

HANDOUT ZUM VORTRAG

Shadow AI als Datenschutzrisiko

nomios secure and connected

SELBSTTEST UND BEWERTUNGSWERKZEUG FÜR DEN KONKRETEN FALL

5 Fragen, die Sie diese Woche beantworten können sollten

Gehen Sie die fünf Fragen für Ihr Unternehmen durch.
Notieren Sie ehrlich: können wir das belegen, ja oder nein?

1

Welche KI-Dienste werden in Ihrem Haus tatsächlich genutzt?

Nicht welche freigegeben sind. Welche genutzt werden, inklusive privater Accounts.

belegbar nicht belegbar

2

Welche Ihrer bestehenden Anwendungen haben in den letzten zwölf Monaten KI-Funktionen dazubekommen?

CRM, Ticketsystem, Office-Suite, Browser. Meist per Update aktiviert, ohne Entscheidung in Ihrem Haus.

belegbar nicht belegbar

3

Deckt Ihr Auftragsverarbeitungsvertrag mit diesen Anbietern diese neuen KI-Funktionen ab?

Und wissen Sie, welche Modellanbieter als Unterauftragsverarbeiter dahinterstehen?

belegbar nicht belegbar

4

Gibt es eine freigegebene, datensichere Alternative, und ist sie bequemer als der inoffizielle Weg?

Falls nein: Ihre Mitarbeitenden haben sich längst entschieden.

belegbar nicht belegbar

5

Wer bemerkt es, wenn ein KI-Agent heute Nacht Daten an einen falschen Ort schreibt, und wie schnell?

Die Meldefrist nach Art. 33 DSGVO beträgt 72 Stunden ab Kenntniss.

belegbar nicht belegbar

IHRE AUSWERTUNG

- 0 – 1x

Weiter als die meisten. Der Reifegrad liegt dann bei der Reaktionsfähigkeit.
- 2 – 3x

Typischer Befund: Richtlinie vorhanden, Durchsetzung nicht. Der erste Schritt kostet kein Lizenzbudget.
- 4 – 5x

Die Dokumentation nach Art. 30 DSGVO ist nicht vollständig führbar, weil die Faktenlage fehlt.

DREI ZAHLEN ZUM WEITERGEBEN

- 8,2 GB

Daten pro Organisation und Monat in SaaS-KI-Apps. Gemessen, nicht befragt.
- 60 %

der KI-Nutzer arbeiten mit privaten Accounts.
- 194 Tage

bis ein Datenabfluss bemerkt wird. Meldefrist: 72 Stunden.

FÜR IHREN DATENSCHUTZBEAUFTRAGTEN

Nicht jeder Shadow-AI-Fund ist eine Datenpanne

DER ENTSCHEIDUNGSWEG

Diese Fragen helfen nach jedem Fund bei der Entscheidung: müssen wir das melden?

1

Waren personenbezogene Daten enthalten?

Nein: kein DSGVO-Fall. Bleibt relevant für Richtlinie und Geheimnisschutz, etwa bei Quellcode.

2

Lagen Rechtsgrundlage, AV-Vertrag und bei Anbietern außerhalb der EU eine Übermittlungsgrundlage vor?

Alle vorhanden: zulässige Verarbeitung, Verzeichnis und ggf. Folgenabschätzung nachziehen.

3

Sind die Daten dadurch unautorisiert offengelegt worden, also gespeichert, weitergegeben oder ins Modelltraining übernommen?

Nein oder nicht feststellbar: Verstoß gegen die Verarbeitungsgrundsätze. Compliance-Verstoß, aber keine Datenschutzverletzung nach Art. 4 Nr. 12.

4

Besteht ein Risiko für die betroffenen Personen?

Ja: mögliche Datenschutzverletzung. Meldung nach Art. 33 innerhalb von 72 Stunden ab Kenntnis, bei hohem Risiko zusätzlich Art. 34.

In jedem Fall: intern immer an den Datenschutzbeauftragten melden.
Die Bewertung trifft der DSB, nicht die IT. Die IT liefert den Sachverhalt.

DER FRAGENKATALOG AN DEN ANBIETER

Für jedes KI-Tool und jede Software mit KI-Funktion. Wer sie beantworten kann, hat die Grundlage für den Eintrag im Verarbeitungsverzeichnis.

- ☐ 1. Liegt ein Auftragsverarbeitungsvertrag vor, und deckt er die KI-Funktion ausdrücklich ab?
- ☐ 2. Bei Anbietern außerhalb der EU: Zertifizierung unter dem EU-US Data Privacy Framework oder Standardvertragsklauseln mit ergänzenden Maßnahmen?
- ☐ 3. Werden Eingaben zum Training eigener Modelle genutzt, und ist der Ausschluss vertraglich zugesagt?
- ☐ 4. Welche Unterauftragsverarbeiter sind eingebunden, insbesondere welche Modellanbieter? Ist die Liste offengelegt und aktuell?
- ☐ 5. Welche Löschfristen gelten für Prompts und Antworten?
- ☐ 6. Lassen sich die KI-Funktionen über die Administrationseinstellungen abschalten?
- ☐ 7. Für welche Datenkategorien ist das Tool intern freigegeben, und ist das dokumentiert?

Praktischer Hinweis zur Tarifwahl:

Business- und Enterprise-Tarife bringen AV-Vertrag und Trainingsausschluss meist mit, kostenlose Consumer-Versionen in der Regel nicht. Der freigegebene Unternehmenstarif ist deshalb auch die Compliance-Antwort.

Kein Rechtsberatungsangebot. Diese Übersicht dient der internen Vorbereitung. Die Bewertung im Einzelfall trifft Ihr Datenschutzbeauftragter oder Ihre Rechtsabteilung.

WIE GEHT ES WEITER?

Wenn Sie mehr als zwei Fragen nicht belegen konnten, ist das kein Versäumnis. Sondern der Normalzustand.

Die Frage ist nur: **Wo liegt der wirksamste nächste Schritt?**

Ihr Selbsttest im Gespräch

- Schicken Sie uns Ihr Ergebnis.
- Wir ordnen in zwanzig Minuten ein, wo bei Ihnen der wirksamste nächste Schritt liegt.
- Ohne Präsentation und ohne Angebot im Anhang.

Security- und KI-Readiness-Check

- Ein strukturiertes Assessment Ihrer Umgebung mit einem Rating Ihrer Sicherheitslage, nicht nur bezogen auf die KI-Nutzung.
- Wir sagen Ihnen vorab, was es umfasst und was es kostet. Ohne Überraschungen.

Unser Team ist jederzeit für Sie da.



Thomas Brandt
Chief Technology Officer

M | thomas.brandt@nomios.de
T | +49 151 544 066 41



Nikolei Engelke
Pre-Sales Security Engineer

M | nikolei.engelke@nomios.de
T | +49 160 403 211 5



Niels Loewe
Regional Sales Director

M | niels.loewe@nomios.de
T | +49 171 768 400 6

Nomios Germany GmbH
Rahmhofstraße 4
60313 Frankfurt am Main Deutschland

Contact us
T: +49 (69) 1728 9001
E: info@nomios.de

www.nomios.de
Besuchen Sie unsere Webseite
für weitere Informationen.