

Datenschutz, Compliance & Hinweisgeberschutz

- [Datenschutz im Unternehmen](#)
- [Hinweisgeberschutz und interne Meldestelle](#)
- [KI-Richtlinie - Umgang mit künstlicher Intelligenz](#)
- [Explizite Datenschutzerklärung für unsere hausinterne KI](#)

Datenschutz im Unternehmen

Als Unternehmen sind wir gemäß der DSGVO dazu verpflichtet datenschutzkonform und sicher mit Daten zu arbeiten und nehmen aber auch unabhängig davon das Thema Datenschutz sehr ernst. Dies betrifft nicht nur die Daten der Kunden und Lieferanten, sondern auch die persönlichen Daten unserer Mitarbeiter.

Entsprechend sind wir dazu verpflichtet einen Datenschutzbeauftragten zu benennen und haben uns hier für die [Fa. Shegon](#) mit Herrn Maßing als Ansprechpartner entschieden.

Hausintern betreut Daniel Schade das Thema Datenschutz und steht im regelmäßigen Austausch mit Herrn Maßing. Solltet ihr Anliegen, Anregungen oder Hinweise haben, dann teilt ihm diese gerne unter den bekannten Kanälen mit.

In der [Datenschutz-Grundverordnung \(DSGVO\)](#) ist sehr genau festgelegt, wie mit personenbezogenen Daten richtig umzugehen ist.

Aus den Pflichten bezüglich der Verarbeitung von Personendaten ergeben sich genauso Rechte und Befugnisse, wenn es um die eigenen Informationen geht.

Wir bitten euch, sich an diese Vorgaben zu orientieren und mit dem Thema Datenschutz sensibel umzugehen.

Orientierungshilfe zur Kundenanlage und Datenschutz

Im täglichen Umgang mit unseren Kundinnen und Kunden ist es wichtig, dass wir bei der Neuanlage von Kundendaten und beim Ausstellen von Rechnungen einige Punkte beachten, um einen reibungslosen Ablauf sicherzustellen und gleichzeitig den Anforderungen der [Datenschutz-Grundverordnung \(DSGVO\)](#) gerecht zu werden.

Wenn ein Kunde unser Geschäft betritt und bereits bei uns im System hinterlegt ist, kann der gewohnte Ablauf also das Erstellen eines Lieferscheins und das Ausstellen einer Rechnung wie gewohnt erfolgen.

Sollte jedoch beim Erfassen ein Hinweis zur [DSGVO](#) erscheinen, weist das darauf hin, dass dieser Kunde schon längere Zeit nichts mehr bei uns gekauft hat und wir noch keine Einverständnis zum Speichern seiner Daten haben. In diesem Fall benötigen wir eine aktuelle Einwilligung zur Datenspeicherung, bevor wir eine Rechnung ausstellen dürfen. Diese Einwilligung wird über das Kundenanlageformular eingeholt und sollte in einem ruhigen Moment gemeinsam mit dem Kunden

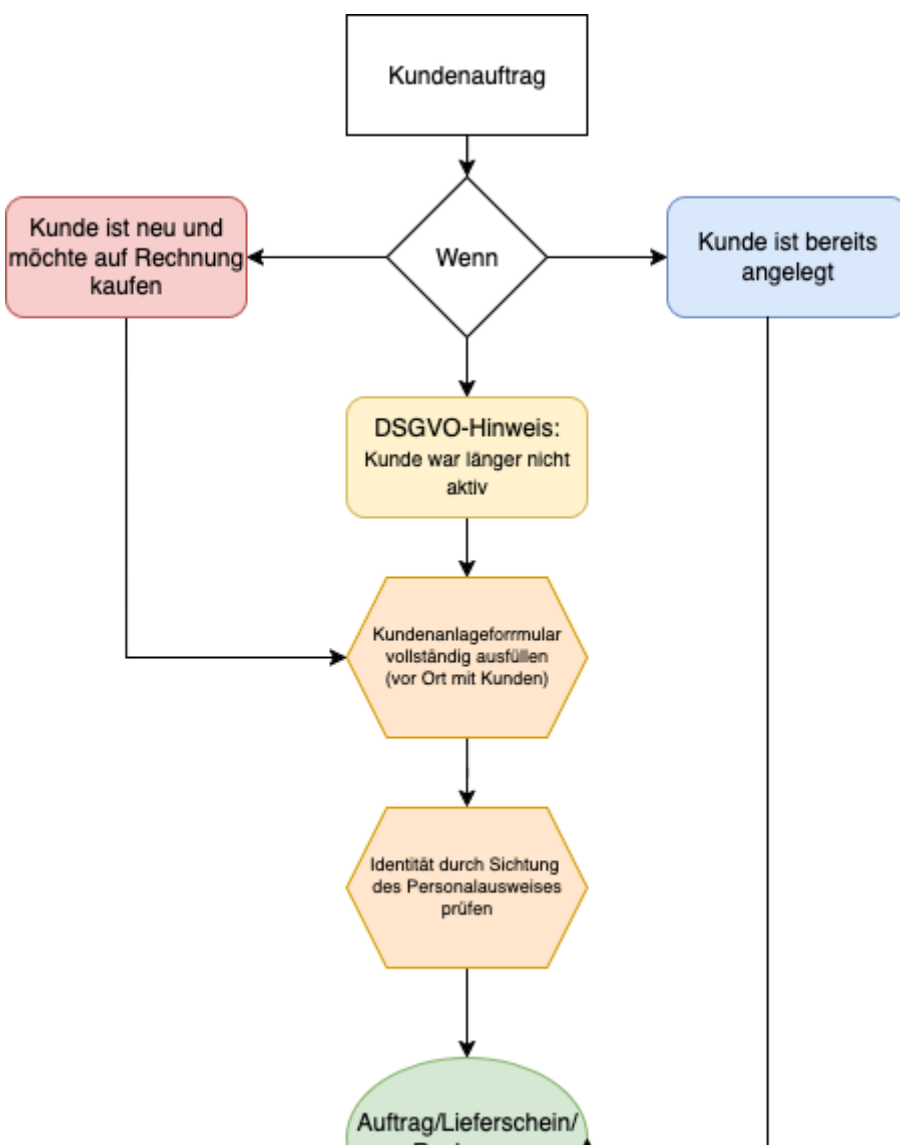
am Tresen ausgefüllt werden.

Auch wenn ein Kunde zum ersten Mal bei uns einkauft und eine Rechnung wünscht, ist vorab das entsprechende [Kundenanlageformular](#) auszufüllen je nach Zahlungsart entweder mit Angabe zur Überweisung oder zum Lastschriftverfahren. Es ist dabei wichtig, dass der Kunde nicht nach oben oder an die Zentrale weitergeleitet wird, sondern direkt von dem Kollegen oder der Kollegin bearbeitet wird, bei dem der Kunde gerade steht. Das Ausfüllen des Formulars erfolgt also unmittelbar vor Ort am Tresen und gemeinsam mit dem Kunden oder der Kunde nimmt das Formular mit und bringt es später.

Ein besonderer Fokus sollte dabei auf der Identitätsprüfung liegen. Um Missbrauch vorzubeugen, bitten wir euch, sicherzustellen, dass die Angaben auf dem Formular mit der Person übereinstimmen, die es ausfüllt. Idealerweise wird dazu der Personalausweis wenn nicht parat dann vielleicht Führerschein etc. eingesehen oder wenn möglich eine Kopie beigelegt. Ziel ist es, sicherzugehen, dass niemand im Namen einer anderen Person ein Kundenkonto eröffnet oder auf fremde Rechnung einkauft.

Abschließend möchten wir noch einmal daran erinnern, dass die Kollegin oder der Kollege, der das Formular gemeinsam mit dem Kunden ausfüllt, auch dafür verantwortlich ist, dass alle Angaben vollständig und korrekt sind. Bitte achtet darauf, euer Kürzel auf dem Formular zu vermerken, sodass bei Rückfragen klar nachvollziehbar ist, wer den Vorgang betreut hat.

Kurzübersicht: Vorgehensweise bei Kundenanlage und DSGVO-Hinweis



WICHTIG

- Kundenanlageformular vor Ort am Tresen vollständig ausfüllen (je nach Zahlungsart auch das Lastschriftformular)

Keine Weitergabe an die die Zentrale - Bearbeitung direkt durch den betreuenden Mitarbeiter.

- Identität prüfen durch Sichtung des Personalausweises.
- Alle Unterlagen vollständig und gewissenhaft ausfüllen. Das eigene Kürzel ist auf dem Formular zu vermerken!



Hinweisgeberschutz und interne Meldestelle

Durch die veränderten rechtlichen Compliance-Vorgaben für Unternehmen ab Mitte 2023 wurde es auch für uns als Firma Schlichter GmbH & Co KG verpflichtend, ein Hinweisgebersystem zu implementieren. Dieser Verpflichtung sind wir nachgekommen und geben seither allen Firmenangehörigen auf unserer Homepage unter (<https://schlichter.biz/hinweisgebersystem/>) digital die Möglichkeit, Fehlverhalten oder Gefahren in Bezug auf unser geschäftliches Handeln zu melden.

Zu möglichen Fehlverhalten und potenziellen Gefahren können u.a. Gesundheits- und Sicherheitsrisiken, Umweltschäden, Bestechung, Diebstahl, Betrug und andere kriminelle Aktivitäten sowie jede Verletzung gesetzlicher Verpflichtungen zählen.

Insbesondere legen wir Wert auf ein respektvolles und gleichberechtigtes Miteinander. Auch Delikte wie sexuelle Belästigung, in Worten, Gesten oder Handlungen, werden in unserem Unternehmen nicht geduldet. Jede und jeder hat das Recht auf einen Arbeitsplatz frei von Übergriffen oder unangemessenen Annäherungen. Wer ein entsprechendes Verhalten erlebt oder beobachtet, kann sich vertrauensvoll an die Geschäftsleitung wenden oder anonym über das Hinweisgeberschutz eine Meldung abgeben. Verstöße können arbeitsrechtliche Konsequenzen nach sich ziehen.

Unter dem angeführten Link muss die hinweisgebende Person zur Wahrung der Anonymität einen vierstelligen PIN eingeben und erhält zugleich einen Zusatzcode. Beides wird benötigt, um die abgegebene Meldung einzusehen und den Bearbeitungsstatus anonym einzuholen. Ihr habt 365 Tage im Jahr rund um die Uhr die Möglichkeit, über das System eine Meldung abzugeben.

Neben der digitalen Hinweisgeberlösung könnt ihr euch auch selbstverständlich weiterhin mit euren Anliegen oder vertraulichen Hinweisen an eure Vorgesetzten oder vertrauten Kolleginnen und Kollegen wenden. Gerne dürft ihr auch Meldungen persönlich an Kerstin Kuper und Daniel Schade übermitteln. Beide sind bei uns im Unternehmen mit der Bearbeitung eingehender Hinweise und eventuell folgenden Maßnahmen betreut und stehen euch bei etwaigen Rückfragen zur Verfügung.

KI-Richtlinie - Umgang mit künstlicher Intelligenz

Einleitung

„Wir bei B. Schlichter möchten Künstliche Intelligenz (KI) in allen Bereichen unseres Unternehmens verwenden. Wir hoffen, hierdurch die Mitarbeitenden zu entlasten, die Effizienz und Innovationsfähigkeit unseres Unternehmens zu erhöhen sowie den Service gegenüber unseren Kundinnen und Kunden weiter zu verbessern.

Jedoch gehen von der unsachgemäßen Verwendung von KI-Systemen Risiken für unser Unternehmen und unsere Kundinnen und Kunden aus, die wir minimieren wollen. Diese Richtlinie regelt daher die verantwortungsvolle und rechtskonforme Nutzung von KI-Systemen in unserem Unternehmen.“

Anwendungsbereiche

Diese Richtlinie hat folgenden Anwendungsbereiche:

1. Sachlicher Anwendungsbereich

Diese Richtlinie gilt für alle Bereiche von B. Schlichter GmbH & Co. KG und der Schlichter Maler und Glashandel GmbH.

2. Räumlicher Anwendungsbereich

Diese Richtlinie gilt für alle unsere Standorte, also derzeit Lathen, Heppenheim, Barsbüttel und Papenburg.

3. Persönlicher Anwendungsbereich

Diese Richtlinie gilt für alle Beschäftigten von B. Schlichter GmbH & Co. KG und Schlichter Maler und Glashandel GmbH. Darüber hinaus gilt sie auch für Personen, die im Auftrag unseres Unternehmens mit dem Betrieb und der Nutzung von KI-Systemen befasst sind.

3. Zeitlicher Anwendungsbereich

Definitionen

Nachfolgend werden einige verwendete Begriffe definiert. Im Rahmen dieser Richtlinie bezeichnet der Ausdruck

1. „KI-System“

Ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können

(Art. 3 Nr. 1 der KI-Verordnung (EU) 2024/1689);

2. „Risiko“

Die Kombination aus der Wahrscheinlichkeit des Auftretens eines Schadens und der Schwere dieses Schadens.

(Art. 3 Nr. 2 der KI-Verordnung (EU) 2024/1689);

3. „Schwerwiegender Vorfall“

Einen Vorfall oder eine Fehlfunktion bezüglich eines KI-Systems, das bzw. die direkt oder indirekt eine der nachstehenden Folgen hat:

- a) den Tod oder die schwere gesundheitliche Schädigung einer Person;
- b) eine schwere und unumkehrbare Störung der Verwaltung oder des Betriebs kritischer Infrastrukturen;
- c) die Verletzung von Pflichten aus den Unionsrechtsvorschriften zum Schutz der Grundrechte;
- d) schwere Sach- oder Umweltschäden

(Art. 3 Nr. 49 der KI-Verordnung (EU) 2024/1689);

4. „Personenbezogene Daten“

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert

werden kann.

(Art. 3 Nr. 50 der KI-Verordnung (EU) 2024/1689 i.V.m. Art. 4 Nr. 1 der Verordnung (EU) 2016/679);

5. „KI-Kompetenz“

Die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden

(Art. 3 Nr. 56 der KI-Verordnung (EU) 2024/1689);

6. „Deepfake“

Einen durch KI erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäßer erscheinen würde.

(Art. 3 Nr. 60 der KI-Verordnung (EU) 2024/1689);

7. Geltung der KI-Verordnung (EU) 2024/1689)

Im Übrigen gelten die Definitionen der KI-Verordnung (EU) 2024/1689.

Unternehmenswerte beim Einsatz von KI-Systemen („KI-Prinzipien“)

Bei der Anwendung von KI-Systemen folgen wir folgenden Grundsätzen:

1. Fairness und Nicht-Diskriminierung

KI-Systeme dürfen Personen nicht benachteiligen, insbesondere nicht aufgrund folgender Merkmale:

1. Herkunft
2. Geschlecht/sexuelle Identität
3. Religion
4. Behinderung
5. Alter

2. Datenschutz und Sicherheit

2.1. Grundsatz zum Umgang mit Daten

Datenschutz hat bei der Nutzung von KI-Systemen oberste Priorität. Da viele KI-Anbieter hochgeladene Informationen zum Training ihrer Modelle nutzen und die rechtliche Lage bezüglich der Eigentumsrechte an Outputs (Text, Bild, Code) derzeit nicht abschließend geklärt ist, gilt eine strikte Daten Disziplin.

Personenbezogene Daten werden nur so weit verarbeitet, wie dies für die Tätigkeit unseres Unternehmens notwendig ist.

Es ist strengstens untersagt, das System für automatisierte Personalanalysen, das Creditscoring oder zur Beurteilung von Menschen einzusetzen. Solche Anwendungen fallen in die Kategorie der Hochrisiko-KI und sind ohne explizite Freigabe verboten.

2.2 Die 3 Goldenen Regeln der KI-Nutzung

Um die Sicherheit unserer Unternehmenswerte und den Schutz personenbezogener Daten zu gewährleisten, sind folgende Regeln ausnahmslos einzuhalten:

- **Regel 1: Keine personenbezogenen Daten in öffentlichen KI-Tools.**

Die Eingabe von Klardaten (Namen, E-Mails, Telefonnummern), die Rückschlüsse auf identifizierbare Personen zulassen, ist in öffentlichen oder nicht-proprietären KI-Systemen untersagt. Es gibt keine Ausnahmen.

- **Regel 2: Anonymisierung vor Upload.**

Sollen unternehmensinterne Daten verarbeitet werden, müssen diese vorab zwingend anonymisiert werden:

- Namen durch Platzhalter ersetzen.
- Spezifische Details abstrahieren.
- Kontext entfernen, der eine Re-Identifizierung ermöglichen könnte.

- **Regel 3: Vorsicht vor Schnelligkeit.**

Im Zweifelsfall ist die Nutzung zu unterlassen oder Rücksprache mit dem Datenschutzbeauftragten zu halten.

2.3 Besonders schützenswerte Datenkategorien

Der Umgang mit den folgenden Datenkategorien ist in Verbindung mit KI-Tools besonders kritisch und unterliegt strengsten Beschränkungen:

- **Gesundheitsdaten & genetische Daten**
- **Unternehmensinterna** (Strategien, unveröffentlichte Berichte)
- **Nicht-öffentliche Finanzdaten**
- **Lebensläufe** und Mitarbeiterdaten

2.4 Transparenz und Datensparsamkeit

Bei der Arbeit mit KI-gestützten Prozessen sind wir gegenüber unseren Kunden zur Transparenz verpflichtet:

- **Informationspflicht:** Kunden müssen darüber in Kenntnis gesetzt werden, wenn ihre Daten durch KI-Systeme verarbeitet werden. Diese Informationen sollten präzise, aber allgemein gehalten sein.
- **Datensparsamkeit:** Es dürfen grundsätzlich nur die für den spezifischen Zweck absolut notwendigen Daten erhoben und verarbeitet werden.

3. Menschliche Aufsicht

Von KI-Systemen geschaffene Ergebnisse dürfen nicht ungeprüft verwendet werden.

Regeln für die Nutzung von KI-Systemen

1. Freigegebene KI-Systeme

Bereitgestellte KI-Tools dienen ausschließlich der Unterstützung im Arbeitsalltag (z. B. für allgemeine Recherchen oder Textentwürfe).

Die unkontrollierte Nutzung von nicht offiziell freigegebenen, öffentlichen KI-Werkzeugen (Schatten-KI) stellt ein erhebliches Risiko für unsere Datensicherheit dar. Für dienstliche Zwecke dürfen daher ausschließlich die vom Unternehmen offiziell geprüften und bereitgestellten KI-Tools genutzt werden.

Sofern das Unternehmen "Enterprise"-Lizenzen (z. B. ChatGPT Enterprise, Microsoft 365 Copilot) bereitstellt, ist die Nutzung privater Accounts für dienstliche Zwecke untersagt.

Beschaffungsprozess: Sollten Sie ein neues KI-Tool für Ihre Abteilung benötigen, darf dieses nicht eigenmächtig beschafft werden. Bitte nutzen Sie den offiziellen Freigabeprozess, damit eine Prüfung der Datentransfers, des Serverstandorts sowie der Verarbeitungslogik durch die IT vorgenommen werden kann

Vor Nutzung eines KI-Systems muss dieses für jeweils spezifische Anwendungsbereiche freigegeben werden. Zulässig sind:

- Das System **LibreChat** in Kombination mit **AKI.IO** für folgende Anwendungsbereiche:
 - Text- und KommunikationsarbeitBeispiele:
 - E-Mails formulieren
 - Rundschreiben
 - IT-Support-Anleitungen
 - interne Dokumentation
 - Meeting-Protokolle strukturieren
 - Stellenanzeigen

- Schulungsunterlagen
- FAQ-Texte
- Wiki-Artikel
- Marketingtexte
- Übersetzungen
- Umformulierungen

Bedingungen:

- es dürfen keine echten Kundendaten enthalten sein
 - Namen MÜSSEN anonymisiert werden
 - es dürfen keine vertraulichen Verträge oder Geheimnisse eingefügt werden
-
- Programmierung und IT-Automatisierung
 - interne Dokumentation
 - Prozessbeschreibungen
 - Zusammenfassungen (auch hier anonymisiert)
 - Das System "**Perplexity**" für folgende Anwendungsbereiche:
 - Recherche technischer Informationen
 - Programmierung von Ergänzungsprogrammen für die 3D-Software

Andere Nutzungen dieser KI-Systeme sind untersagt.

2. Verbot der Verwendung anderer KI-Systeme

Unzulässig ist die Verwendung aller anderen als der soeben genannten KI-Systeme. Dies betrifft insbesondere KI-Systeme auf privaten Endgeräten und die Verwendung kostenloser KI-Systeme bzw. von Versionen, die nicht auf Unternehmensnutzer zugeschnitten sind.

Die Eingabe von Unternehmensdaten in nicht autorisierte KI-Systeme ist untersagt.

3. Wahrung von Urheberrechten

Bei der Nutzung von KI-Systemen dürfen keine Urheberrechte, Lizenzbestimmungen, Markenrechte oder Persönlichkeitsrechte verletzt werden.

4. Transparenz

Seit dem 2. August 2026 gilt in der Europäischen Union eine gesetzliche Kennzeichnungspflicht für bestimmte KI-generierte oder manipulierte Inhalte nach Artikel 50 der KI-Verordnung (EU AI Act).

Geltungsbereich:

Die Pflicht betrifft vor allem Unternehmen, gewerbliche Anbieter und Behörden, die KI in der Kommunikation oder im Marketing einsetzen. Reine Privatanwender sind ausgenommen.

Betroffene Inhalte: Gekennzeichnet werden müssen KI-generierte Bilder, Videos, Audios und Deepfakes (täuschend echte Simulationen von realen Personen, Orten oder Ereignissen) sowie Service-Chatbots.

Art der Kennzeichnung: Der Hinweis muss klar, sichtbar und direkt beim ersten Kontakt mit dem Inhalt erfolgen. Versteckte Hinweise im Kleingedruckten oder in den AGB reichen nicht aus. Zusätzlich ist eine maschinenlesbare Kennzeichnung (wie Metadaten oder

Wasserzeichen) vorgeschrieben. Das [BSI Verbraucherschutz](#) bietet hierzu hilfreiche Einschätzungen zur Erkennung und Kennzeichnung von KI-Bildern.

Beispiele:

Text-Hinweise: Beschriftungen wie „KI-generiert“, „Erstellt mit KI“ oder „AI generated“ direkt am Bild, im Video oder am Anfang eines Artikels.

Visuelle Symbole: Die von der EU bereitgestellten EU-Icons zur Kennzeichnung von KI-generierten Inhalten (z. B. für vollständig KI-erzeugte oder teilweise KI-modifizierte Inhalte).



Overlays und Wasserzeichen: Sichtbare Banner, Pop-ups oder Wasserzeichen bei realistischen Deepfake-Bildern und -Videos.

Chatbots: Ein klarer Hinweis im Chatfenster sowie in der Datenschutzerklärung, dass Nutzer mit einer KI kommunizieren.

Technische Metadaten: Unsichtbare, maschinenlesbare Markierungen in Bilddateien (wie Content Credentials), die von KI-Anbietern eingebettet werden.

5. Überprüfung der Ergebnisse (menschliche Aufsicht)

Die durch ein KI-System erzeugten Ergebnisse müssen stets durch einen Menschen überprüft werden.

Achtung: KI-Systeme neigen zu Halluzinationen und zu gut klingenden, aber falschen Ergebnissen! Prüfe jede Ausgabe eines KI-Systems kritisch! Vor allem bei Weitergabe an Dritte. Achte auf sachliche Richtigkeit, Logik und Diskriminierungsfreiheit

Die Verantwortung für die Ausgabe trägt immer der Anwender, nicht die KI.

6. Unternehmensinterne Datenschutzrichtlinie

Alle datenschutzrechtlichen Anforderungen gemäß der Datenschutzrichtlinie unseres Unternehmens gelten vollumfänglich auch für den Einsatz von KI-Systemen.

Personenbezogene Daten: Es dürfen unter keinen Umständen personenbezogene Daten von Kunden, Mitarbeitenden oder Geschäftspartnern eingegeben werden, um Verstöße gegen die DSGVO zu vermeiden.

7. Geheimnisschutz

Wir erinnern hiermit an Folgendes: Es ist unzulässig, Geschäftsgeheimnisse, unternehmensinterne und sonstige vertrauliche Informationen in KI-Systeme einzugeben.

Interne Finanzdaten, Strategiepapiere, Passwörter (Credentials) und proprietärer Quellcode dürfen nicht in KI-Systeme kopiert werden.

8. Hinweispflichten

Alle Beschäftigten sind verpflichtet, Fehler des KI-Systems, die sie bei der Verwendung von KI-Systemen bemerken, unverzüglich [der KI-Einheit und dem Geschäftsbereich] anzuzeigen. Anzeigepflichtige Fehler sind insbesondere solche, die zu unzulässigen Diskriminierungen von Personen führen können [...].

Rollen und Verantwortlichkeiten

1. ALLE Mitarbeitende der B. Schlichter GmbH & Co. KG und der Schlichter Maler und Glashandel GmbH

Jede/r Einzelne ist für die Einhaltung dieser Richtlinie, [der Datenschutz-Richtlinie] und die Einhaltung aller anwendbaren Gesetze verantwortlich.

2. KI-Team

Bei Fragen zu der Anwendung dieser Richtlinie und/oder der anwendbaren Gesetze steht unser KI-Team oder die IT-Abteilung bereit. Die IT-Abteilung ist erreichbar unter der Durchwahl 164/168, das KI-Team per E-mail unter ki-team@schlichter.biz

Meldet euch ebenfalls gerne beim KI-Team, wenn Ihr Vorschläge für die Implementierung weiterer KI-Systeme habet oder weitere mögliche Anwendungsbereiche für durch uns bereits verwendete KI-Systeme vorschlagen möchtet.

3. Geschäftsbereiche

Die Geschäftsbereiche sind verantwortlich für die Veröffentlichung von Anwendungshinweisen für spezifische in den Geschäftsbereichen verwendete KI-Systeme.

Die Geschäftsbereichsleitungen überwachen die Einhaltung dieser Richtlinie durch die ihnen zugewiesenen Mitarbeiterinnen und Mitarbeiter.

4. Geschäftsführung

Die Geschäftsführung setzt den Rahmen für die Verwendung von Künstlicher Intelligenz in unserem Unternehmen und entwickelt den Rahmen weiter.

KI-Kompetenz

Alle Beschäftigten unseres Unternehmens erhalten in regelmäßigen Abständen Schulungen zur Förderung ihrer KI-Kompetenz. Dies gilt ebenfalls für Personen, die im Auftrag unseres Unternehmens mit dem Betrieb und der Nutzung von KI-Systemen befasst sind. Inhalt dieser Schulungen sollen auch diese Richtlinie sowie die Grundlagen der KI-Regulierung sein.

Explizite Datenschutzerklärung für unsere hausinterne KI

(Version 1.0 – 13. Oktober 2026 – unter Berücksichtigung der KI-Richtlinie [1] und der EU-DSGVO)

1. Verantwortlicher und Anbieter

Rolle	Angaben
Verantwortlicher	Schlichter GmbH & Co. KG / Schlichter Maler- und Glashandel GmbH, vertreten durch die Geschäftsführung.
Datenschutz-Beauftragter	[Name], E-Mail: datenschutz@schlichter.biz , Telefon +49 123 456 7890
KI-Anbieter	AKI.IO – ein in Deutschland ansässiger Anbieter von KI-Plattformen, der sämtliche Verarbeitungstätigkeiten im Einklang mit der EU-Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG) durchführt.

2. Zweck und Rechtsgrundlage der Datenverarbeitung

Zweck	Verarbeitete Daten	Rechtsgrundlage (Art. 6 DSGVO)
Unterstützung bei Text- und Kommunikationsaufgaben (z. B. E-Mails, Dokumente, Protokolle)	• Eingabedaten (Text, Metadaten) • Anonymisierte Personen- bzw. Unternehmensbezeichnungen	Art. 6 Abs. 1 b – Verarbeitung zur Erfüllung eines berechtigten Interesses des Unternehmens (Effizienzsteigerung, Qualitätsverbesserung).

Zweck	Verarbeitete Daten	Rechtsgrundlage (Art. 6 DSGVO)
Programmierung & IT-Automatisierung (z. B. Code-Snippets, Prozessbeschreibungen)	• Technische Eingaben (Code, Befehle)	Art. 6 Abs. 1 b – Berechtigtes Interesse.
Technische Recherche (z. B. öffentliche Fachinformationen)	• Suchbegriffe, URLs	Art. 6 Abs. 1 b – Berechtigtes Interesse.
Audit- und Qualitätskontrolle (z. B. Protokollierung von KI-Nutzungen)	• Nutzungs-Logs (Benutzer-ID, Zeitstempel, Eingabekategorien)	Art. 6 Abs. 1 c – Erfüllung einer rechtlichen Verpflichtung (Nachweis- und Dokumentationspflichten).

Hinweis: Personenbezogene Daten dürfen nur verarbeitet werden, wenn sie für den jeweiligen Zweck zwingend erforderlich und zuvor **anonymisiert** bzw. **pseudonymisiert** wurden (vgl. KI-Richtlinie § 2 „Datenschutz & Sicherheit“).

3. Kategorien personenbezogener Daten

Kategorie	Beispiele	Zweck
Identifikationsdaten (nach Anonymisierung)	Platzhalter für Namen, Kundennummern, E-Mail-Adressen	Text-Generierung, Dokumentation
Kontaktdaten (anonymisiert)	Ersatz-Tokens für Telefonnummern, Adressen	Recherche, Kontextualisierung
Beschäftigtendaten (pseudonymisiert)	Rollen- bzw. Funktionsbezeichnungen	Zugriffs- und Berechtigungsmanagement
Technische Daten	IP-Adresse des Zugriffsgeräts, Browser-Informationen (Log-Daten)	Sicherheits- und Performance-Monitoring

Keine sensiblen Daten (Gesundheits-, genetische, religiöse, politische Angaben etc.) werden verarbeitet.

4. Empfänger und Datenübermittlung

Empfänger	Zweck	Drittlandtransfer?
AKI.IO (Deutschland)	Bereitstellung und Betrieb der KI-Plattform	Nein – Verarbeitung ausschließlich innerhalb der EU (EU-Datenschutzstandard).
Interne IT-Abteilung	Systemadministration, Monitoring	Nein – innerhalb des Unternehmens.

Empfänger	Zweck	Drittlandtransfer?
Externe Auftragsverarbeiter (z. B. Cloud-Infrastruktur)	Hosting, Backup	Nur, wenn der Auftragsverarbeiter EU-Standard-Vertragsklauseln (SCC) bzw. ein Äquivalent nach Art. 46 DSGVO erfüllt.

Eine Übermittlung personenbezogener Daten an Drittländer **findet nicht** statt.

5. Speicherfristen

Datenkategorie	Aufbewahrungsdauer	Grundlage
Nutzungs-Logs	12 Monate	Interne Aufbewahrungspflicht, Nachweis- und Audit-Erfordernisse.
Anonymisierte Eingabedaten (zur Modellverbesserung)	6 Monate	Optimierung der KI-Leistung; danach automatisierte Löschung.
Pseudonymisierte Beschäftigtendaten	24 Monate	Erfüllung von internen Qualitäts- und Compliance-Kontrollen.
Technische Metadaten (z. B. Fehlermeldungen)	30 Tage	Kurzfristige Fehleranalyse.

Nach Ablauf der jeweiligen Frist werden die Daten automatisch gelöscht oder endgültig anonymisiert.

6. Technische und organisatorische Maßnahmen (TOM)

AKI.IO und die Schlichter-IT setzen nach Art. 32 DSGVO folgende Maßnahmen ein:

- **Verschlüsselung** von Daten während Übertragung (TLS 1.3) und im Ruhezustand (AES-256).
- **Zugangskontrollen** (Mehr-Faktor-Authentifizierung, Rollen-basiertes Berechtigungskonzept).
- **Datenminimierung** – nur notwendige Daten werden erfasst; automatisierte Anonymisierung vor Weitergabe an die KI.
- **Audit-Logs** und **Intrusion-Detection-Systeme** zur Überwachung von Zugriffen und ungewöhnlichen Aktivitäten.
- **Regelmäßige Pen-Tests** und **Sicherheitsaudits** durch unabhängige Dienstleister.

Alle Maßnahmen entsprechen dem **Stand der Technik** und den Vorgaben des BSI-IT-Grundschatzes.

7. Rechte der betroffenen Personen

Betroffene Personen haben nach Art. 15-22 DSGVO folgende Rechte:

1. **Auskunftsrecht** – Übermittlung von Informationen über die verarbeiteten personenbezogenen Daten.
2. **Recht auf Berichtigung** – Korrektur unrichtiger Daten.
3. **Recht auf Löschung** („Recht auf Vergessenwerden“).
4. **Recht auf Einschränkung der Verarbeitung.**
5. **Recht auf Datenübertragbarkeit** (für strukturierte, gängige Formate).
6. **Widerspruchsrecht** – insbesondere gegen die Verarbeitung für Direktmarketing oder Profiling.
7. **Beschwerderecht** bei einer Aufsichtsbehörde (Landesdatenschutzbehörde Nordrhein-Westfalen).

Ausübung der Rechte:

Anfragen können schriftlich oder per E-Mail an den Datenschutz-Beauftragten (datenschutz@schlichter.biz) gerichtet werden. Die Bearbeitung erfolgt innerhalb eines Monats.

8. Auftragsverarbeitung

Mit AKI.IO besteht ein **Auftragsverarbeitungsvertrag (AVV)**, der die Vorgaben der Art. 28 DSGVO erfüllt:

- AKI.IO verarbeitet Daten ausschließlich im Auftrag und nach dokumentierten Anweisungen der Schlichter-Gruppe.
 - AKI.IO darf Daten nicht für eigene Zwecke nutzen oder an Dritte weitergeben.
 - AKI.IO garantiert die Einhaltung aller technischen und organisatorischen Maßnahmen (TOM).
-

9. Änderungen dieser Datenschutzerklärung

Änderungen und Ergänzungen dieser Datenschutzerklärung werden im Intranet veröffentlicht und den Mitarbeitenden per E-Mail mitgeteilt. Die jeweils aktuelle Fassung ist jederzeit auf der internen

10. Kontakt

Datenschutz-Beauftragter

Schlichter GmbH & Co. KG

E-Mail: datenschutz@schlichter.biz

Telefon: +49 123 456 7890

KI-Anbieter

AKI.IO – Deutschland

Web: <https://aki.io>

E-Mail: privacy@aki.io
