INCIDENT-PLAYBOOK DAT-03

# Vertrauliches in öffentliche KI eingegeben

Daten & Datenschutz

Vertrauliche Unterlagen, Kundendaten oder interne Informationen wurden in einen KI-Dienst eingegeben, den das Unternehmen dafür nicht freigegeben hat. Je nach Dienst und Vertragsart können Eingaben gespeichert, vom Personal des Anbieters eingesehen oder zum Training verwendet werden.

- Vertrag zum Zusammenfassen in einen Chatbot kopiert
- Kundenliste von einer KI auswerten lassen
- Quellcode mit Zugangsdaten zur Fehlersuche eingefügt
- Protokoll mit Personaldaten übersetzen lassen

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Keine weiteren Inhalte in den Dienst eingeben und die Sitzung beenden.

02 Den Verlauf nicht löschen, bevor er dokumentiert ist. Screenshots der Eingaben und Antworten anfertigen.

03 Notieren, welcher Dienst mit welchem Konto genutzt wurde, etwa privat, kostenlos oder über eine Firmenlizenz.

04 Festhalten, welche Daten eingegeben wurden und ob personenbezogene Daten oder Zugangsdaten darunter waren.

05 Sofort melden. Ob daraus eine Meldepflicht entsteht, bewerten andere.

## Melden

SOFORT

WEN

Datenschutz-Ansprechperson und IT-Verantwortliche gemeinsam. Bei Geschäftsgeheimnissen oder Kundendaten zusätzlich die Geschäftsführung.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Die eingegebenen Inhalte nicht erneut in Mails oder Chats kopieren, nur beschreiben.

WAS BEREITHALTEN

- Welcher KI-Dienst mit welchem Konto genutzt wurde
- Welche Inhalte eingegeben wurden
- Ob personenbezogene Daten oder Zugangsdaten enthalten waren
- Wann die Eingabe erfolgte
- Ob Ergebnisse weitergegeben oder gespeichert wurden

## Nicht tun

HÄUFIGE FEHLER

- × Den Verlauf sofort löschen und den Vorfall für sich behalten.
- × Davon ausgehen, dass gelöschte Eingaben auch beim Anbieter gelöscht sind.
- × Mit demselben Dienst weiterarbeiten, bis die Frage geklärt ist.
- × Eingegebene Zugangsdaten weiter verwenden.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Eingegebene Zugangsdaten und Schlüssel werden sofort gewechselt.
- → Die IT prüft die Bedingungen des Dienstes zu Speicherung und Training und beantragt, wo möglich, die Löschung beim Anbieter.
- → Waren personenbezogene Daten betroffen, bewertet die Datenschutz-Ansprechperson den Fall nach Art. 33 DSGVO.
- → Die Geschäftsführung legt fest, welche KI-Dienste für welche Daten freigegeben sind, und macht die Regel bekannt.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Datenschutzverletzung (DAT-05) · Passwort oder Zugangsdaten preisgegeben (ACC-01) · Interne Kontakte siehe Incident-Kontaktblatt

**Playbooks sind der Anfang. Der Prozess dahinter ist Führungsarbeit.**

Alle Playbooks, Kontaktblatt und Hintergründe online — kostenfrei und ohne Anmeldung.

wermescher.com/tools/it-notfallplan