

Acceptable Use Policy

Version 1.1 | Effective 10 September 2026 | <https://prduct.com/acceptable-use>

Replaces the Acceptable Use Policy (15 November 2025).

Product ApS

Last Updated: 10 September 2026

1. PURPOSE

1.1 This Acceptable Use Policy ("AUP") defines permitted and prohibited uses of the Product Platform. It is incorporated into the Terms of Use and the Subscription Agreement.

1.2 Violation of this AUP may result in immediate suspension or termination of your access to the Platform.

2. PERMITTED USES

2.1 You may use the Platform for lawful business purposes, including: managing product data and specifications; tracking regulatory compliance (EUDR, REACH, etc.); collaborating with suppliers and customers in your supply chain; generating compliance reports and analyses; integrating the Platform with your own systems via API where your subscription permits.

3. PROHIBITED ACTIVITIES

3.1 Illegal activities. You may not use the Platform in violation of applicable law, to facilitate illegal activities, to violate export controls or sanctions, to infringe intellectual property rights, or to violate data protection law.

3.2 Security. You may not upload malicious code; attempt unauthorised access to the Platform, other accounts or our systems; interfere with the Platform's integrity or performance; bypass security or authentication; scrape or harvest data with automated tools without authorisation; probe or test vulnerabilities; or conduct penetration testing without prior written approval.

3.3 Reverse engineering. You may not reverse engineer, decompile or disassemble the Platform, derive source code or algorithms, create derivative works, or remove proprietary notices or security features.

3.4 Unauthorised distribution. You may not resell, sublicense, rent, lease or distribute the Platform; provide Platform access to third parties as a service, except connections permitted under Terms of Use Section 15; use the Platform to develop or support a competing product; or share login credentials.

3.5 Content. You may not upload or transmit unlawful, harmful, threatening, abusive or harassing content; defamatory or fraudulent content; content infringing intellectual property rights; pornographic or obscene content; spam or unsolicited communications; or false or misleading information.

3.6 Resource abuse. You may not place excessive load on our systems, send mass invitations without notice under Section 4, perform bulk operations that disrupt other users, generate excessive API calls with automated scripts, or intentionally consume excessive storage or bandwidth.

4. SYSTEM LOAD MANAGEMENT

4.1 You must notify support@prduct.com at least 48 hours in advance of: sending invitations to 100+ suppliers simultaneously; bulk uploading 1,000+ products; bulk updating 500+ records; or any other extraordinary system load.

4.2 If you perform high-load activities without notice, we may throttle your requests, temporarily suspend your account, or contact you to reschedule the activity.

5. DATA QUALITY

5.1 You are responsible for ensuring that data you submit is accurate, complete and up to date, lawfully obtained, and that you hold the rights to upload it.

5.2 You may not upload knowingly false or misleading product data; data that violates confidentiality obligations to third parties; Personal Data except as permitted by the Data Processing Agreement; classified or sensitive government information; or data obtained through illegal means.

5.3 You must only upload Personal Data as permitted in the Data Processing Agreement, ensure a lawful basis for it, comply with data protection law, and not upload special categories of Personal Data unless explicitly agreed.

6. ACCOUNT SECURITY

6.1 You must use a strong, unique password (minimum 12 characters), enable two-factor authentication where available, never share your password, and change it immediately if compromised.

6.2 You must monitor your account for unauthorised activity, notify security@prduct.com immediately of any security breach, and promptly remove access for former employees and contractors.

6.3 You are responsible for all activities under your account, including by your employees, contractors, anyone you have granted access, and unauthorised users who gained access due to your security failures.

7. REPORTING VIOLATIONS

7.1 Report suspected violations to abuse@prduct.com with details, evidence, dates and affected users. We investigate all reports and may warn, suspend or terminate the violating user, report illegal activity to authorities, or take legal action.

8. CONSEQUENCES OF VIOLATION

8.1 If you violate this AUP, we may: issue a warning and require remediation; temporarily suspend your access; permanently terminate your account; delete violating content; report illegal activity to law enforcement; pursue legal remedies; and, for Customers with a Subscription Agreement, refuse refunds in accordance with that agreement.

8.2 Minor violations: warning and 14 days to cure. Serious violations: immediate suspension and 7 days to cure. Critical violations (security breaches, illegal activity, malware): immediate permanent termination.

8.3 We are not obliged to monitor user activity but may investigate suspected violations.

9. COOPERATION WITH AUTHORITIES

9.1 We cooperate with law enforcement investigating illegal activity conducted through the Platform and may disclose user information when required by law or court order, or where we believe in good faith that

disclosure is necessary to comply with legal obligations, protect our rights or property, prevent fraud or illegal activity, or ensure Platform security.

10. CHANGES

10.1 We may update this AUP to address new security threats, legal requirements or Platform changes. Changes are notified and take effect in accordance with Terms of Use Section 17 and Subscription Agreement Section 12.

11. CONTACT

General questions: support@prduct.com

Violations: abuse@prduct.com

Security: security@prduct.com