PERFEKTER DATENSCHUTZ

Muster KI-Richtlinie

Wir machen Ihr Franchise System **zukunfts-fit.**

April 2025

Perfekter Datenschutz (OT) GmbH
Speicherstraße 13, 60327 Frankfurt am Main

A. Richtlinie zum Einsatz künstlicher Intelligenz (KI)

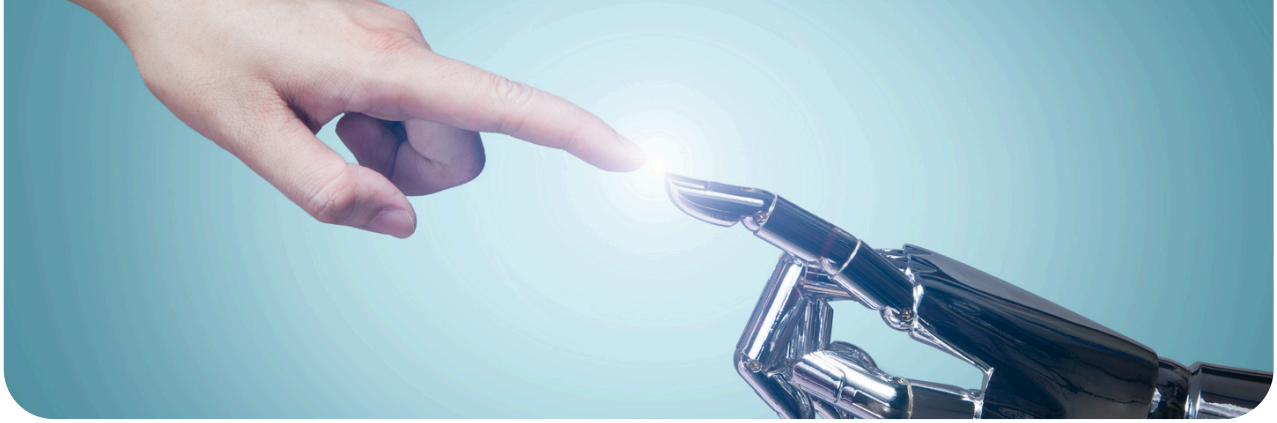
Bei der Musterfirma XYZ sollen IT-Tools zum Einsatz kommen, deren Output durch KI-Algorithmen generiert werden (nachfolgend KI-Tools genannt). Die meisten KI-Tools basieren auf einem textbasiertes Dialogsystem, das über eine Benutzerschnittstelle Eingaben (Input) entgegennimmt und dann unter Verwendung maschinellen Lernens eine Ausgabe (Output) generiert. Diese Richtlinie regelt den sicheren und rechtskonformen Einsatz von KI-Tools, insbesondere im Hinblick auf Datenschutz, Informationssicherheit und ethische Aspekte, und definiert die Rahmenbedingungen für die Nutzung.

Begrifflichkeiten und Definitionen

- Künstliche Intelligenz (KI): Computerprogramme, die maschinelles Lernen nutzen, um durch Datenanalyse Muster zu erkennen und selbstständig Aufgaben zu lösen.
- KI-System: Eine praktische Umsetzung der KI, die auf Eingaben reagiert und Ergebnisse wie Vorhersagen oder Empfehlungen erzeugt.
- Deepfakes: Durch KI erzeugte oder manipulierte Inhalte, die authentisch wirken können, müssen als solche gekennzeichnet werden.

Geltungsbereich

- Geltung für alle Beschäftigten: Diese Richtlinie gilt für alle Standorte und Beschäftigten der Musterfirma XYZ sowie für alle externen Personen, die im Auftrag der Musterfirma XYZ tätig sind und KI-Tools nutzen.
- Geltung für alle KI-Systeme- und Tools: Der Geltungsbereich dieser KI-Richtlinie umfasst alle bestehenden und zukünftigen KI-Systeme und -Tools, die im Rahmen der betrieblichen Tätigkeiten eingesetzt werden.
- Die KI-Richtlinie findet Anwendung auf jegliche Nutzung von KI durch die Beschäftigten, einschließlich der Erstellung von Inhalten, z. B. Texten, Bildern oder Videos, der Analyse von Daten, der Automatisierung von Aufgaben, der Unterstützung von Entscheidungen und sonstigen mit KI verbundenen Aktivitäten.
- Dies schließt sowohl intern entwickelte als auch von dritten Anbietern bezogene KI-Systeme, -Ergebnisse oder sonstige mit KI verbundene Leistungen ein.



Zugelassener Personenkreis

- Der Einsatz von KI-Tools ist nur nach Genehmigung durch den bzw. die Vorgesetzte oder Vorgesetzten und ggf. die IT-Abteilung zulässig.
- Der Zugriff auf KI-Tools wird nur autorisierten und geschulten Mitarbeitenden gewährt.
- Die Nutzung privat angeschaffter KI-Systeme für betriebliche Zwecke ist ohne ausdrückliche Zustimmung des Arbeitgebers untersagt.
- Durch den Arbeitgeber bereitgestellte oder im Rahmen der Arbeitsaufgaben beschaffte oder beauftragte KI-Systeme dürfen, einschließlich der mit ihnen verbundenen Benutzerkonten und erstellten Inhalte, ausschließlich für berufliche bzw. dienstliche Zwecke genutzt werden. Eine private Nutzung ist ohne Zustimmung des Arbeitgebers untersagt.

Grundsätze für den Einsatz von KI-Tool

Rechtskonformität (insbesondere DSGVO)

Die Nutzung von KI-Tools bei der Musterfirma XYZ basiert auf klar definierten Grundsätzen, um Datenschutz, Sicherheit und Rechtskonformität sicherzustellen.

- Rechtsgrundlage (Art. 6 DSGVO): Datenverarbeitung ist nur zulässig bei Einwilligung, Vertragserfüllung, rechtlicher Verpflichtung oder berechtigtem Interesse.
- Zweckbindung: Daten dürfen nur für klar definierte und rechtmäßige Zwecke verwendet werden.
- Datenminimierung: Es dürfen nur die für den jeweiligen Zweck notwendigen Daten verarbeitet werden.
- Transparenz: Betroffene Personen müssen über die Datenverarbeitung und den KI-Einsatz informiert werden, z. B. in Datenschutzhinweisen.
- Betroffenenrechte: Personen haben das Recht auf Auskunft, Berichtigung, Löschung und Widerspruch.
- Besonders sensible Daten (Art. 9 DSGVO): Die Verarbeitung von sensiblen Daten durch KI-Systeme darf nur bei zwingender Notwendigkeit erfolgen darf. Es muss sichergestellt werden, dass vor der Verarbeitung eine rechtliche Prüfung der Zulässigkeit durchgeführt und die Verarbeitung protokolliert wird. Es sollte zudem eine DSFA durchgeführt werden, wenn eine ständige Verarbeitung von besonders sensiblen Daten erforderlich ist.

Sicherheit und Kontrolle

- Technische Maßnahmen: KI-Tools müssen durch Verschlüsselung, Zugriffsbeschränkungen und Datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) gesichert sein.
- Prüfung der Outputs: Ergebnisse von KI-Tools müssen durch Mitarbeitende geprüft werden, bevor sie verwendet oder veröffentlicht werden.

Einschränkungen

- Verbotene Inputs: Keine Eingabe von Betriebsgeheimnissen, urheberrechtlich geschützten Informationen oder personenbezogenen Daten, wenn keine gültige Rechtsgrundlage vorliegt.
- Automatisierte Entscheidungen: Entscheidungen, die erhebliche Auswirkungen auf Personen haben, dürfen nur nach menschlicher Überprüfung oder mit Einwilligung erfolgen.
- Verbot der Datennutzung für KI-Training: Eingaben dürfen nicht zum Training von KI-Tools verwendet werden, wenn personenbezogene Daten enthalten sind, insbesondere wenn keine Einwilligung vorliegt, die nachträgliche Löschung nicht möglich ist, keine Transparenz über die Nutzung besteht, unzureichende Datensicherheitsmaßnahmen getroffen wurden oder unklare Verantwortlichkeiten bei Datenmissbrauch vorliegen.
- Verbot der Manipulation: Jegliche Eingaben zur Manipulation des KI-Systems sind untersagt. Dies umfasst alle Versuche, das KI-System zu täuschen, zu manipulieren oder dessen Ergebnisse absichtlich zu verzerren. Dazu zählen unter anderem das Eingeben falscher, irreführender oder irreführend strukturierter Daten sowie das Umgehen von Sicherheitsmechanismen und Eingabebeschränkungen.

Grenzen der Nutzung von KI-Tools

- Die Verwendung von:
  - Betriebs- und Geschäftsgeheimnissen,
  - urheberrechtlich geschützten Informationen, an denen die Musterfirma XYZ keine Nutzungsrechte besitzt,
- zur Erstellung von Inputs in KI-Systemen ist untersagt.

- Ebenfalls untersagt ist die Nutzung von personenbezogenen Daten (z.B. von Kundinnen und Kunden, Beschäftigten, sonstigen Vertragspartnern oder Dritten) zur Erstellung von Inputs, es sei denn, es liegt eine gültige Einwilligung vor oder es existiert eine andere rechtliche Grundlage.
- Der Einsatz von KI-Tools ist nur zulässig, wenn diese Datenschutzanforderungen entsprechen und sichergestellt ist, dass Eingabedaten nicht zu Trainingszwecken weitegegeben wird (insbesondere bei der Nutzung von ChatGPT). Für die Nutzung von KI-Tools müssen geeignete Sicherheits- und Datenschutz-einstellungen vorgenommen werden, die eine Weitergabe oder missbräuchliche Verwendung von Daten verhindern (z.B. Die Nutzung von ChatGPT ausschließlich in der Pro-Version).
- Sofern Outputs von KI-Tools durch die Musterfirma XYZ gegenüber Dritten verwendet werden, müssen diese klar und deutlich als maschinengeneriert gekennzeichnet werden, um Transparenz sicherzustellen und ethische Standards einzuhalten. Die Kennzeichnungspflicht gilt sowohl intern als auch extern, um mögliche Täuschungen oder ethisch fragwürdige Anwendungen, wie etwa durch Deepfakes, zu verhindern.
- Zudem ist darauf zu achten, dass bei der Verwendung von KI-Systemen regelmäßig geprüft wird, ob diese den aktuellen rechtlichen und ethischen Anforderungen entsprechen, und ob alle genutzten Tools entsprechend den Unternehmensrichtlinien zugelassen sind.

Sanktionen

- Verstöße gegen diese Richtlinie können arbeitsrechtliche Konsequenzen nach sich ziehen und rechtliche Haftung auslösen.

B. Richtlinie zur Nutzung von Cloud-Services

Die Nutzung von Cloud-Services ist ein wesentlicher Bestandteil moderner IT-Strategien und bietet erhebliche Vorteile wie Flexibilität, Kosteneffizienz und Skalierbarkeit. Trotz dieser Vorteile ist die Gewährleistung des Schutzes personenbezogener Daten bei der Nutzung solcher Dienste von zentraler Bedeutung. Diese Richtlinie beschreibt die Anforderungen und Standards für den sicheren und datenschutzkonformen Einsatz von Cloud-Services innerhalb der Musterfirma XYZ.

Begrifflichkeiten und Definitionen

- Künstliche Intelligenz (KI): Computerprogramme, die maschinelles Lernen nutzen, um durch Datenanalyse Muster zu erkennen und selbstständig Aufgaben zu lösen.
- KI-System: Eine praktische Umsetzung der KI, die auf Eingaben reagiert und Ergebnisse wie Vorhersagen oder Empfehlungen erzeugt.
- Deepfakes: Durch KI erzeugte oder manipulierte Inhalte, die authentisch wirken können, müssen als solche gekennzeichnet werden.

Geltungsbereich

- Diese Richtlinie gilt für alle Mitarbeitenden der Musterfirma XYZ sowie für externe Personen, die im Auftrag der Musterfirma XYZ tätig sind und Cloud-Services nutzen. Der Anwendungsbereich umfasst alle Arten von Cloud-Diensten, sei es zur Datenspeicherung, Verarbeitung oder zum Datentransfer. Es sind sowohl lokale als auch globale Anbieter von Cloud-Services in diese Vorgaben einzubeziehen.

Anforderungen und Grundsätze

Rechtskonformität (insbesondere DSGVO)

Der Einsatz von Cloud-Services muss stets im Einklang mit den geltenden Datenschutzgesetzen, insbesondere der Datenschutz-Grundverordnung (DSGVO), erfolgen. Vor der Nutzung eines Cloud-Dienstes ist ein Auftragsverarbeitungsvertrag (AVV) mit dem Anbieter abzuschließen, um die Rechte und Pflichten beider Parteien zu regeln. Zusätzlich dürfen Daten nur in Länder übertragen werden, die ein angemessenes Datenschutzniveau gemäß der DSGVO gewährleisten.

Datenminimierung

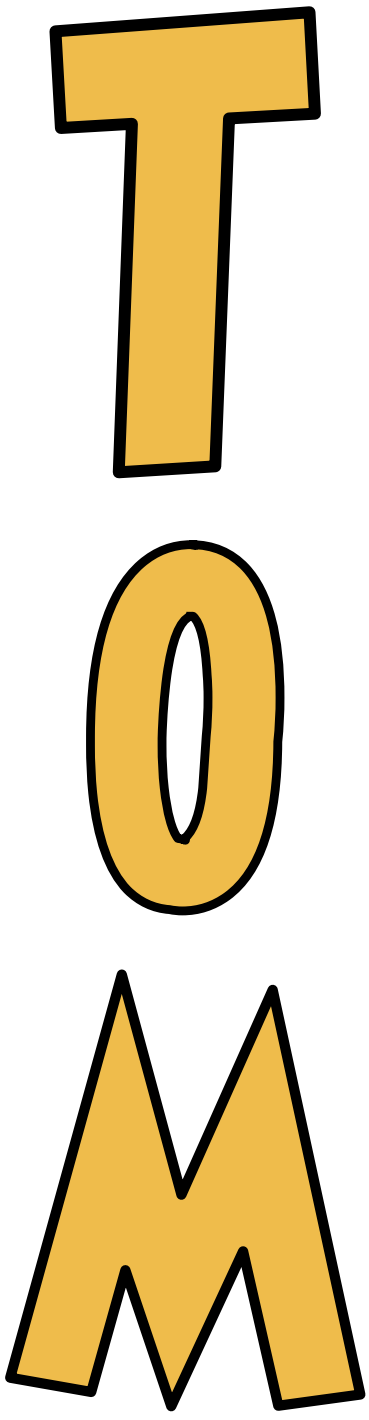
Im Rahmen der Nutzung von Cloud-Services ist das Prinzip der Datenminimierung strikt einzuhalten. Es dürfen ausschließlich die für den jeweiligen Verarbeitungszweck erforderlichen Daten in die Cloud hochgeladen oder verarbeitet werden. Besondere Vorsicht ist bei der Verarbeitung sensibler Daten geboten, die vorzugsweise anonymisiert oder pseudonymisiert werden sollten, um das Risiko eines Datenmissbrauchs zu minimieren.

Transparenz

Betroffene Personen sind über die Verarbeitung ihrer Daten in der Cloud umfassend zu informieren. Diese Transparenzpflicht umfasst insbesondere:

- Den Zweck und die Rechtsgrundlage der Verarbeitung.
- Die Art der erhobenen und verarbeiteten Daten.
- Die Identität der eingesetzten Cloud-Anbieter sowie deren Standort.

Technische und organisatorische Maßnahmen (TOMs)



Verschlüsselung:

Alle personenbezogenen Daten, die in der Cloud verarbeitet werden, müssen vor der Übertragung verschlüsselt werden. Die eingesetzten Verschlüsselungsverfahren müssen den aktuellen Sicherheitsstandards entsprechen und regelmäßig überprüft werden, um sicherzustellen, dass sie den Anforderungen gerecht werden.

Zugriffsbeschränkungen:

Die Zugriffsrechte auf Cloud-Services müssen strikt reglementiert sein. Nur autorisierte Mitarbeitende dürfen Zugriff auf die Daten erhalten. Hierbei sind rollenbasierte Berechtigungssysteme zu implementieren, um sicherzustellen, dass nur diejenigen Mitarbeitenden Zugriff haben, die diesen für ihre Aufgaben benötigen.

Sicherheitsüberprüfungen:

Cloud-Dienste sind regelmäßig auf Sicherheitslücken und Schwachstellen zu überprüfen. Anbieter müssen nachweisen können, dass sie umfassende technische und organisatorische Maßnahmen ergriffen haben, um die Sicherheit der verarbeiteten Daten zu gewährleisten. Zertifizierungen wie ISO 27001 dienen als Indikator für die Einhaltung von Sicherheitsstandards.

Einschränkungen

- Die Nutzung privater Cloud-Dienste für betriebliche Zwecke ist untersagt, sofern keine ausdrückliche Genehmigung der IT-Abteilung vorliegt. Zudem dürfen Cloud-Dienste, die personenbezogene Daten ohne Einwilligung der betroffenen Personen oder ohne rechtliche Grundlage verarbeiten, nicht verwendet werden. Die IT-Abteilung ist angehalten, solche Dienste vorab zu prüfen und ggf. zu sperren.

Datenschutz-Folgenabschätzung (DSFA)

- Vor der Einführung eines neuen Cloud-Dienstes ist eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen, wenn die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen könnte. Kriterien, die eine DSFA erforderlich machen, umfassen:
- Die Verarbeitung sensibler personenbezogener Daten.
- Die Verarbeitung großer Datenmengen.
- Der Einsatz neuer Technologien oder Verfahren, die eine systematische Überwachung ermöglichen.

Verantwortung

- Die Verantwortung für die Auswahl und regelmäßige Überprüfung der eingesetzten Cloud-Dienste liegt bei der IT-Abteilung der Musterfirma XYZ. Darüber hinaus sind Datenschutzbeauftragte frühzeitig in den Prozess einzubinden, insbesondere wenn die Einführung neuer Dienste geplant ist. Sie stellen sicher, dass alle datenschutzrechtlichen Anforderungen erfüllt werden.

Sanktionen

- Verstöße gegen diese Richtlinie werden nicht toleriert und können sowohl arbeitsrechtliche Konsequenzen als auch rechtliche Haftung nach sich ziehen. Alle Mitarbeitenden sind dazu verpflichtet, die in dieser Richtlinie festgelegten Vorgaben einzuhalten.

PERFEKTER
DATENSCHUTZ

Jetzt KI Kompetenz aufbauen mit unserer KI-Schulungsstrategie

Jetzt unverbindliches Angebot erhalten.
Schreiben Sie uns:
info@perfekter-datenschutz.de

Perfekter Datenschutz (OT) GmbH
Speicherstraße 13, 60327 Frankfurt am Main