Safety protocols

Version: v1-2026-10-15 | Updated: 2026-10-15

Prohibited activities: prevention and response protocols

RentDate is an adults-only social and dating platform. Human trafficking, sexual exploitation, paid sexual services, illegal activity, misleading impersonation and child sexual abuse material (CSAM) are prohibited. These are the Operator’s operating procedures, read together with the Terms of Service, particularly sections 4-5, 7, 11-12 and 18-24. The Operator, Maciej Waśkiewicz, is responsible for handling safety cases and the restricted moderation queue. Contact: kontakt@rentdate.pl.

1. Reporting, triage and records

Users can report accounts, profiles, photos, posts and individual private messages through the available reporting features. Anyone, including a person without an account, can email kontakt@rentdate.pl. Identify the profile or content, explain the concern and include the relevant date and identifiers if available. Do not send passwords, payment-card data or copies of suspected CSAM.

The Operator reviews the available account, content and transaction context. In-app reports and automated violation signals enter an access-controlled moderation queue; suspected minors, illegal activity and sexual-service offers can be prioritised using the existing report categories. Email reports are handled by the Operator and recorded in the case record or moderation queue as appropriate. A reported private message is captured by the server for review; we do not continuously screen all private conversations.

The case record should identify the report or signal, affected account and content identifiers, time, assessed risk, reviewer, action and reason, any payment restriction, referral to authorities and outcome of an appeal. Records and access are limited to what is necessary for safety, legal duties and legitimate case handling under the Privacy Policy. Available evidence is preserved where lawful; not every rejected upload or deleted item remains recoverable.

Credible risks to a child, coercion, trafficking, serious violence or exploitation require priority human assessment and proportionate protective restrictions while the facts are checked. Confirmed serious violations may lead directly to a permanent ban. Automated text or image signals alone do not establish guilt. The Operator reviews challenges at kontakt@rentdate.pl under Terms sections 21-22.

This is not an emergency channel and there is no continuous 24/7 monitoring commitment. Contact local emergency services immediately if someone is in immediate danger; in Poland and the EU, call 112.

2. Human trafficking and sex trafficking

Prevention: the Terms prohibit human trafficking, coercion, exploitation, escort and paid sexual services, sexual sponsorship and exchanging money, gifts, accommodation or other benefits for sexual acts. The prohibition covers public content, private messages, coded offers and attempts to move prohibited arrangements off-platform. Registration requires an adult date of birth and an explicit 18+ declaration; this is not universal identity-document verification.

Identification: selected Polish and English public-text rules block some sexual-service, trafficking and threat signals before publication and create a moderation case. New profile photos are screened for general explicit-content and violence signals before approval. Reports are reviewed for coercion, threats, a third party controlling another person’s profile or earnings, recruitment or travel offers linked to sexual exploitation, and similar indicators. These contextual checks are manual; the filters do not identify every trafficking scenario.

Response: the Operator assesses credible concerns as a priority, restricts the account and removes or hides the relevant content when necessary to limit exposure, preserves available lawful account, report, message and payment records and checks linked accounts or transactions where the information supports doing so. Confirmed involvement results in a permanent ban. The Operator refers suspected crimes and immediate threats to competent authorities where required by law or otherwise lawfully justified, using the law-enforcement request procedure. Users are not asked to investigate or confront a suspected trafficker.

3. Illegal acts

Prevention and identification: the Terms prohibit unlawful offers, fraud, phishing, account takeover, extortion, threats, violence, exploitation and payment manipulation. Selected public Profile fields, availability notes, posts and replies are validated on the server using Polish and English violation rules. New profile images remain pending until an acceptable SafeSearch result is returned; incomplete results and service errors do not approve publication. Users can report conduct or individual messages, and the Operator reviews relevant account, content and transaction records.

Response: the Operator evaluates the report and its context, restricts or bans responsible accounts and removes or hides violating content as appropriate. Serious risk can justify immediate restriction without first issuing a warning. New meeting checkout and the release of held meeting funds include checks of the recipient’s account restrictions. Disputed or suspicious settlements are handled with the payment provider under the Terms; a hold is not automatic forfeiture of money. Earlier payment links and transfers require separate review and are not automatically recalled by an account ban.

The Operator records the reason and action, preserves available relevant records where lawful and notifies competent authorities when required or otherwise lawfully justified. Affected users receive reasons and an email appeal route subject to legal limits on disclosure. A good-faith complaint or chargeback is not itself a violation.

4. Impersonation

Prevention: the Terms require truthful account details and prohibit stolen photographs, unauthorised use of another person’s identity, account sharing, deceptive fake accounts and evasion of bans. Registration uses email verification and an age declaration. Email verification establishes control of an inbox; it does not establish legal identity, ownership of every photograph or adulthood. Payment-provider KYC applies where required for payouts and is not a universal profile verification badge.

Identification: users can report impersonation, stolen images or account takeover. The Operator checks the reported profile, the ownership claim, inconsistencies and available account and moderation history, and may request only the clarification necessary to resolve the concern. Sensitive identity documents must not be posted publicly or sent in ordinary user chat; any document-based check needs a separately arranged secure channel. We do not claim automated reverse-image matching or identity-document verification for every user.

Response: credible impersonation or takeover concerns may lead to temporary restrictions while reviewed. Confirmed impersonating accounts or unauthorised content are removed or banned, and account recovery is handled only after the claimant’s authority is established. Decisions and reasons are recorded, with an appeal available by email.

RentDate’s own Platform Profiles are a separate, disclosed feature: they are labelled as platform-operated, may be handled by authorised staff, do not represent an independent real person available for an offline meeting and disclose this before paid chat access. They must not impersonate a real person without permission. Ordinary users are not permitted to create deceptive profiles under this exception.

5. Child sexual abuse material (CSAM)

Prevention: minors, photographs of minors, sexual exploitation of children and CSAM are prohibited. The backend rejects registration that fails the declared-date-of-birth and 18+ requirements. New profile photos are held from the approved gallery while Google Cloud Vision SafeSearch assesses general adult, racy and violence signals. Selected public-text rules also flag some underage admissions and prohibited offers.

Detection limits: declared age is not identity-document verification. SafeSearch is a general image-safety tool, not a dedicated CSAM hash-matching database, age-estimation system or proof of consent. RentDate has no dedicated CSAM-matching integration and does not claim that all harmful material is automatically detected. User reports and priority human review remain necessary.

Reporting and response: report the content location or account/message identifier through the reporting feature or kontakt@rentdate.pl; do not download, forward or attach suspected CSAM. The Operator treats credible child-safety concerns as a priority, restricts the account and access to the relevant content where necessary, and preserves available relevant records only as lawfully necessary, with limited access and no unnecessary copies of the material. The Operator assesses reporting to competent authorities and fulfils applicable

mandatory reporting and preservation duties. Suspected online child-abuse content can also be reported to NASK’s Dyżurnet.pl team through its official form. Immediate danger must be reported to emergency services.

Confirmed child-exploitation or CSAM violations result in permanent removal of the responsible account. The Operator records actions and the legal basis for any disclosure. Account restrictions and content removal do not guarantee that every previously shared copy or storage link can be recalled; known exposure must be assessed and addressed as part of the incident.

6. Review of the protocols

The Operator reviews these procedures after a material incident or a relevant change in features, moderation tools, payment-provider requirements or law. Changes to public policies follow the Terms’ notice rules. This document describes available controls and the required human response; it does not promise universal identity checks, continuous human monitoring or guaranteed prevention of every violation.

Law-enforcement requests and preservation procedure

Contact point for competent authorities and legal requests: kontakt@rentdate.pl. Operator: Maciej Waśkiewicz, RentDate, Al. Grunwaldzka 116, 80-244 Gdańsk, Poland. Requests may be submitted in Polish or English. This procedure supplements Terms sections 20.9 and 24.6-24.8 and the Privacy Policy; it does not create unrestricted access to user data.

1. Information to include

Identify the requesting authority, officer or official, role, official contact details, case reference, jurisdiction and legal basis. Attach the relevant order or other legal instrument where applicable. Specify the accounts or content, the categories of records sought, the date range and time zone, the reason for the scope, the response deadline and any lawful confidentiality requirement. Provide available profile URLs, user, message, conversation, Meeting or transaction identifiers; do not include unnecessary sensitive material.

For urgent safety matters, describe the specific threat, persons at risk and why delay creates an immediate risk. An urgent subject line alone does not establish a lawful basis for disclosure. This email address is not continuously monitored and does not replace emergency services.

2. Verification and assessment

The Operator checks the authority, authenticity, applicable jurisdiction, legal basis and scope of the request. Identity and contact details are verified independently through official sources rather than relying solely on a reply address or links supplied in the request. Ambiguous, excessive or unsupported requests are clarified or challenged as appropriate; records are not disclosed solely on an unverified assertion of authority.

Each disclosure must be required by law or otherwise legally permitted and necessary for the specific proceeding, protection of rights or safety. The Operator limits disclosure to relevant data in its possession, subject to applicable legal safeguards. A request does not provide direct access to the database or another user’s account.

3. Preservation and secure disclosure

Where legally required or otherwise lawfully justified, the Operator preserves available relevant account information, reports, messages, logs and transaction records within the scope and period appropriate to the request and applicable law. Preservation does not mean that disclosure is automatically authorised. Data that was never collected or is no longer available cannot be reconstructed on demand; not every rejected upload is retained.

Only authorised persons handle the request. Before transferring sensitive records, the Operator verifies the recipient and agrees an appropriate secure delivery method. Copies, access and retention are limited to what is needed. Passwords, authentication secrets or unrestricted database credentials are not a response mechanism.

4. Decision records, notices and reporting

The Operator records the request, verification, legal basis, scope, preservation decision, action taken, date, authorised recipient and any disclosure restrictions. Users are informed where required and permitted by law; a notice is not sent where legally prohibited or where an applicable lawful exception requires otherwise.

Where facts trigger a mandatory crime, child-safety or other legal reporting duty, the Operator notifies the competent authority and supplies only the relevant lawful information. This procedure does not promise a fixed response time or a particular foreign reporting integration. Requests are assessed according to urgency and applicable deadlines.

Public documents and reporting channel

https://www.rentdate.pl/legal/prohibited-activities

https://www.rentdate.pl/legal/law-enforcement

https://dyzurnet.pl/formularz-zgloszeniowy