supervisory authority competent for their habitual residence, place of work or place of the alleged infringement. In Poland, this is the President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych), Personal Data Protection Office, ul. Stanisława Moniuszki 1A, 00-014 Warsaw, <https://uodo.gov.pl/>. Lodging a complaint does not affect the right to a judicial remedy.

19. Future Web3 and blockchain functions

Descriptions of community funding, tokenised memberships, NFTs, Smart Contracts, on-chain ownership, withdrawals or revenue sharing currently describe only a possible direction of future development. On this basis, the Platform does not collect Wallet addresses, transaction identifiers, KYC or AML data or other blockchain data.

Before launching a function that uses blockchain technology, the Controller will define the roles of participants, on-chain and off-chain data flows, purposes, legal bases, recipients, transfers and retention periods, carry out any required impact assessment and provide a separate or updated notice. The assessment will take account of the public and potentially immutable nature of the ledger, data subject rights and data minimisation; directly identifying personal data and verification documents will not be stored on a public blockchain.

Acceptance of this Policy or the Terms and Conditions does not constitute consent to future blockchain processing. If consent is required, it will be obtained separately before processing begins. The Operator never requests a Wallet private key or seed phrase.

20. Changes to the Policy

The Controller may update this Policy due to changes in law, functions, service providers, risks or processing practices. The current version is published with its version number and effective date. Account holders are informed appropriately of a material change before it takes effect, unless an immediate change is required by law or for security reasons.

Continued use of the Platform does not replace consent required for a new purpose, optional cookies, marketing, biometric processing or another operation based on consent. An amendment to the Policy cannot legitimise prior unlawful processing.

21. Final provisions

This Policy describes the current, entirely free-of-charge stage of YunitHub.com. It does not cover paid, transactional, crowdfunding, token or blockchain functions that have not been launched. The scope of processing must be reassessed before any such function is launched.

This Policy is governed by the GDPR, the Polish Personal Data Protection Act, the Electronic Communications Law and other applicable laws. The English version is intended for international users. Any translation must convey the same information; mandatory law and data subject rights prevail.