

Freigabe-Kit für KI-Projekte mit JanuaPort

Mit diesen Unterlagen bringen Sie ein KI-Projekt mit JanuaPort durch IT, Datenschutz und Betriebsrat: (A) Antworten für den Datenschutz, (B) eine Vorlage für den TOM-Anhang, (C) eine Folie für den Betriebsrat.

Vorlage, keine Rechtsberatung. Diese Unterlagen beschreiben, was JanuaPort technisch tut, Stand Version 0.73. Die Bewertung für Ihr Unternehmen treffen Sie selbst, mit Ihrem Datenschutzbeauftragten und, wo nötig, mit Ihrem Betriebsrat.

A. Antworten für den Datenschutz (10 Fragen)

1. Wer ist verantwortlich, und ist der Hersteller Auftragsverarbeiter?

Verantwortlich ist das Unternehmen, das JanuaPort betreibt. JanuaPort läuft auf dessen eigenem Server; die JanuaPort GmbH hat keinen Zugriff auf die Anlage und verarbeitet keine Daten aus ihr. Ein Auftragsverarbeitungsvertrag mit dem Hersteller ist deshalb für den Betrieb selbst nicht nötig. Auftragsverarbeiter werden wir nur im Einzelfall: wenn Sie uns den Betrieb übergeben (JanuaPort Managed) oder uns im Support Zugang zur Anlage geben. Dafür gibt es einen AVV.

2. Was schickt die Anlage an den Hersteller?

Von sich aus nur die Abfrage nach neuen Versionen: ein Abruf einer öffentlichen Datei, ohne Lizenz und ohne Kennung der Installation. Er zeigt uns IP-Adresse und Zeitpunkt, und er lässt sich abschalten. Einen Lizenz- oder Katalog-Abruf gibt es nur, wenn Sie dessen Adresse eintragen; ab Werk ist sie leer. Keine Telemetrie, keine Nutzungsdaten. Die Lizenz wird offline geprüft.

3. Wo liegen die Zugangsdaten zu unseren Systemen?

Im Tresor der Anlage, verschlüsselt (AES-256-GCM). JanuaPort gibt sie nie an die KI, ins Protokoll oder an den KI-Anbieter heraus. Ein Administrator kann sie setzen und löschen, aber nicht auslesen.

4. Was sieht der KI-Anbieter?

Was die KI über JanuaPort abrufen, sieht auch ihr KI-Anbieter. Felder, die Sie als sensibel festlegen, etwa Kundennamen oder IBANs, ersetzt JanuaPort vorher durch Kürzel — nach festen Regeln, ohne KI dazwischen. Das ist eine Pseudonymisierung, keine Anonymisierung: Sie ist umkehrbar, und sie schützt nur die Felder, die Sie festlegen. Die Wahl des KI-Anbieters und dessen Vertrag bleiben Ihre Sache.

5. Wer darf was?

Nichts ist erlaubt, was nicht ausdrücklich freigegeben ist (deny-by-default). Rechte werden je Werkzeug vergeben, an Personen (Anmeldung über das Unternehmenskonto per OIDC, etwa Microsoft Entra) oder an Tokens für Agenten, Skripte und RPA. Schreibende Werkzeuge sind gesondert freigegeben und als schreibend gekennzeichnet.

6. Was wird protokolliert, und wie lange?

Jeder Werkzeugaufruf, mit Zeitpunkt, Aufrufer, Werkzeug und Ergebnis. Standard ist ein Protokoll nur mit Metadaten; Abfragen oder Antworten mitzuschreiben ist eine bewusste Einstellung. Kann der Protokolleintrag nicht geschrieben werden, gibt JanuaPort kein Ergebnis heraus. Vor einem löschenden oder überschreibenden Schreibvorgang wird die Absicht protokolliert, bevor er läuft. Die Aufbewahrungsdauer legen Sie fest, global und je Anbindung; ab Werk ist sie unbegrenzt, bis Sie eine Frist setzen. Mitgeschriebene Inhalte haben eine eigene Frist, ab Werk 30 Tage. Jeder Löschlauf protokolliert sich selbst. Die Protokolltiefe erhöhen kann nur ein Mensch mit frischer Anmeldung; die KI kann sie nur senken.

7. Gibt es eine Leistungs- oder Verhaltenskontrolle?

Das Produkt zeigt keine personenbezogene Aktivität an („wann hat Person X zuletzt gearbeitet“ gibt es nicht). Das Protokoll nennt aber je Aufruf, wer ihn ausgelöst hat; es ist damit grundsätzlich geeignet, Verhalten nachzuvollziehen. Siehe Teil C.

8. Wo läuft die Software?

Als Docker-Container auf einem Server Ihrer Wahl: im eigenen Rechenzentrum, auf einer VM oder bei einem Hoster Ihrer Wahl. Daten und Schlüssel bleiben dort.

9. Was passiert, wenn wir aufhören?

Die Anlage gehört Ihnen. Läuft die Lizenz aus, bleiben Daten und Konfiguration bei Ihnen; es gibt keinen Export, den Sie bei uns anfordern müssten.

10. Wogegen schützt JanuaPort nicht?

Gegen jemanden, der den Server vollständig kontrolliert (Root auf dem Host) — er erreicht auch die Schlüssel. Gegen einen böswilligen eigenen Administrator. JanuaPort begrenzt, welche Werkzeuge aufgerufen werden, filtert aber keine einzelnen Zeilen oder Felder aus den Antworten des Zielsystems; was ein Werkzeug liefert, bestimmt dessen Berechtigung im Zielsystem. Und JanuaPort ist nicht zertifiziert (kein ISO 27001, kein Pentest-Bericht). Diese Grenzen stehen so auch in unserer Dokumentation.

B. Vorlage TOM-Anhang (Art. 32 DSGVO) — „System: JanuaPort“

Vorlage, keine Rechtsberatung. Diese Unterlagen beschreiben, was JanuaPort technisch tut, Stand Version 0.73. Die Bewertung für Ihr Unternehmen treffen Sie selbst, mit Ihrem Datenschutzbeauftragten und, wo nötig, mit Ihrem Betriebsrat.

Bereich	Maßnahme durch JanuaPort	Maßnahme des Betreibers (ausfüllen)
Zutritt / Zugang	Verwaltung nur nach Anmeldung; Anmeldung über das Unternehmenskonto (SSO) möglich; Admin-Fläche ab Werk nur lokal erreichbar	Serverstandort, physischer Schutz, Netzsegment, TLS (Pflicht)
Zugriff	deny-by-default, Rechte je Werkzeug, Teams, Tokens je Abnehmer, schreibende Werkzeuge gesondert	Rollenkonzept, wer ist Admin, Freigabeprozess
Weitergabe	Zugangsdaten verschlüsselt im Tresor, nie an die KI; Pseudonymisierung festgelegter Felder vor der KI	Wahl des KI-Anbieters und dessen AVV; welche Felder als sensibel festgelegt sind
Eingabekontrolle	Protokoll jedes Werkzeugaufrufs; Protokolltiefe einstellbar; Verwaltungsakte nachvollziehbar	Aufbewahrungsdauer; wer das Protokoll einsehen darf
Verfügbarkeit	Ein Container, Datenbank im Volume; Backup braucht Datenbank UND Master-Key	Backup-Konzept, getrennte Verwahrung des Master-Keys, Wiederherstellung einmal probeweise durchspielen
Trennung	Sichten und Teams je Zweck; Ablagen und Integrationen getrennt berechtigt	Zuschnitt je Anwendungsfall
Updates	Signierter Update-Feed; Images mit SBOM und Herkunftsnachweis; Abfrage abschaltbar; Einspielen durch Sie	Update-Fenster, Verantwortlicher

C. Folie für den Betriebsrat

Vorlage, keine Rechtsberatung. Diese Unterlagen beschreiben, was JanuaPort technisch tut, Stand Version 0.73. Die Bewertung für Ihr Unternehmen treffen Sie selbst, mit Ihrem Datenschutzbeauftragten und, wo nötig, mit Ihrem Betriebsrat.

Titel: KI-Agenten mit JanuaPort — was protokolliert wird und was nicht

- **Zweck:** JanuaPort regelt, welche KI-Agenten auf welche Systeme zugreifen dürfen, und protokolliert jeden Zugriff. Das dient der Sicherheit und der Nachvollziehbarkeit von Abläufen.
- **Keine Aktivitätsanzeige:** Es gibt keine Ansicht, die zeigt, wann eine Person zuletzt gearbeitet hat oder wie viel. Auswertungen sind nach Systemen geschnitten, nicht nach Personen.
- **Aber:** Das Protokoll nennt je Aufruf den Aufrufer. Damit ist es grundsätzlich geeignet, Verhalten nachzuvollziehen (§ 87 Abs. 1 Nr. 6 BetrVG).
- **Was Sie regeln können:** wer das Protokoll einsehen darf; wie lange es aufbewahrt wird (technisch durchgesetzt); ob Inhalte mitgeschrieben werden (ab Werk nein); keine Auswertung zur Leistungskontrolle (Zweckbindung).
- **Vorschlag:** diese Punkte in einer Betriebsvereinbarung oder einer Ergänzung der bestehenden IT-Vereinbarung festhalten.