DE/EU — Nutzungsrichtlinie (AUP) sowie Sicherheits- und Missbrauchsrichtlinie (EU/DE)

Datum: 12.02.2026
Letztes Update: 17.02.2026

Diese Nutzungsrichtlinie („AUP“) definiert erlaubte und untersagte Nutzungen von AILA sowie unseren Umgang mit Sicherheitsvorfällen und Missbrauch. Sie ergänzt insbesondere die **Nutzungsbedingungen & Software-Lizenz**, die **Abonnementbedingungen**, die **Key- & License Policy** sowie die **Datenschutzerklärung** und ist Bestandteil der AILA-Nutzungsbedingungen.

---

1) Anbieter / Kontakt (Abuse & Security)

Palindrom – Institution of Innovation LLC
Geschäftsanschrift (USA):
1007 N Orange St, 4th Floor Suite #5410
Wilmington, DE 19801
United States

Ladungsfähige Anschrift / Zustellanschrift (Deutschland):
M. Heigl
Anna-Ebermann-Straße 26
13053 Berlin
Deutschland

E-Mail (Allgemein/Legal): info@palindrom-ioi.com
E-Mail (Abuse/Security): info@palindrom-ioi.com
Website: institutionofinnovation.com

---

2) Geltungsbereich

1. Diese AUP gilt für Nutzer in Deutschland/EU sowie für alle AILA-bezogenen Online-Komponenten (Website, Account, Updates, Support, Lizenzvalidierung), soweit anwendbar.
2. Zwingende nationale Verbraucherschutz-, Datenschutz- und Produktsicherheitsvorgaben bleiben unberührt.
3. AILA ist local-first: Inhalte aus AILA-Chats, lokalen Dateien, Prompts, Konfigurationen oder Lernspeichern werden durch uns im Normalbetrieb **nicht erhoben** und **nicht zentral gespeichert** (siehe Datenschutzerklärung).

---

3) Warum dieses Dokument wichtig ist

AILA ist local-first und wird vom Nutzer typischerweise mit hohen lokalen Rechten betrieben (z. B. Konfiguration von Regeln, Policies oder Workflows in natürlicher Sprache). Wir haben **keine inhaltliche Kontrolle** über lokale Inhalte und erheben diese Inhalte nicht. Diese Architektur:
• entbindet Nutzer nicht von geltendem Recht,
• begrenzt aber unsere tatsächlichen Eingriffsmöglichkeiten in lokale Umgebungen.

Diese AUP schafft:
• klare Nutzungsgrenzen,
• ein verhältnismäßiges, abgestuftes Durchsetzungsmodell (insbesondere für Online-Leistungen),
• Schutz für Nutzer, Anbieter, Dritte und die Öffentlichkeit.

---

4) Definitionen

AILA / lokaler Betrieb
AILA läuft primär lokal. Nach Installation/Aktivierung kann AILA grundsätzlich offline starten und genutzt werden. Ohne Internet ist AILA funktional auf lokale Ressourcen beschränkt.

Online-Leistungen
Leistungen, die eine Online-Komponente voraussetzen (z. B. Account, Abonnementverwaltung, Updates, Support, Online-Validierung, Zugriff auf internetbasierte Quellen/Connectoren).

Missbrauch (Abuse)
Jede Nutzung von AILA, die gegen geltendes Recht, diese Richtlinie, Key- & Lizenzrichtlinie oder diese Nutzungsrichtlinie verstößt oder berechtigte Sicherheitsinteressen verletzt.

Hochrisiko-Nutzung
Nutzung mit erheblicher Gefahr für Leib oder Leben, kritische Infrastruktur, großskaligen Betrug oder schwere Cyberangriffe.

Lizenz / Key
Der AILA Key sowie die damit verbundene personenbezogene Lizenz und ggf. ein aktives Abonnement.

Tampering / Umgehung
Jede Manipulation oder Umgehung von Schutz-, Update-, Validierungs-, Lizenz- oder Sicherheitsmechanismen (z. B. Patchen von Checks, Key-Gen, Entfernen von Integritätsprüfungen).

---

5) Erlaubte Nutzung

Erlaubt ist insbesondere:

1. Rechtmäßige Nutzung für Produktivität, Analyse, Kreativarbeit, lokale Automatisierung und Bildung.
2. Nutzung im privaten oder unternehmerischen Umfeld, sofern rechtlich zulässig und intern geregelt.
3. Sicherheitsforschung ausschließlich
   – auf eigenen Systemen, oder
   – mit ausdrücklicher Genehmigung des jeweiligen Rechteinhabers
   (siehe Responsible Disclosure, Abschnitt 12).

---

6) Untersagte Nutzung (nicht abschließend)

Untersagt ist insbesondere:

1. Illegale Handlungen, Anstiftung, Beihilfe oder Planung von Straftaten.
2. Entwicklung, Einsatz oder Anleitung zu Malware, Exploits, Phishing, Credential Theft, Botnets oder Ransomware.
3. Gewaltförderung, Terrorismusunterstützung, ernsthafte Drohungen oder Aufrufe zu Gewalt.
4. Betrug, Identitätsdiebstahl, Umgehung von Zahlungs-, Abo- oder Lizenzsystemen sowie Chargeback-Betrug.
5. Umgehung oder Manipulation von Lizenz-/Aktivierungsmechaniken, personenbezogener Lizenzbindung sowie Update-, Integritäts- oder Sicherheitsmechanismen.
6. Unautorisierter Zugriff auf Systeme Dritter, Scans oder DoS/DDoS-Angriffe ohne Berechtigung.
7. Datenschutzverstöße oder unrechtmäßige Verarbeitung personenbezogener oder sensibler Daten.
8. Verletzung von Rechten Dritter (z. B. Urheberrecht, Geschäftsgeheimnisse), soweit die Nutzung rechtswidrig ist.
9. Verstöße gegen anwendbares Exportkontroll- oder Sanktionsrecht, soweit dies im konkreten Nutzungs- oder Lieferkontext rechtlich relevant ist.

---

7) Nutzer als Admin & lokale Änderungen

1. Nutzer dürfen AILA lokal konfigurieren (z. B. Regeln, Rollen, Workflows), soweit dies innerhalb der vorgesehenen Funktionen erfolgt.
2. Sicherheits-, Lizenz- oder Schutzmechanismen dürfen nicht deaktiviert, manipuliert oder umgangen werden.
3. Lokale Änderungen erfolgen auf eigenes Risiko und entbinden nicht von geltendem Recht, Key- & Lizenzrichtlinie und dieser AUP.

4. Eine bewusste Konfiguration zur Ermöglichung oder Förderung von Missbrauch gilt selbst als Verstoß.
5. Hinweis zur Eingriffsmöglichkeit: Da AILA local-first ist, können wir lokale Inhalte nicht „moderieren“ oder „entfernen“. Maßnahmen betreffen daher typischerweise Online-Leistungen, Abonnements und Lizenz-/Account-Status (siehe Abschnitt 8).

---

8) Durchsetzung (abgestuftes & verhältnismäßiges Modell)

Stufe 1 — Hinweis / Warnung
Information über den Verstoß und – sofern sinnvoll – Frist zur Korrektur.

Stufe 2 — Temporäre Einschränkung
Vorübergehende Einschränkung von:
• Account, und/oder
• Online-Leistungen (z. B. Updates, Support, Abonnementfunktionen, Online-Validierung), sofern dies zur Missbrauchsvermeidung, Sicherheit oder zur Aufklärung erforderlich ist.

Stufe 3 — Kündigung / dauerhafte Sperre
Bei schweren oder wiederholten Verstößen:
• Kündigung des Abonnements, und/oder
• Sperre oder Widerruf von Online-Leistungen und/oder Lizenz-/Account-Funktionen, unter Beachtung zwingender Verbraucherrechte.

Sofortmaßnahmen bei Hochrisiko
Bei erheblichem Risiko können wir direkt Stufe 2 oder 3 anwenden, um unmittelbare Schäden zu verhindern.

Grundsatz der Verhältnismäßigkeit
Maßnahmen richten sich nach:
• Schwere und Art des Verstoßes,
• Wiederholung,
• Gefahrenlage,
• Zumutbarkeit für den Nutzer.

Offline-Nutzung / lokale Basislizenz
Soweit technisch möglich und rechtlich zulässig, kann AILA nach Installation/Aktivierung weiterhin offline gestartet und mit lokal beschränktem Funktionsumfang genutzt werden. Online-Leistungen können unabhängig davon eingeschränkt werden. Zwingende gesetzliche Rechte bleiben unberührt.

---

9) Meldung, Abuse-Handling & Behörden

1. Meldungen: **info@palindrom-ioi.com**
2. Prüfung erfolgt nach Plausibilität, Schwere und Risikobewertung – unter strikter Datensparsamkeit.
3. Minimale Abuse-Logs (Metadaten), soweit erforderlich:
   – License ID (pseudonym),
   – Zeitstempel,
   – Klassifikation des Vorfalls,
   – Status / Maßnahmenstufe.
   Keine Inhalte aus Chats, Prompts oder lokalen Dateien.
4. Behörden werden nur informiert, wenn:
   – gesetzlich verpflichtet, oder
   – zur Abwehr konkreter Gefahren erforderlich.
   Details: Datenschutzerklärung.

---

10) Einspruch / False Positives

1. Gegen Maßnahmen kann per E-Mail Einspruch eingelegt werden: **info@palindrom-ioi.com**
2. Wir können geeignete Nachweise verlangen (z. B. Bestell- oder Identitätsnachweis, geschwärzt, nur soweit erforderlich).
3. Bis zur Klärung können Online-Leistungen eingeschränkt bleiben. Eine lokale Nutzung kann – soweit technisch möglich und rechtlich zulässig – weiter möglich sein.
4. Wir bemühen uns um eine zeitnahe und faire Prüfung unter Berücksichtigung der Verhältnismäßigkeit.

---

11) Ersatz-Key & Missbrauchsprävention

1. Ein einmaliger Ersatz-Key kann kostenfrei gewährt werden, sofern ein plausibler Nachweis vorliegt.
2. Mehrfache Ersatzanfragen können abgelehnt oder kostenpflichtig sein
3. Ersatz kann verweigert werden bei Hinweisen auf Key-Sharing, Piraterie, Betrug oder Umgehung von Schutzmechanismen.
4. Verbraucherrechte bleiben unberührt; Maßnahmen erfolgen verhältnismäßig.

---

12) Responsible Disclosure (Sicherheitsmeldungen)

1. Wir begrüßen verantwortungsvolle Meldungen von Sicherheitslücken.
2. Voraussetzungen:
   – keine aktive Ausnutzung,
   – kein Zugriff auf Daten Dritter,
   – keine Veröffentlichung vor Abstimmung und angemessener Frist.
3. security.txt und eine formale Vulnerability Disclosure Policy (VDP) werden ergänzend bereitgestellt.
   Hinweis: Link/Ort der security.txt & VDP wird vor Live-Gang ergänzt.

---

13) B2B / Enterprise

1. Unternehmen sind verantwortlich für interne Policies, Schulungen und zulässige Use-Cases.
2. Für bestimmte Branchen können zusätzliche Anforderungen gelten (z. B. AVV/DPA, SLA).
3. Enterprise-Leistungen werden ausschließlich individuell vertraglich geregelt.

---

14) Änderungen dieser Policy

Wir können diese AUP aktualisieren. Die jeweils aktuelle Version ist auf unserer Website verfügbar; wesentliche Änderungen teilen wir per E-Mail oder im Nutzerkonto mit.