AI Policy

Präambel

Dieses Dokument („AI Policy“) regelt den Einsatz von Künstlicher Intelligenz („KI“) in der brandcom GmbH (im Folgenden „Agentur“). Ziel ist es, Text- und Bildmaterial für unsere Kunden sowohl innovativ als auch verantwortungsvoll zu erstellen. Dabei legen wir besonderen Wert auf die Einhaltung aller relevanten Datenschutzbestimmungen (insbesondere DSGVO), auf Vertraulichkeit, Qualität und ethische Grundsätze.

Die Agentur verfolgt das Ziel, Kundendaten und KI-Modelle in einem sicheren, transparenten und rechtskonformen Umfeld zu nutzen, um den größtmöglichen Mehrwert für ihre Kunden zu erzielen. Diese AI Policy bietet einen Rahmen, der von allen Mitarbeiterinnen und Mitarbeitern einzuhalten ist, damit die Verarbeitung von Kundendaten und die Erstellung von KI-generierten Inhalten reibungslos funktioniert und potenzielle Risiken minimiert werden.

Hinweis: Diese Richtlinie dient als verbindlicher Leitfaden für unsere Arbeitsabläufe. Bei spezifischen rechtlichen Fragen empfehlen wir, qualifizierte Rechtsberatung in Anspruch zu nehmen.

1. Geltungs- und Anwendungsbereich

1. Diese Richtlinie ist für alle internen Mitarbeiterinnen und Mitarbeiter sowie beauftragte Subunternehmer verbindlich.
2. Die AI Policy findet Im Verhältnis zu den Kunden innerhalb der gemeinsamen Projektarbeit ab sofort Anwendung.
3. Die AI Policy ergänzt die bestehenden Unternehmensrichtlinien, darunter insbesondere unsere Datenschutzrichtlinie, IT-Sicherheitsrichtlinie, die AGB und die ADV.

2. Grundsätze und Ziele

1. **Datenschutz und Rechtmäßigkeit**
   Die brandcom GmbH verpflichtet sich, die Vorgaben der DSGVO sowie relevanter

Branchenstandards einzuhalten. Personenbezogene Daten, geistiges Eigentum sowie internes Firmen-Know-How werden nur verarbeitet, wenn eine geeignete Rechtsgrundlage vorliegt (z.B. Einwilligung des Betroffenen oder berechtigtes Interesse).

2. **Transparenz und Ethische Verantwortung**
   Wir machen gegenüber unseren Kunden transparent, wenn KI-Systeme an der Erstellung von Inhalten beteiligt sind. Jeder Mitarbeiter achtet darauf, dass die erstellten Texte und Bilder keine diskriminierenden, diffamierenden oder sonst wie unzulässigen Inhalte enthalten.
3. **Risikobewertung**
   Vor Einführung neuer Tools oder Workflows erfolgt eine strukturierte Prüfung möglicher Risiken, insbesondere wenn personenbezogene Daten verarbeitet werden. Die Risikobewertung erfolgt anhand folgender Kriterien:

   - Handelt es sich um sensible oder personenbezogene Daten?
   - Wird der KI-Dienst von einem Drittland-Anbieter betrieben?
   - Ist eine vertragliche Absicherung durch eine AVV oder Standardvertragsklauseln möglich?
   - Besteht ein erhöhtes Risiko von Diskriminierung oder Intransparenz im Output?
   - Können Kundenrechte (z. B. Widerruf, Korrektur) gewährleistet werden?

3. Nutzung von KI-Systemen und Tools

1. **Zulässige Tools**

   - Logicc dient bei brandcom als zentrale Plattform für Textgenerierung. Die Plattform stellt sicher, dass die Daten den europäischen Datenraum nicht verlassen und die eingegebenen Daten auch nicht zum Training weiter verwendet werden. Darunter die Modelle:
     - Claude 3.7 Sonnet
     - Gemini 2.0 Flash
     - Llama 3.3
     - GPT 4.0
     - Mixtral Small
   - Diese Modelle werden auch innerhalb des Tools **GitHub Co-Pilots** eingesetzt.
   - **Midjourney** sowie **Ideogram** zur Bildgenerierung. Wir nutzen ausschließlich die Pro-Varianten, bei der die generierten Bilder nicht öffentlich zugänglich

sind. Dies gewährleistet, dass kundenbezogene Bildinhalte vertraulich bleiben.
- Bevor neue KI-Modelle in Kundenprojekten eingesetzt werden, müssen sie von der IT-Sicherheit, den KI-Spezialisten oder – falls erforderlich – von der Geschäftsführung freigegeben werden. Zur Exploration ist ein neues Modell ohne kundenbezogenen Daten zulässig.

2. Prompt-Design und Eingaberegeln

- Generell ist beim Erstellen von Prompts auf Datenminimierung zu achten. Sensibles oder geschütztes Material ist vor Eingabe zu pseudonymisieren oder zu anonymisieren.
- **Verboten** ist die Eingabe von Passwörtern, Zugangsdaten, Bankinformationen, Gesundheitsdaten oder ähnlichen sensiblen Personendaten, es sei denn, dies ist vertraglich ausdrücklich erlaubt und DSGVO-konform abgesichert.
- Bei der Nutzung dieser KI-Systeme sind Mitarbeiter verpflichtet, ausschließlich solche Kundendaten zu verwenden, welche für die jeweilige Aufgabenstellung notwendig sind und deren Verarbeitung vorab mit dem Kunden vertraglich vereinbart oder anderweitig genehmigt wurde.
- Personalisierte oder identifizierende Kundendaten dürfen nur nach ausdrücklicher Einwilligung des Kunden oder auf Basis einer ausreichenden Rechtsgrundlage verwendet werden. Ansonsten sind diese Daten zu anonymisieren oder zu pseudonymisieren.

3. Verbotene Nutzung

KI darf nicht in folgenden Kontexten verwendet werden:

- Verstöße gegen Datenschutzrechte
- Manipulative Gestaltung von Benutzeroberflächen
- Erstellung von irreführenden oder falschen Darstellungen in Werbemaßnahmen
- Eingabe von vertraulichen, geschützten Informationen ohne entsprechende Rechtsgrundlage

4. Prüfung und Nachbearbeitung des Outputs

- Alle KI-generierten Inhalte (Texte, Bilder) sind vor der Weitergabe an Kunden fachlich zu überprüfen, damit keine sensiblen Informationen preisgegeben werden oder Rechtsverletzungen entstehen.
- Sofern die Inhalte externe Veröffentlichung finden (z.B. Marketingkampagnen), stellt das Projektteam sicher, dass der KI-Output den Kundenanforderungen und branchenüblichen Standards entspricht.

4. Vertraulichkeit und Geheimhaltung

1. **Allgemeine Geheimhaltungspflicht**
   Alle Mitarbeiter sind zur Verschwiegenheit über Geschäfts- und Betriebsgeheimnisse der Kunden verpflichtet. Diese Pflicht besteht auch über die Beendigung des Arbeitsverhältnisses hinaus.
2. **Umgang mit sensiblen Daten**
   Insbesondere Unterlagen, die Betriebs- oder Geschäftsgeheimnisse enthalten (etwa Prototypen, interne Kommunikationsdokumente, Kundendatenbanken), dürfen nur auf freigegebenen Systemen verarbeitet und nicht an unbefugte Dritte weitergegeben werden.
3. **Externe KI-Tools**
   Bei der Nutzung externer KI-Dienste ist zu prüfen, ob Daten verschlüsselt übertragen werden und ob der Dienst die Daten dauerhaft speichert. Sensible Daten sind, soweit möglich, vorab zu anonymisieren. Verstöße gegen diese Vorgaben können zu erheblichen Reputations- und Haftungsschäden führen.

5. Urheberrechte und Nutzungsrechte

1. **KI-generierte Inhalte**
   Die urheberrechtliche Einordnung von KI-generierten Werken ist nach aktuellem Stand nicht abschließend geklärt. Die Agentur nimmt jedoch alle notwendigen Schritte vor, um sicherzustellen, dass aus Sicht des Kunden weitestgehende Nutzungsrechte an den generierten Inhalten übertragen werden.
2. **Rechteübertragung an den Kunden**
   Soweit rechtlich möglich, räumt die Agentur dem Kunden im Rahmen der vertraglichen Vereinbarungen (z.B. gemäß AGB oder Projektvertrag) die ausschließlichen Nutzungsrechte an den finalen Texten und Bildern ein.
3. **Urheberrechtliche Absicherung von KI-generierten Inhalten:**

   - KI-Outputs werden nur verwendet, wenn deren Nutzungsbedingungen eine kommerzielle Weiterverwendung ohne Rechteverletzung ermöglichen.
   - Bei Unsicherheiten wird der Kunde darüber transparent informiert.

6. Verantwortlichkeiten und Rollen

1. **Projektmanager**

- Koordiniert die Anforderungen mit dem Kunden und sorgt für schriftliche Freigaben (z.B. ADV, Freigabe zur Datennutzung)

2. **Anwender**
   - Alle Mitarbeiter, die aktiv KI-Systeme zur Inhaltserstellung oder -bearbeitung einsetzen.
   - Verantwortlich für die rechtmäßige und zweckgebundene Nutzung der KI-Tools gemäß dieser Policy.
   - Verpflichtet zur sorgfältigen Prüfung aller KI-generierten Inhalte vor der Weitergabe an Kunden.
3. **KI-Spezialisten**
   - Verantwortlich für die Qualitätskontrolle der Modelle sowie für den technischen Support bei Fragen zur KI-Nutzung.
   - Prüfen neue Tools (inkl. Datensicherheit, Lizenz- und Vertragsfragen) und führen eine Risiko- sowie Datenschutzbewertung durch.
4. **Datenschutzbeauftragter**
   - Ist für alle Fragen rund um die Einhaltung datenschutzrechtlicher Vorgaben zuständig.
5. **Geschäftsführung**
   - Übernimmt die Gesamtverantwortung für die Einhaltung dieser AI Policy.
   - Entscheidet über neue strategische Richtungen im KI-Bereich und behält sich vor, bei schwerwiegenden Verstößen einschneidende Maßnahmen zu ergreifen.

7. IT-Sicherheit

1. **Sicherheitsvorfälle**
   Bei potenziellen oder tatsächlichen Datenlecks oder Sicherheitsvorfällen ist umgehend der IT-Sicherheitsbeauftragte und die Geschäftsführung zu informieren. Ggf. ist der Datenschutzbeauftragte hinzuzuziehen und eine Meldung an die Aufsichtsbehörde vorzunehmen (Art. 33 DSGVO).

8. Schulungen und Sensibilisierung

1. **Regelmäßige Trainings**

   - Mindestens einmal pro Jahr werden Mitarbeiter zu den Themen Datenschutz, Umgang mit KI-Systemen (Prompt-Design, Datenminimierung) und ethische Gesichtspunkte geschult.

   - Neue Mitarbeiter erhalten im Onboarding-Prozess eine Einweisung in diese AI Policy.
2. **Fachlicher Austausch**
   Die KI-Spezialisten organisieren in regelmäßigen Abständen interne Sessions, in denen Anwendungsfälle, Verbesserungspotenziale und mögliche Risiken (z.B. Bias, Urheberrecht) diskutiert werden. Ziel ist ein stetiger Lernprozess, damit die Agentur innovativ und sicher im KI-Bereich agiert.

9. Sanktionen und Konsequenzen bei Verstößen

1. **Arbeitsrechtliche Maßnahmen**
   Verstöße gegen diese AI Policy können je nach Schweregrad arbeitsrechtliche Konsequenzen nach sich ziehen (z.B. Abmahnung, Kündigung). Dies gilt insbesondere bei grob fahrlässigem oder vorsätzlichem Umgang mit Kundendaten.
2. **Haftung und Regress**
   Sollte es zu Datenpannen oder sonstigen Schäden kommen, kann die Agentur Regressansprüche gegen verantwortliche Mitarbeiter geltend machen, wenn diese vorsätzlich oder grob fahrlässig gehandelt haben.
3. **Straf- oder Ordnungswidrigkeitenrecht**
   Darüber hinaus können Verstöße gegen datenschutzrechtliche Vorgaben auch zu Bußgeldern oder strafrechtlichen Konsequenzen führen. Die Agentur arbeitet in solchen Fällen mit den zuständigen Behörden zusammen und behält sich weitere rechtliche Schritte vor.

10. Inkrafttreten und Geltungsdauer

1. Diese AI Policy tritt mit Freigabe durch die Geschäftsführung in Kraft und ist ab diesem Zeitpunkt für alle Mitarbeiterinnen und Mitarbeiter der brandcom GmbH verbindlich.
2. Die Gültigkeit dieser AI Policy bleibt bestehen, bis sie durch eine aktualisierte Fassung ersetzt wird oder ausdrücklich außer Kraft gesetzt wird.
3. Änderungen oder Ergänzungen werden schriftlich bekanntgegeben (z.B. via E-Mail, Slack) und treten zum darin definierten Zeitpunkt in Kraft.

Ort, Datum: _____
Geschäftsführung (GF): _____

Zusatz-Bestimmung für ADV

3.7. Der Auftragnehmer setzt zur Erfüllung der vereinbarten Leistungen im Rahmen der Zusammenarbeit teilweise Systeme zur automatisierten Verarbeitung der Daten auf Basis Künstlicher Intelligenz (KI) ein, insbesondere zur Unterstützung von Text- und Bildgenerierung. Die dabei eingesetzten Tools und Systeme (z. B. ChatGPT, Claude, Midjourney, Ideogram) werden ausschließlich unter Einhaltung der geltenden datenschutzrechtlichen Anforderungen eingesetzt. Eine Verarbeitung personenbezogener Daten durch solche Systeme erfolgt nur nach unterzeichneter ADV durch den Auftraggeber, unter Berücksichtigung der Zweckbindung und auf Basis vertraglicher oder gesetzlicher Rechtsgrundlagen.

Der Auftragnehmer verweist ergänzend auf die unternehmensinterne AI Policy in ihrer jeweils aktuellen Fassung. Diese regelt detailliert den verantwortungsvollen Umgang mit KI, einschließlich Datenminimierung, Informationspflichten, interner Zugriffsbeschränkungen sowie technischer und organisatorischer Schutzmaßnahmen. Die AI Policy kann dem Auftraggeber auf Wunsch zur Verfügung gestellt werden.