ATVANTAGE
part of TIMETOACT GROUP

Digitale Souveränität für Cloud, Daten & KI

Checkliste

Digitale Souveränität für Cloud, Daten und KI – Checkliste

Digitale Souveränität erfordert bewusste Entscheidungen über Kontrolle, Abhängigkeiten und Risiken – gerade dort, wo Kosten- und Innovationsdruck scheinbar dagegenstehen; diese Checkliste schafft dafür Orientierung.

Daten & Datensouveränität

01
10

Haben wir eine klare Klassifikation sensibler und geschäfts-kritischer Daten?

Ohne Klassifikation ist nicht entscheidbar, welche Daten besondere Schutz- und Souveränitätsanforderungen haben.

Status

☐ geklärt ☐ teilweise geklärt ☐ ungeklärt ☐ bewusst akzeptiert

Relevanz

☐ hoch ☐ mittel ☐ gering

Handlungsbedarf

☐ keiner ☐ klären ☐ entscheiden ☐ strukturell aufsetzen

Ist nachvollziehbar, wer auf welche Daten zugreift - intern und extern?

Technische, organisatorische und operative Zugriffe müssen transparent sein.

Ist klar, unter welcher Jurisdiktion Daten verarbeitet werden?

Rechtlicher Zugriff ist oft relevanter als der physische Speicherort.

Wissen wir, wo Metadaten entstehen und gespeichert werden?

Medatdaten können Rückschlüsse auf Inhalte, Nutzung und Geschäftsprozesse erlauben.

Sind Daten logisch und physisch sauber getrennt?
Mandatentrennungen, Schlüsseltrennungen und Isolation sind Grundlage für Kontrolle.

Können Daten vollständig und zeitnah exportiert werden?
Format, Vollständigkeit und Dauer entscheiden über reale Wechseloptionen.

Sind Datenformate offen und portabel?
Proprietäre Formate erhöhen Abhängigkeiten und erschweren Migrationen.

Gibt es Einschränkungen beim Datenabzug oder bei Löschung?
Technische oder vertragliche Hürden zählen gleichermaßen.

Cloud, Betrieb, Zugriff, Recht & Lock-in

Wissen wir, welche Workloads kritisch sind – und welche nicht?
Nicht jeder Workload benötigt maximale Souveränität.

Haben wir Transparenz über Abhängigkeiten von Cloud- und Plattformanbietern?
Plattformdienste, proprietäre APIs und Betriebsmodelle erzeugen Bindungen.

Ist bekannt, wo technologische Lock-ins bestehen?
Proprietäre Services, Automatisierung oder Toolchains können Wechsel verhindern.

Wie aufwendig wäre ein Anbieterwechsel realistisch?
Technisch, organisatorisch, zeitlich und finanziell – nicht nur theoretisch.

Gibt es realistische Wechsel- oder Exit-Szenarien?
Ein Exit muss umsetzbar sein, nicht nur vertraglich erlaubt.

Sind Exit-Szenarien dokumentiert und idealerweise getestet?
Ein ungetesteter Exit ist kein belastbarer Exit.

Ist klar geregelt, wer Entscheidungen über Cloud-Nutzung trifft?
Unklare Entscheidungsrechte führen zu impliziten Abhängigkeiten.

Ist klar, wer die Plattformen operativ betreibt?
Eigenbetrieb, Anbieterbetrieb oder Mischformen beeinflussen Kontrolle.

Ist geregelt, wer im Incident-Fall entscheidet?
Technisch, organisatorisch und rechtlich.

Ist nachvollziehbar, wo Betrieb und Support angesiedelt sind?
Regionale Nähe kann sicherheits- und rechtsrelevant sein.

Gibt es kritische Abhängigkeiten außerhalb der EU?
Auch indirekte Abhängigkeiten zählen.

Entspricht die Infrastruktur den Anforderungen an Auditierbarkeit und Kontrolle?
Nachweise und Evidenzen sind wichtiger als Zusicherungen.

KI-Nutzung & KI-Workloads

Ist klar definiert, wo KI eingesetzt wird?
Analyse, Automatisierung, Entscheidungsunterstützung oder Agenten.

Ist nachvollziehbar, wie KI eingesetzt wird?
Transparenz ist Voraussetzung für Vertrauen und Verantwortung.

Wissen wir, welche Daten KI nutzt?
Input-, Kontext-, Trainings- und Ergebnisdaten müssen unterschieden werden.

Gibt es Leitplanken, wo KI eingesetzt werden darf – und wo nicht?
Nicht jede Aufgabe ist für KI geeignet.

Ist geregelt, wer Verantwortung für KI-Ergebnisse trägt?
Verantwortung bleibt immer menschlich.

Gibt es Abhängigkeiten von proprietären KI-Services oder Modellen?
Managed KI-Dienste können Lock-ins erzeugen.

Sind KI-Modelle, Pipelines und Artefakte portabel?
Modelle, Prompts, Embeddings und Workflows sollten migrierbar sein.

Trainingsdaten, RAG & Wissensbasen

Ist klar getrennt, welche Daten für Training, RAG oder Fine-Tuning genutzt werden?
Unterschiedliche Datenarten haben unterschiedliche Risiken.

Sind sensible Daten explizit ausgeschlossen oder besonders geschützt?
Trainingsdaten dürfen kein Nebenprodukt produktiver Systeme sein.

Ist nachvollziehbar, wo Trainings- und Wissensdaten gespeichert werden?
Speicherort und Zugriff entscheiden über Souveränität.

Ist geregelt, welche Daten ein Modell „lernen“ darf?
Lernfähigkeit braucht klare Grenzen.

Sind RAG-Indizes, Embeddings und Vektordaten portabel?
Technische Portabilität entscheidet über Wechseloptionen.

Ist der Wiederaufbau von Wissensbasen realistisch möglich?
Zeit, Kosten und Know-how müssen berücksichtigt werden.

Gibt es Regeln zur Wiederverwendung oder Löschung von Trainingsdaten?
Trainingsdaten benötigen einen definierten Lebenszyklus.

Agentic AI & Autonomie

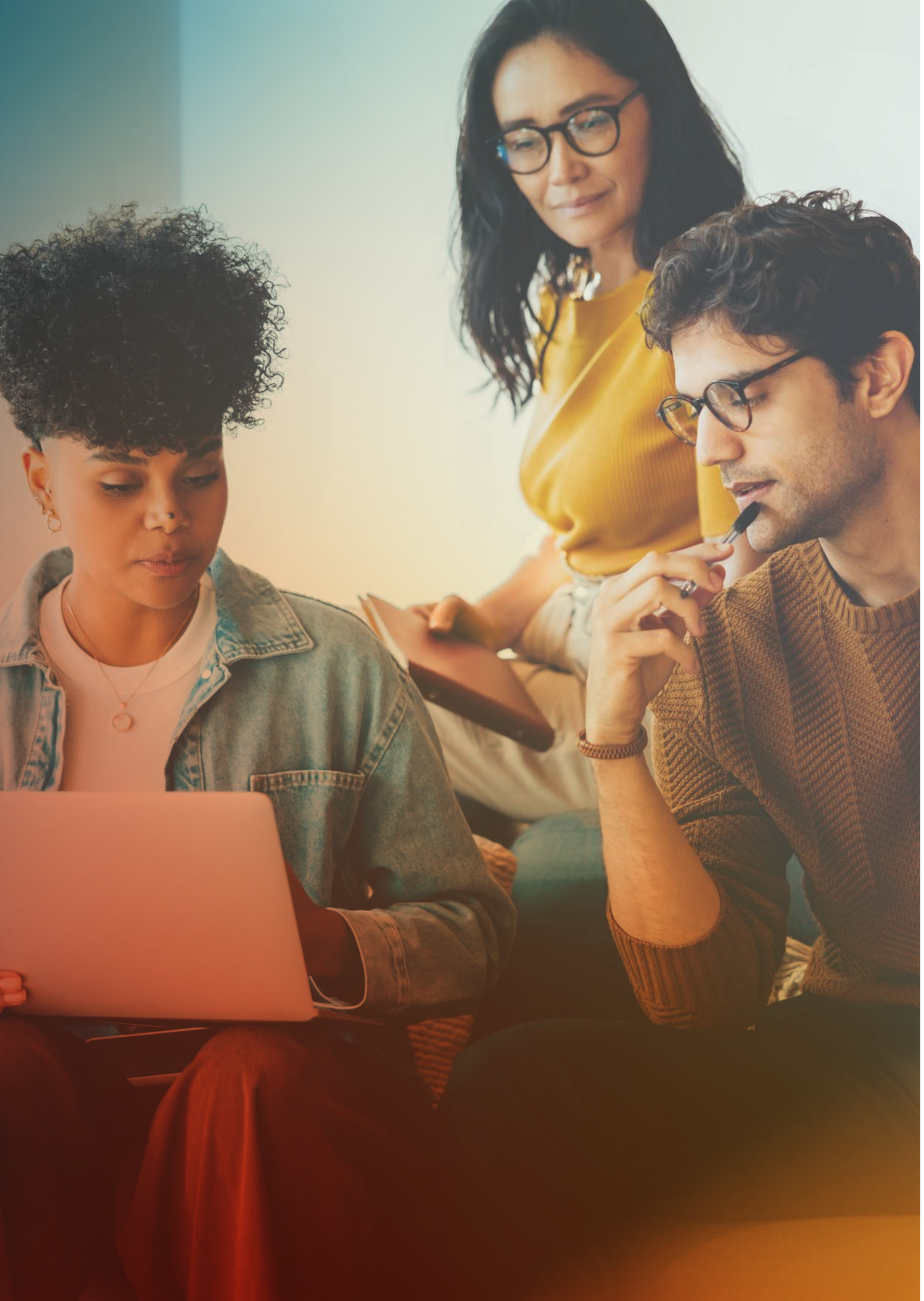
Gibt es KI-Systeme mit eigener Handlungslogik?
Agenten und teilautonome Systeme erhöhen Komplexität und Risiko.

Ist definiert, wie viel Autonomie sinnvoll und verantwortbar ist?
Autonomie ist eine bewusste Entscheidung, kein technischer Default.

Können Entscheidungen von KI-Agenten nachvollzogen werden?
Nachvollziehbarkeit ist Voraussetzung für Kontrolle.

Gibt es Abbruch-, Kontroll- oder Eskalationsmechanismen?
Eingriffsmöglichkeiten müssen vorab definiert sein.

Ist Verantwortung bei autonomen KI-Szenarien eindeutig geklärt?
Auch bei Fehlern oder Schäden.



Governance & Organisation

Sind Rollen und Verantwortlichkeiten für Cloud, Daten und KI klar definiert?
Unklare Zuständigkeiten untergraben Souveränität.

Arbeiten IT, Fachbereiche, Legal und Compliance abgestimmt zusammen?
Souveränität entsteht an Schnittstellen.

Gibt es verbindliche Leitplanken statt Einzelfallentscheidungen?
Konsistenz ist wichtiger als Geschwindigkeit.

Werden neue Cloud- oder KI-Nutzungen systematisch geprüft?
Spontane Nutzung erzeugt implizite Risiken.

Ist digitale Souveränität auf Management-Ebene verankert?
Ohne Management-Verantwortung bleibt sie operativ.

Transparenz & Entscheidungsfähigkeit

Haben wir eine konsolidierte Sicht auf Daten, Cloud und KI?
Übersicht verhindert blinde Flecken.

Können Abhängigkeiten frühzeitig erkannt werden?
Nicht erst im Krisenfall.

Sind Entscheidungen dokumentiert und nachvollziehbar?
Dokumentation schafft Verantwortung.

Können akzeptierte Risiken klar benannt und begründet werden?
Begründetes Vertrauen statt implizitem Vertrauen.

Sind nächste Schritte und Entscheidungsbedarfe klar?
Souveränität ist kein Zustand, sondern ein Prozess

Du möchtest diese Punkte nicht nur abhaken, **sondern konkret einordnen und voranbringen?**

ATVANTAGE unterstützt dich dabei, die relevanten Fragestellungen im Detail zu betrachten, Abhängigkeiten und Risiken transparent zu machen und daraus konkrete Handlungsempfehlungen abzuleiten – herstellerneutral, entlang deiner Prioritäten – und bis zur Umsetzung.

Michael Hölken ist Sales- und Presales-Leader mit über 27 Jahren Erfahrung in der IT-Branche. Er unterstützt Unternehmen dabei, komplexe IT-Landschaften gezielt zu modernisieren und Innovationen rund um Cloud, Künstliche Intelligenz und Rechenzentrumsinfrastruktur erfolgreich in den Geschäftserfolg zu überführen. Durch die Verbindung von technischer Expertise und strategischer Vertriebsführung entwickelt er passgenaue Lösungen, die sowohl skalierbar als auch zukunftssicher sind. Seine Stärke liegt darin, technologische Möglichkeiten klar an geschäftlichen Zielen auszurichten und Transformationen effizient umzusetzen. Er steht für eine klare Umsetzungsorientierung, verbindet Fachbereiche und IT wirkungsvoll miteinander und schafft so die Grundlage für messbare Ergebnisse und nachhaltiges Wachstum.

michael.hoelken@atvantage.com
+49 172 5246 601

Maik Saewert ist Solution Sales Manager für Cloud-Transformation bei der ATVANTAGE GmbH (Teil der TIMETOACT GROUP). Er begleitet Unternehmen bei der Entwicklung und Umsetzung moderner Cloud-Strategien mit besonderem Fokus auf digitale Souveränität. Mit über 27 Jahren Erfahrung im IT-Vertrieb berät er Kunden praxisnah bei Cloud-Migrationen und der Auswahl geeigneter Plattformen wie STACKIT und AWS. Dabei berücksichtigt er gezielt regulatorische Anforderungen, Datensouveränität sowie technische und organisatorische Rahmenbedingungen. Unternehmen profitieren von seiner langjährigen Erfahrung in komplexen IT-Projekten, seiner strategischen Beratungskompetenz sowie seinem klaren Fokus auf sichere, zukunftsfähige Cloud-Lösungen.

maik.saewert@atvantage.com
+49 151 6107 9391

Über ATVANTAGE

ATVANTAGE ist ein führender Partner für ganzheitliche Digitalisierung, moderne Softwarearchitekturen und intelligente Prozesslösungen. Unser interdisziplinäres Team begleitet Unternehmen bei der erfolgreichen Transformation ihrer IT-Landschaft – von der strategischen Beratung bis zur technischen Umsetzung.

ATVANTAGE GmbH
Im Mediapark 5
50670 Köln

Telefon **+49 221 97343 0**
E-Mail **info@atvantage.com**
Web **www.atvantage.com**

Mit tiefem Verständnis für Geschäftsprozesse und technologischer Exzellenz entwickeln wir individuelle Lösungen in den Bereichen Data, AI, Cloud, App Modernization und Process Optimization. Dabei steht für uns nicht die Technologie im Vordergrund, sondern der konkrete Mehrwert für unsere Kunden: spürbar effizientere Abläufe, messbare Kostensenkungen und nachhaltiger Business Impact.

ATVANTAGE ist aus dem Zusammenschluss mehrerer etablierter IT-Unternehmen entstanden. Gemeinsam verfügen wir über jahrzehntelange Erfahrung und tiefes Branchenwissen – insbesondere in Industrie, Handel und Logistik.
Was uns auszeichnet: partnerschaftliches Arbeiten auf Augenhöhe, klare Kommunikation und der Anspruch, gemeinsam mit unseren Kunden echte Fortschritte zu erzielen.

ATVANTAGE
part of TIMETOACT GROUP