

Was IT wissen will, *bevor Agenten schreiben dürfen.*

Agenten, die in CRM, Ads und Website schreiben, gehören durch jeden ordentlichen Security-Review. Dieses Pack beantwortet die Fragen vorab: Rechte, Datenflüsse, DSGVO, Prompt Injection, EU AI Act — plus ein ausgefüllter Fragebogen. Offen, ohne Formular, zum Weiterleiten.

STAND **OKTOBER 2026** IGROMO E.U. WWW.IGROMO.COM/SECURITY-GOVERNANCE

- 01 Rechte-Leiter
- 02 Datenflüsse pro Tool
- 03 DSGVO & Auftragsverarbeitung
- 04 Prompt Injection
- 05 EU AI Act
- 06 Security-Fragebogen

AUF EINEN BLICK

Sechs Antworten für *den eiligen Review.*

Läuft in euren Konten

Tools, Knowledge Base, Hub und Agenten-Setup laufen in eurer Umgebung. Modelle, Enrichment und Tools laufen über eure eigenen Verträge.

Lesen ist nicht Schreiben

Agenten lesen für die Analyse. Schreibrechte werden gezielt pro Tool und Agent vergeben — nicht pauschal.

Kein Go, keine Außenwirkung

Outreach, Veröffentlichungen und Budgets brauchen ein einzelnes Go. Nicht umkehrbare Aktionen immer.

Lückenloser Change-Log

Jede Änderung mit Vorher/Nachher, Grund, Freigabe und Zeitpunkt. Rollback, wo technisch möglich.

Daten sind keine Befehle

Inhalte aus E-Mails, Chats und Webseiten sind Information, nie Anweisung. Regeln kommen nur aus der Knowledge Base.

Jederzeit stoppbar

Freigegebene Regeln widerrufen, Agenten pausieren, Zugang entziehen: Der Agent stoppt sofort.

Rechte werden *Stufe für Stufe* vergeben.

Jeder Agent startet unten und steigt nur so weit, wie sein Job es verlangt — pro Tool festgelegt, dokumentiert und jederzeit zurückzunehmen.

L0 Lesen Agenten lesen CRM, Ads, Web und Doku für die Analyse. Pipeline-Daten für den Wochenreport lesen	L1 Vorschlagen Nummerierte Vorschläge mit Wirkung, Risiko und Messpunkt — nichts ändert sich im Tool. „Creative B3 pausieren, Budget auf B1 verschieben“	L2 Schreiben nach Go Nach einem einzelnen Go schreibt der Agent die Änderung direkt ins Tool und loggt sie. Landingpage live stellen, Sequenz starten	L3 Freigegebene Regel Eng umrissene Routinen laufen nach einer einmal freigegebenen Regel — jederzeit widerrufbar. CRM-Notizen schreiben, Audiences pflegen
---	---	--	--

Immer ein einzelnes Go — auch mit freigegebener Regel

- Nachrichten an Externe (Outreach, Sequenzen, E-Mails)
- Budget- und Gebotsänderungen
- Veröffentlichungen (Landingpages, Posts, Ads live)
- Alles, was sich nicht zurückdrehen lässt

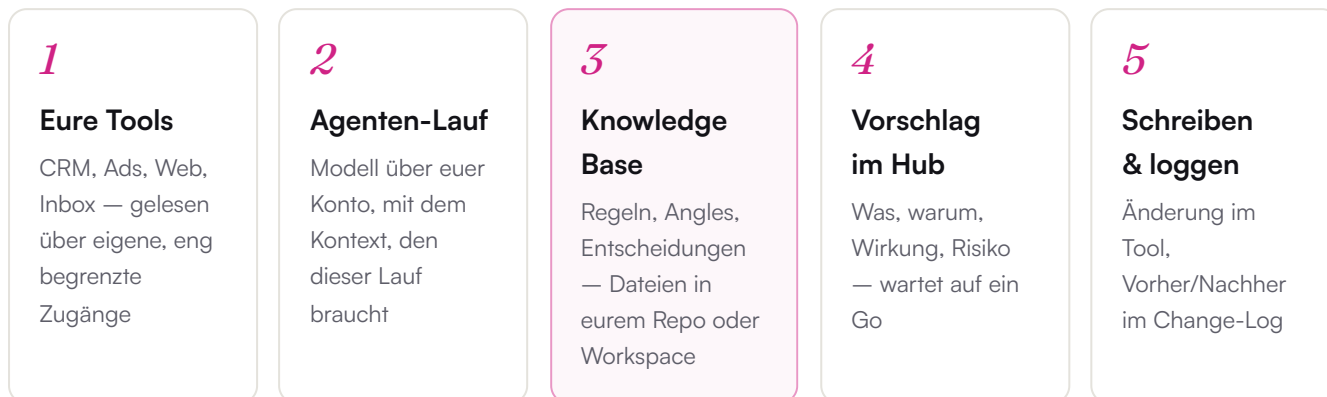
Typische Startkonfiguration der Kern-Agenten

AGENT	LIEST	SCHREIBT	MAX.
Signal Agent	CRM, Web, Intent	Scores und Notizen im CRM (Regel), Hinweis an Sales	L3
Angle & Content Agent	Knowledge Base, bestehende Assets	Entwürfe; Veröffentlichung nur nach Go	L2
Paid Media Agent	LinkedIn Ads, Google Ads, GA4	Optimierungen, Budgets, Gebote — je nach Go	L2
Pipeline Reporting Agent	CRM, Ads, Analytics	Reports und Dashboards im Hub	L1
Outreach Routing Agent	CRM, Outreach-Tools	Routing, Kontakthygiene (Regel); Sequenzen nach Go	L3
Inbox & Ops Agent	Freigegebene Postfächer und Kanäle	Aufgaben mit Owner nach Go	L2
Product Truth Agent	Produktdoku, Release Notes, Website	Hinweise auf Widersprüche	L1
QA & Brand Guard Agent	Live-Seiten, Ads, E-Mails	Befunde; Fixes nach Go	L2

Richtwerte. Welche Stufe ein Agent pro Tool tatsächlich bekommt, wird im Projekt festgelegt und dokumentiert. Viele Teams starten bewusst nur mit L0 und L1.

Woher die Daten kommen – *und wohin sie gehen.*

Ein Agenten-Lauf folgt immer demselben Weg. Das konkrete Datenfluss-Dokument mit euren Tools, Feldern und Zugängen entsteht im Projekt und wird mit übergeben.



BEREICH	BEISPIELE	AGENTEN LESEN	AGENTEN SCHREIBEN	PERSONENBEZUG
CRM	HubSpot, Salesforce	Firmen, Kontakte, Deals, Stages, Aktivitäten	Notizen, Scores, Properties, Workflows, Deal-Stages	Ja — Geschäftskontaktdaten
Ads	LinkedIn Ads, Google Ads	Kampagnen, Kosten, Performance	Audiences, Creatives, Gebote, Budgets (Budget immer mit Go)	Gering — Audience-Listen
Web & Analytics	GA4, Search Console, Fiddler	Seiten, Traffic, Suchanfragen, Besuche auf Firmenebene	— (nur lesen)	Gering — aggregiert
Enrichment & Outreach	Clay, Sales Navigator, HeyReach, Instantly	Firmen- und Rollendaten, Sequenz-Status	Listen anreichern; Sequenzen nur nach Go	Ja — Geschäftskontaktdaten
Website & CMS	Webflow, Vercel, Lovable, HubSpot CMS	Seiten und Inhalte	Landingpages und Inhalte, nur nach Go	Nein
Kommunikation & Arbeit	Slack, Teams, Outlook, Gmail, Notion, ClickUp	Freigegebene Kanäle, Postfächer, Aufgaben	Aufgaben, Zusammenfassungen, Entwürfe	Ja — Nachrichteninhalte
Modell	Claude (Standard), weitere nach Test	Den Kontext des jeweiligen Laufs	—	Je nach Lauf — über euer Konto
Knowledge Base & Hub	Euer Repo oder Workspace	Regeln, Angles, Entscheidungen, Kennzahlen	Updates nach Go des Owners	Minimal — aggregiert

Auswahl typischer Tools. Welche Tools, Felder und Postfächer ein Agent tatsächlich sieht, legt ihr im Projekt fest — neue Tools kommen nur dazu, wenn die Revenue-Logik es verlangt.

Klare Rollen. *Eure Verträge.* Daten bleiben, wo sie sind.

Weil RevPrime® in euren Konten läuft, ändert sich an eurer Datenlandkarte weniger, als man denkt:
Die Daten liegen in den Tools, die ihr schon geprüft habt.

VERANTWORTLICHE

Ihr

Ihr entscheidet über Zwecke und Mittel der Verarbeitung — und über jede Freigabe im System.

AUFTRAGSVERARBEITER

igromo

Wo igromo beim Aufbau und Betrieb Zugriff auf personenbezogene Daten hat, regelt das ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO.

EURE

AUFTRAGSVERARBEITER

Modell- und Tool-Anbieter

Anthropic, HubSpot, LinkedIn & Co. laufen über eure Konten und eure Verträge — genau wie heute schon.

Datenminimierung

Agenten bekommen Zugriff auf die Felder, Kanäle und Postfächer, die ihr Job verlangt — nicht auf alles. Der Hub speichert aggregierte Kennzahlen und Status statt Personendaten.

Keine besonderen Kategorien

RevPrime® verarbeitet Geschäftskontaktdaten (Name, Rolle, Firma, geschäftliche E-Mail, Aktivitäten). Besondere Kategorien nach Art. 9 DSGVO sind kein Teil des Setups.

Keine automatisierten Einzelentscheidungen

Scores und Routing bereiten Entscheidungen vor; Entscheidungen mit rechtlicher oder ähnlich erheblicher Wirkung im Sinne von Art. 22 DSGVO trifft das System nicht.

Rechtsgrundlagen

Für Account-Recherche und B2B-Ansprache ist häufig das berechnete Interesse die Grundlage — die Abwägung trifft ihr. Eure Regeln (z. B. zu E-Mail-Werbung) liegen im Modul Brand, Claims & Legal der Knowledge Base, und jeder Agent hält sich daran.

Drittland

Viele Tools im Stack sind US-Anbieter. Übermittlungen laufen über eure Verträge mit diesen Anbietern, etwa auf Basis des EU-US Data Privacy Framework oder von Standardvertragsklauseln. Wo Anbieter EU-Datenregionen anbieten, können sie genutzt werden.

Dokumentation für DSFA und Verzeichnis

Ob eine Datenschutz-Folgenabschätzung nötig ist, entscheidet ihr. igromo liefert Systembeschreibung, Datenflüsse und Maßnahmen als Input für DSFA und Verzeichnisse.

Betroffenenrechte

Weil die Daten in euren Systemen liegen, greifen eure bestehenden Prozesse für Auskunft, Berichtigung und Löschung. Agenten legen keine Schattenkopien an.

Projektende

Das System wird dokumentiert übergeben. Zugänge von igromo werden entzogen, Tokens rotiert. Bei igromo bleiben keine Kopien eurer Kundendaten.

Sicherheit hängt *nicht am Modell*, sondern an der Architektur.

Kein Modell ist heute vollständig immun gegen Prompt Injection. Deshalb verlässt sich RevPrime® nicht darauf, dass das Modell eine Manipulation erkennt, sondern begrenzt, was ein getäuschter Agent überhaupt tun kann.

RISIKO	GEGENMASSNAHME
Versteckte Anweisungen in E-Mails, Webseiten oder Formularen	Daten sind keine Befehle: Externe Inhalte werden als Information behandelt und werden nie ungeprüft zur Regel. Regeln kommen nur aus der Knowledge Base, mit Go des Owners.
Datenabfluss über ausgehende Aktionen	Keine Außenwirkung ohne einzelnes Go. Empfänger und Inhalt stehen im Vorschlag. Schreibrechte nur auf die Tools, die der Agent braucht.
Zu weit gefasste Rechte	Least Privilege pro Tool und Agent nach der Rechte-Leiter. Start lesend, mehr Rechte erst, wenn der Agent sich bewährt hat.
Falsche oder veraltete Claims gehen live	Freigegebene Claims im Modul Brand, Claims & Legal. Der QA & Brand Guard Agent prüft alles vor und nach Go-live, der Product Truth Agent gleicht mit der Produktdoku ab.
Fehlerkaskaden und ausufernde Kosten	Budget- und Gebotsänderungen brauchen immer ein Go. Routinen laufen mit Schwellen aus der freigegebenen Regel und lassen sich jederzeit pausieren.
Kompromittierte Zugangsdaten	Getrennte, eng begrenzte Zugänge pro Tool. Keine Secrets in Knowledge Base oder Prompts. Zugang entziehen oder rotieren stoppt den Agenten sofort.

Ehrlich gesagt: Auch innerhalb freigegebener Routinen kann ein Agent Fehler machen, etwa eine falsche CRM-Notiz. Deshalb sind diese Routinen eng umrissen, jede Änderung steht im Change-Log, und alles mit Außenwirkung bleibt beim einzelnen Go.

Wo agentisches Marketing *im AI Act steht*.

Eine Einordnung aus Sicht der Architektur, keine Rechtsberatung. Sie hilft eurer Rechtsabteilung, schneller zu den richtigen Fragen zu kommen.

AUG 2024	FEB 2025	AUG 2025	AB AUG 2026
In Kraft getreten	Verbotene Praktiken und Pflicht zur AI-Kompetenz (Art. 4) gelten	Pflichten für Anbieter von General-Purpose-AI-Modellen gelten	Weitere Pflichten, u. a. Transparenz (Art. 50), werden schrittweise anwendbar

Für einzelne Pflichten hat die EU mit dem Digital-Omnibus-Paket Anpassungen und Fristverschiebungen auf den Weg gebracht. Den jeweils aktuellen Stand prüft eure Rechtsberatung.

Risikoklasse

Die typischen RevPrime®-Einsätze — Content, Reporting, Kampagnen-Monitoring, Account-Recherche und Scoring auf Firmenebene — fallen nach unserer Einschätzung nicht unter die Hochrisiko-Bereiche des Anhangs III, etwa Beschäftigung, Kreditwürdigkeit natürlicher Personen oder kritische Infrastruktur. Einsätze in solchen Bereichen sind nicht Teil von RevPrime®.

Transparenz

Chatbots, die direkt mit Menschen sprechen, müssen sich als AI zu erkennen geben; synthetische Bilder, Audio und Video — insbesondere Deepfakes — sind zu kennzeichnen. Bei RevPrime® gehen Nachrichten an Externe nur nach individuellem Go raus. Eure Kennzeichnungsregeln liegen im Modul Brand, Claims & Legal und gelten für jeden Agenten.

Aufsicht und Nachvollziehbarkeit

Menschliche Freigabe, Change-Log mit Vorher/Nachher und klare Owner sind formal vor allem für Hochrisiko-Systeme vorgeschrieben. RevPrime® hat sie trotzdem eingebaut — weil Leadership einem System sonst nicht vertraut.

Rollen

Ihr setzt das System in eurem Unternehmen ein und seid damit in der Regel Betreiber. Der Modellanbieter (standardmäßig Anthropic) ist Anbieter des General-Purpose-Modells. Die Rollenverteilung wird im Projekt dokumentiert.

AI-Kompetenz

Art. 4 verlangt, dass Menschen, die mit AI-Systemen arbeiten, ausreichend geschult sind. Onboarding, Playbooks und die dokumentierte Übergabe sind Teil jedes Projekts und zählen darauf ein.

Die üblichen Fragen. *Schon beantwortet.*

Die Fragen, die in fast jedem Vendor- und Security-Review auftauchen — mit Antworten, die für jedes RevPrime®-Projekt gelten. Was vom konkreten Setup abhängt, ist so markiert.

01 · UNTERNEHMEN & VERANTWORTUNG

Wer ist igromo?	igromo e.U. mit Sitz in Heiligeneich, Niederösterreich (EU), ist das founder-led Studio von Mario Maier: Unternehmensberatung und IT-Dienstleistung aus einer Hand. Kontakt: hello@igromo.com.
Wer hat Zugriff auf unsere Systeme?	Mario Maier persönlich — jedes Projekt läuft founder-led und senior-only. Weitere Personen bekommen nur nach eurer vorherigen Zustimmung und im Rahmen des Auftragsverarbeitungsvertrags Zugriff.
Hat igromo Zertifizierungen wie ISO 27001 oder SOC 2?	Nein. igromo betreibt keine eigene Plattform, auf der eure Kundendaten liegen: Die Daten bleiben in euren Tools, für die deren Zertifizierungen und eure Verträge gelten. Die Maßnahmen von igromo beschreibt dieses Pack; Details regelt der Auftragsverarbeitungsvertrag.

02 · ZUGRIFF & IDENTITÄTEN

Wie greifen die Agenten auf unsere Tools zu?	Über die offiziellen Schnittstellen der Tools (APIs, Connectoren, MCP) mit eigenen, eng begrenzten Zugängen pro Tool — keine geteilten persönlichen Logins. Welche Rechte ein Agent bekommt, folgt der Rechte-Leiter und wird dokumentiert.
Wer vergibt und entzieht die Rechte?	Ihr. Die Zugänge werden in euren Tools angelegt, und ihr könnt sie jederzeit entziehen. Ohne Zugang kann ein Agent nichts lesen und nichts schreiben.
Wo liegen Zugangsdaten und Tokens?	Nicht in der Knowledge Base, nicht in Prompts und nicht im Repo, sondern in der Secret-Verwaltung der jeweiligen Laufzeitumgebung. Wo genau, wird pro Projekt festgelegt und dokumentiert.
Wie sind die Zugänge von igromo abgesichert?	igromo nutzt in euren Tools personalisierte Zugänge mit Multi-Faktor-Authentifizierung, wo das Tool sie unterstützt. Eure Vorgaben, z. B. SSO oder Zugriff nur über bestimmte Konten, werden übernommen.

03 · DATEN & SPEICHERUNG

Wo werden unsere Daten gespeichert?	In euren Tools und Konten. Die Knowledge Base liegt als versionierte Dateien (Markdown, YAML) in eurem Repo oder Workspace, der Hub speichert aggregierte Kennzahlen und Status. Kundendaten werden nicht in Systeme von igromo kopiert.
Welche personenbezogenen Daten verarbeiten die Agenten?	Geschäftskontaktdaten aus CRM und Outreach-Tools (Name, Rolle, Firma, geschäftliche E-Mail, Aktivitäten) und Inhalte aus Postfächern und Kanälen, die ihr freigibt. Keine besonderen Kategorien nach Art. 9 DSGVO.
Werden unsere Daten zum Training von Modellen genutzt?	Die Agenten laufen über euer eigenes Modell-Konto zu euren Vertragsbedingungen. Bei kommerziellen API- und Business-Verträgen der gängigen Anbieter werden Eingaben standardmäßig nicht zum Training genutzt — prüft das in eurem Vertrag mit dem Anbieter.
Wie lange werden Daten aufbewahrt?	Die Daten bleiben in euren Systemen und unterliegen euren Löschkonzepten. Wie lange der Change-Log aufbewahrt wird, legt ihr im Projekt fest.

04 · AI & AGENTEN

Auf welchem Modell laufen die Agenten?	Standardmäßig auf Claude von Anthropic. Das System ist modellunabhängig konzipiert; andere Modelle und Agent-Harnesses sind möglich. Jede Kombination wird für den konkreten Einsatz getestet und freigegeben — ein Wechsel ist kein Knopfdruck.
Können Agenten ohne Freigabe handeln?	Nur innerhalb von Routinen, die ihr einmal ausdrücklich freigegeben habt, etwa Audience-Pflege oder CRM-Notizen. Alles mit Außenwirkung — Outreach, Veröffentlichungen, Budgets — und alles Nicht-Umkehrbare braucht ein einzelnes Go.
Was passiert, wenn ein Agent falsch liegt?	Ihr lehnt den Vorschlag ab, und die Ablehnung mit Grund landet im Entscheidungsgedächtnis. Umgesetzte Änderungen stehen mit Vorher/Nachher im Change-Log und lassen sich zurückdrehen, wo das technisch möglich ist.
Können wir einen Agenten sofort stoppen?	Ja. Ihr könnt jede freigegebene Regel widerrufen, jeden Agenten pausieren und jeden Zugang entziehen. Danach handelt der Agent nicht mehr.

05 · BETRIEB & VORFÄLLE

Ist jede Aktion nachvollziehbar?	Ja. Der Change-Log hält jede Änderung mit Agent, Vorher/Nachher, Grund, Freigabe und Zeitpunkt fest. Agenten-Status, offene Freigaben und Anomalien sind im Hub sichtbar.
Was passiert bei einem Sicherheitsvorfall?	igromo informiert euch unverzüglich, sperrt betroffene Zugänge und analysiert den Vorfall gemeinsam mit euch. Fristen und Kontaktwege regelt der Auftragsverarbeitungsvertrag.

06 · VERTRAG & EXIT

Gibt es einen Auftragsverarbeitungsvertrag?	Ja, sobald igromo Zugriff auf personenbezogene Daten hat. Ihr könnt eure eigene Vorlage verwenden.
Wem gehört das System?	Euch. Knowledge Base, Prompts, Playbooks, Hub und Integrationen laufen in eurer Umgebung und werden dokumentiert übergeben. Die Nutzungsrechte regelt das Angebot.
Wie hoch ist das Lock-in-Risiko?	Gering. Die Knowledge Base besteht aus offenen Dateien, das System ist modellunabhängig konzipiert und läuft in euren Konten. Euer Team kann es nach der Übergabe weiterbetreiben.

Dieses Pack beschreibt Architektur und Arbeitsweise von RevPrime®. Es ist keine Rechtsberatung und ersetzt nicht die Prüfung durch eure Datenschutz- und Rechtsberatung. Verbindlich sind das Angebot und der Auftragsverarbeitungsvertrag.

Ihr habt einen eigenen Fragebogen? Schickt ihn mit. Ich fülle ihn aus — in der Regel vor dem ersten Termin mit IT oder Datenschutz.

KONTAKT

Mario Maier · igromo e.U.
Hasengasse 6, 3452 Heiligeneich, Österreich
hello@igromo.com
www.igromo.com/security-governance