rankscan

rankscan.ai

VERTRAG · DATENSCHUTZ

Auftragsverarbeitungsvertrag

nach Art. 28 DSGVO und Art. 9 DSG, mit den Standardvertragsklauseln der Europäischen Kommission

VERANTWORTLICHER

Der Kunde, wie im Kundenkonto von RankScan angegeben

AUFTRAGSVERARBEITER

Klarplan AG, Sälihalde 11, 6005 Luzern, Schweiz, Anbieterin von RankScan

FASSUNG

1.2 vom 28.10.2026

GELTENDE FASSUNG

rankscan.ai/de/data-processing-agreement

Inhalt

Teil A – Rahmenbestimmungen 3
- A.1 Begriffe 3
- A.2 Geltung, Laufzeit und Fassungen 3
- A.3 Rangfolge 4
- A.4 Gegenstand und Rollen 4
- A.5 Weisungen (zu Klausel 7.1) 6
- A.6 Schweizer Datenschutzrecht 6
- A.7 Nachweise und Prüfungen (zu Klausel 7.6) 7
- A.8 Unterauftragsverarbeiter (zu Klausel 7.7) 7
- A.9 Ende des Tarifs, Ruhephase, Rückgabe und Löschung (zu Klausel 10 Buchstabe d) 7
- A.10 Export, einzelne Daten und Betroffenenanfragen (zu Klausel 8) 9
- A.11 Haftung 10
- A.12 Anwendbares Recht, Gerichtsstand und Sprache 11

Teil B – Standardvertragsklauseln 12
- Abschnitt I 12
- Abschnitt II – Pflichten der Parteien 13
- Abschnitt III – Schlussbestimmungen 17

Anhang I – Liste der Parteien 19

Anhang II – Beschreibung der Verarbeitung 20
- 1. Abgrenzung nach Vorgang 20
- 2. Kategorien betroffener Personen 20
- 3. Kategorien personenbezogener Daten 21
- 4. Sensible Daten (zu Klausel 7.5) 21
- 5. Art der Verarbeitung 22
- 6. Zwecke 22
- 7. Dauer der Verarbeitung 22
- 8. Verarbeitung durch Unterauftragsverarbeiter 24

Anhang III – Technische und organisatorische Massnahmen 25

Anhang IV – Liste der Unterauftragsverarbeiter 29
- Dienste ohne Auftragsverarbeitung 35

Auftragsverarbeitungsvertrag (AVV) RankScan zwischen dem Kunden (Verantwortlicher) und der Klarplan AG, Sälihalde 11, 6005 Luzern, Schweiz, Anbieterin von RankScan (Auftragsverarbeiter).

Dieser Vertrag besteht aus zwei Teilen. Teil A ergänzt die Standardvertragsklauseln. Teil B enthält die Standardvertragsklauseln der Europäischen Kommission nach Art. 28 Abs. 7 DSGVO (Durchführungsbeschluss (EU) 2021/915) mit den Anhängen I–IV.

TEIL A

Rahmenbestimmungen

Teil A ergänzt Teil B nach Klausel 2 Buchstabe b. Keine Bestimmung von Teil A darf so ausgelegt werden, dass sie Teil B unmittelbar oder mittelbar widerspricht oder die Rechte betroffener Personen beschneidet.

A.1 Begriffe

1. **Nutzungsvertrag:** der Vertrag über die Nutzung von RankScan nach den Allgemeinen Geschäftsbedingungen der Klarplan AG (AGB). Er beginnt mit der Registrierung und endet mit der Löschung des Kundenkontos.
2. **Kundenkonto:** das Konto des Kunden in RankScan mit seinen Websites (Properties), Teammitgliedern und Daten.
3. **Teammitglieder:** alle Personen mit Zugang zum Kundenkonto. Ihre Rollen sind Inhaber, Admin und Mitglied. Der Inhaber ist die Person, die im Kundenkonto als Inhaber eingetragen ist. Er hat immer die Rechte eines Admins. Hat ein Kundenkonto keinen Inhaber, nimmt ein Admin die Rechte des Inhabers nach diesem Vertrag wahr.
4. **Tarif:** ein laufendes kostenpflichtiges Abonnement (Abo), eine laufende Testphase oder ein Tarif, den die Klarplan AG mit dem Kunden einzeln vereinbart hat.
5. **Testkonto:** ein Kundenkonto, dessen einziger Tarif eine Testphase war.
6. **Ruhephase:** die Zeit, in der ein Kundenkonto ohne Tarif besteht (A.9 Ziffer 2).
7. **Kundendaten:** die personenbezogenen Daten, die die Klarplan AG nach Anhang II im Auftrag des Kunden verarbeitet.
8. **Unterauftragsverarbeiter:** ein Unterauftragsverarbeiter nach Klausel 7.7. Die vereinbarte Liste ist Anhang IV.
9. **Superadmin:** eine Person der Klarplan AG mit Zugriff auf alle Kundenkonten für Betrieb und Support.

A.2 Geltung, Laufzeit und Fassungen

1. Dieser Vertrag gilt für jeden Kunden, soweit die Klarplan AG für ihn Kundendaten verarbeitet. Er ist Bestandteil des Nutzungsvertrags. Er gilt mit der Annahme der AGB bei der Registrierung. Für Kunden, die sich vor der Veröffentlichung der ersten Fassung registriert haben, gilt Ziffer 8.
2. Auf Wunsch stellt die Klarplan AG eine unterzeichnete Fassung zur Verfügung. Inhaltlich gilt dieselbe Fassung.
3. Dieser Vertrag gilt, bis die Klarplan AG alle Kundendaten nach A.9 gelöscht hat. Für verbleibende Daten nach A.9 Ziffer 7 gilt er bis zu deren Löschung. Das Ende eines Tarifs beendet ihn nicht.

4. Jede Fassung trägt eine Nummer und ein Datum. Die geltende Fassung steht unter https://rankscan.ai/de/data-processing-agreement (englische Übersetzung: https://rankscan.ai/data-processing-agreement). Frühere Fassungen stellt die Klarplan AG auf Anfrage zur Verfügung.
5. Teil B ändert die Klarplan AG nicht. Änderungen von Anhang IV richten sich nach Klausel 7.7 Buchstabe a und A.8.
6. Änderungen von Teil A und der Anhänge I–III kündigt die Klarplan AG mindestens 30 Tage vorher per E-Mail an den Inhaber und die Admins an. Die Ankündigung nennt den Tag, an dem die Änderung wirksam wird. Der Kunde kann bis zu diesem Tag in Textform widersprechen. Widerspricht er nicht, wird die Änderung an diesem Tag für ihn wirksam. Widerspricht er, gilt für ihn die bisherige Fassung weiter. Die Klarplan AG kann den Nutzungsvertrag dann nach den AGB kündigen. Eine Änderung, die den Schutz der Kundendaten mindert, wird nur mit Zustimmung des Kunden in Textform wirksam.
7. Ziffer 6 regelt abschliessend, wie Änderungen dieses Vertrags wirksam werden. Die Regel der AGB, nach der Schweigen als Zustimmung zu geänderten AGB gilt, gilt für diesen Vertrag nicht.
8. **Bestandskunden.** Für Kunden, die sich vor der Veröffentlichung der ersten Fassung dieses Vertrags registriert haben, gilt:
   - 8.1 Die Klarplan AG sendet dem Inhaber und den Admins diesen Vertrag per E-Mail und fordert den Kunden auf, ihn innerhalb von 30 Tagen nach Erhalt ausdrücklich in Textform anzunehmen, zum Beispiel per E-Mail an hello@rankscan.ai. Die Mitteilung nennt das Ende dieser Frist.
   - 8.2 Dieser Vertrag gilt ab Eingang der ausdrücklichen Annahme des Kunden bei der Klarplan AG, sofern die Parteien keinen späteren Beginn vereinbaren. Schweigen oder die blosse Weiternutzung von RankScan ersetzen die Annahme nicht. Die Klarplan AG dokumentiert die Annahme und die angenommene Fassung.
   - 8.3 Lehnt der Kunde den Vertrag ab oder nimmt er ihn nicht innerhalb der Frist nach Ziffer 8.1 an, kann die Klarplan AG den Nutzungsvertrag nach den AGB kündigen. Bestehende gesetzliche und vertragliche Datenschutzpflichten bleiben unberührt.

A.3 Rangfolge

Bei Widersprüchen gilt diese Rangfolge: Teil B mit den Anhängen I–IV, dann Teil A, dann die AGB. Die Datenschutzerklärung regelt nur die Verarbeitungen, für die die Klarplan AG selbst verantwortlich ist.

A.4 Gegenstand und Rollen

1. Die Klarplan AG verarbeitet Kundendaten nur für die Zwecke in Anhang II, Abschnitt 6.
2. Für welche Vorgänge die Klarplan AG Auftragsverarbeiter und für welche sie selbst Verantwortlicher ist, regelt Anhang II, Abschnitt 1. Massgeblich ist der Vorgang, nicht die Datenkategorie.
3. **Websites Dritter.** Der Kunde bestimmt, welche Websites, Wettbewerber, Keywords und Prompts RankScan überwacht. RankScan verarbeitet dafür auch öffentliche Inhalte Dritter: Websites der Wettbewerber, Suchergebnisse, Antworten von KI-Assistenten und Seiten, die diese Antworten zitieren. Diese Verarbeitung erfolgt im Auftrag des Kunden. Der Kunde stellt sicher, dass er die Inhalte analysieren lassen darf und dass für die Verarbeitung eine Rechtsgrundlage besteht.

4. **Kunden, die selbst im Auftrag handeln.** Verarbeitet der Kunde mit RankScan Daten, für die ein Dritter (Endkunde) verantwortlich ist, gilt zusätzlich:

   4.1 Der Kunde handelt gegenüber dem Endkunden als Auftragsverarbeiter. Die Klarplan AG ist sein Unterauftragsverarbeiter (Art. 28 Abs. 4 DSGVO, Art. 9 Abs. 3 DSG). Dieser Vertrag ist dann der Vertrag zwischen Auftragsverarbeiter und Unterauftragsverarbeiter. Die Rechte, die Teil B dem Verantwortlichen gibt, übt der Kunde gegenüber der Klarplan AG aus. Seine Pflichten gegenüber dem Endkunden bleiben unberührt.

   4.2 Der Kunde sichert zu, dass seine Weisungen den Weisungen des Endkunden entsprechen und dass der Endkunde dem Einsatz der Klarplan AG und der Unterauftragsverarbeiter nach Anhang IV zugestimmt hat.

   4.3 Die Klarplan AG nimmt Weisungen nur vom Kunden an. Mitteilungen nach Teil B richtet sie an den Kunden. Der Kunde leitet sie an den Endkunden weiter.

   4.4 Prüfungen und Auskünfte für den Endkunden verlangt der Kunde. Ein Endkunde kann diesem Vertrag nach Klausel 5 beitreten.

5. **Microsoft Copilot auf Weisung des Kunden.**

   5.1 Wählt der Kunde für eine Website den KI-Assistenten Microsoft Copilot, weist er die Klarplan AG an, die Prompts dieser Website über den technischen Integrationsdienstleister cloro (Anhang IV Nr. 7) an den Dienst Microsoft Copilot zu übermitteln.

   5.2 Microsoft verarbeitet und beantwortet die Prompts als eigenständiger Verantwortlicher nach den jeweils dort geltenden Nutzungs- und Datenschutzbestimmungen. Microsoft ist kein Unterauftragsverarbeiter der Klarplan AG; zwischen der Klarplan AG und Microsoft besteht kein Vertragsverhältnis. Die Weiterleitung an Microsoft stellt eine Datenbekanntgabe des Kunden an einen Dritten dar. Für diese Bekanntgabe stellt der Kunde eine eigene Rechtsgrundlage nach DSGVO bzw. eine Rechtfertigung nach DSG sicher, soweit nötig. Microsoft verarbeitet Daten typischerweise auch ausserhalb der Schweiz und der EU/des EWR (insbesondere in den USA).

   5.3 Microsoft behält sich nach eigenen Bestimmungen vor, übermittelte Prompts zur Bereitstellung, Analyse und Weiterentwicklung eigener Dienste zu nutzen oder durch Personal prüfen zu lassen. Die Klarplan AG hat keinen Einfluss auf die Speicherdauer, Weiterverarbeitung oder Löschung von Daten bei Microsoft und kann eine Löschung dort weder veranlassen noch überprüfen.

   5.4 Die technische Abfrage erfolgt über cloro als Vermittlungsdienst. cloro stellt die Anfragen über die öffentlich zugängliche Oberfläche von Microsoft Copilot. cloro sichert den Abfrageweg vertraglich nicht zu und kündigt technische Anpassungen nicht vorab an. Der Kunde entscheidet eigenverantwortlich darüber, ob er trotz dieser Rahmenbedingungen und der Nutzungsbestimmungen von Microsoft eine Abfrage über cloro veranlasst. Die Klarplan AG kann die Abfrage über Microsoft Copilot jederzeit einstellen.

   5.5 Microsoft Copilot gilt als eingeschränkter KI-Assistent nach Ziffer 6. RankScan weist bei der Auswahl auf die Eigenschaften nach den Ziffern 5.2 bis 5.4 hin.

   5.6 Der Kunde kann die Auswahl von Microsoft Copilot für jede Website jederzeit mit Wirkung für die Zukunft deaktivieren. Danach werden keine weiteren Prompts dieser Website an Microsoft Copilot übermittelt.

6. **Eingeschränkte KI-Assistenten.**

   6.1 Die Klarplan AG bezeichnet einen KI-Assistenten in Anhang IV als «eingeschränkt», wenn sein Anbieter oder der Empfänger der Prompts in einem Staat ohne angemessenen Datenschutz sitzt und für die Bekanntgabe aus der Schweiz oder für die Übermittlung aus der EU keine anerkannte Garantie besteht; es genügt, dass eine der beiden fehlt. Eingeschränkt ist auch ein KI-Assistent, dessen Empfänger die Prompts als eigenständiger Verantwortlicher erhält.

   6.2 Der Kunde gibt in Prompts für eingeschränkte KI-Assistenten keine Personendaten ein. Diese Pflicht ist eine vertragliche Regel, keine technische Sperre.

   6.3 RankScan kennzeichnet eingeschränkte KI-Assistenten bei der Auswahl je Website und bei der Eingabe von Prompts und weist auf die Pflicht nach Ziffer 6.2 hin.

   6.4 Eingeschränkte KI-Assistenten erhalten Prompts nur, wenn der Kunde sie selbst auswählt. Sie gehören nicht zur Standardauswahl.

   6.5 Änderungen der Bezeichnung kündigt die Klarplan AG nach A.8 Ziff. 6 an.

A.5 Weisungen (zu Klausel 7.1)

Als dokumentierte Weisung im Sinne von Klausel 7.1 gelten:

1. die AGB und dieser Vertrag,
2. die Einstellungen und Aktionen des Kunden in RankScan, in der Reporting-API und im MCP-Server. Beispiele: überwachte Websites, Keywords, Prompts, Wettbewerber, die Auswahl der KI-Assistenten je Website, die Verbindung der Search Console und von Google Analytics 4, Teammitglieder, Empfänger von Benachrichtigungen und geteilten Reports, delegierte Massnahmen und die Löschung von Daten,
3. weitere Weisungen des Inhabers oder eines Admins in Textform an hello@rankscan.ai. Die Klarplan AG bewahrt diese Weisungen auf.

A.6 Schweizer Datenschutzrecht

Soweit die Verarbeitung dem Bundesgesetz über den Datenschutz (DSG) untersteht, gilt zusätzlich:

1. Verweise in Teil B auf die Verordnung (EU) 2016/679 gelten auch als Verweise auf die entsprechenden Bestimmungen des DSG, insbesondere Art. 9 DSG (Bearbeitung durch Auftragsbearbeiter).
2. «Aufsichtsbehörde» umfasst den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).
3. «Recht eines Mitgliedstaats» umfasst Schweizer Recht.
4. «Drittland» meint für Bekanntgaben aus der Schweiz einen Staat ohne angemessenen Schutz nach Art. 16 DSG. Verweise auf Kapitel V der Verordnung (EU) 2016/679 gelten für solche Bekanntgaben als Verweise auf Art. 16 und 17 DSG.
5. Die allgemeine Genehmigung nach Klausel 7.7 Buchstabe a ist die vorgängige Genehmigung nach Art. 9 Abs. 3 DSG.
6. Meldungen nach Klausel 9 erfolgen so, dass der Kunde seine Pflicht nach Art. 24 DSG erfüllen kann.

A.7 Nachweise und Prüfungen (zu Klausel 7.6)

1. Die Klarplan AG weist die Einhaltung in erster Linie durch Unterlagen nach: diesen Vertrag, Anhang III, die Liste der Unterauftragsverarbeiter und auf Anfrage weitere Auskünfte.
2. Der Kunde kann eine Prüfung nach Klausel 7.6 Buchstaben c und d in angemessenen Abständen durchführen oder durchführen lassen, in der Regel höchstens einmal je Kalenderjahr. Bei Anzeichen für eine Nichteinhaltung ist eine Prüfung jederzeit möglich.
3. Der Kunde kündigt eine Prüfung mindestens 30 Tage vorher in Textform an. Bei Anzeichen für eine Nichteinhaltung gilt eine angemessene kürzere Frist.
4. Ein beauftragter Prüfer ist zur Vertraulichkeit verpflichtet und kein Wettbewerber der Klarplan AG.
5. Jede Partei trägt ihre eigenen Kosten der Prüfung.

A.8 Unterauftragsverarbeiter (zu Klausel 7.7)

1. Die vereinbarte Liste nach Klausel 7.7 Buchstabe a ist Anhang IV in der Fassung, die unter https://rankscan.ai/de/subprocessors veröffentlicht ist.
2. Die Klarplan AG informiert mindestens 30 Tage vor dem Hinzufügen oder Ersetzen eines Unterauftragsverarbeiters per E-Mail an den Inhaber und die Admins. Die Mitteilung nennt Name, Anschrift, Tätigkeit, Daten, Ort der Verarbeitung und Grundlage der Übermittlung. Gleichzeitig kündigt die Klarplan AG die Änderung auf der Seite nach Ziffer 1 mit dem Datum an, ab dem sie gilt. Erst ab diesem Datum gehört der neue Unterauftragsverarbeiter zur vereinbarten Liste.
3. Der Kunde kann innerhalb dieser Frist in Textform begründet Einwand erheben. Die Parteien suchen dann eine Lösung, zum Beispiel den Verzicht auf die betroffene Funktion für dieses Kundenkonto. Bis zur Lösung gibt die Klarplan AG dem neuen Unterauftragsverarbeiter keine Kundendaten dieses Kundenkontos, soweit sich der Dienst je Kundenkonto trennen lässt. Das ist bei Diensten der Fall, die RankScan je Kundenkonto oder je Website wählt, zum Beispiel bei den KI-Assistenten der KI-Sichtbarkeit. Bei gemeinsamer Infrastruktur wie Datenbank, Server oder E-Mail-Versand ist es nicht der Fall.
4. Finden die Parteien keine Lösung oder lässt sich der Dienst nicht je Kundenkonto trennen, kann der Kunde den Nutzungsvertrag auf den Zeitpunkt der Änderung kündigen. Die Klarplan AG erstattet im Voraus bezahlte Entgelte für die Zeit danach anteilig. Der Ausschluss der Erstattung in den AGB gilt dafür nicht.
5. Die KI-Assistenten der KI-Sichtbarkeit wählt der Kunde je Website. Ohne eigene Wahl gilt eine Standardauswahl nach Anhang IV. Wählt der Kunde einen Anbieter ab, gehen keine neuen Prompts dieser Website an ihn. Eingeschränkte KI-Assistenten (A.4 Ziff. 6) gehören nicht zur Standardauswahl.
6. Andere Änderungen von Anhang IV, zum Beispiel neue Datenkategorien bei einem Anbieter oder eine geänderte Standardauswahl, kündigt die Klarplan AG nach A.2 Ziffer 6 an.
7. Die Verträge der Unterauftragsverarbeiter nennt Anhang IV.

A.9 Ende des Tarifs, Ruhephase, Rückgabe und Löschung (zu Klausel 10 Buchstabe d)

1. **Ende des Tarifs.** Ein Abo endet nach den AGB, zum Beispiel durch Kündigung zum Ende der Abrechnungsperiode. Eine Testphase endet mit ihrem Ablauf. Ein einzeln vereinbarter Tarif endet nach der Vereinbarung. Das Kundenkonto und der Nutzungsvertrag bestehen danach in der Ruhephase weiter.

2. **Ruhephase.** Grundlage der Ruhephase ist dieser Vertrag als Weisung des Kunden. Der Kunde kann sie jederzeit nach Ziffer 3 beenden.

   2.1 **Beginn:** der Tag, an dem der letzte Tarif endet.

   2.2 **Ende:** ein neuer Tarif beendet die Ruhephase. Ein Login beendet sie nicht. Sonst löscht die Klarplan AG das Kundenkonto 12 Monate nach Beginn der Ruhephase, ein Testkonto 3 Monate nach Beginn.

   2.3 **Erinnerung:** 30 Tage vor der Löschung erhält der Inhaber eine E-Mail mit dem Löschdatum und dem Hinweis auf Export und Löschung nach Ziffer 3 und 4. Ohne Inhaber geht sie an die Admins, ohne Admins an alle Teammitglieder. Die Löschung erfolgt frühestens 30 Tage nach der Erinnerung. Geht die Erinnerung später hinaus, verschiebt sich die Löschung entsprechend.

   2.4 **Zulässige Verarbeitung:** Speicherung; Löschung nach den Fristen in Anhang II; die Erinnerung; Export, Löschung und Wiederaufnahme auf Weisung; Support.

   2.5 **Nicht mehr verarbeitet:** Die Klarplan AG startet keine Scans, ruft die Search Console, Google Analytics 4 und den Chrome UX Report nicht ab und sendet keine Anfragen an Sprachmodelle oder Suchdienste. Aufträge, die vor dem Ende des Tarifs begonnen haben, laufen zu Ende. Bereits ausgelöste Benachrichtigungen können noch versandt werden.

   2.6 **Zugang:** Ohne Tarif hat der Kunde keinen Zugang zu den Daten in der Anwendung und über die Reporting-API. Der Inhaber sieht nur die Tarifwahl oder eine Sperrseite. Die Rückgabe erfolgt deshalb über den Export nach A.10 Ziffer 2.

3. **Frühere Löschung auf Weisung.** Der Kunde kann die Löschung jederzeit verlangen.

   3.1 Mit Tarif löscht der Inhaber das Kundenkonto selbst in den Einstellungen, mit seinem Passwort.

   3.2 Ohne Tarif oder ohne Inhaber schreibt der Inhaber oder ein Admin (A.1 Ziffer 3) von der im Kundenkonto hinterlegten E-Mail-Adresse an hello@rankscan.ai. Die Klarplan AG löscht das Kundenkonto innerhalb von 10 Arbeitstagen nach der Anfrage.

   3.3 Einzelne Websites löscht ein Admin selbst (A.10 Ziffer 4).

4. **Rückgabe und Wahl nach Klausel 10 Buchstabe d.** Bis zur Löschung kann der Kunde den Export nach A.10 Ziffer 2 verlangen, auch nach dem Ende des Tarifs und in der Ruhephase. Er wählt Rückgabe mit anschliessender Löschung oder nur Löschung. Trifft er bis zum Ende der Ruhephase keine Wahl, löscht die Klarplan AG die Daten. Nach der Löschung ist keine Rückgabe mehr möglich.

5. **Ablauf der Löschung.** Die Löschung sperrt das Kundenkonto sofort und entfernt alle Teammitglieder. Danach löscht ein Hintergrundauftrag alle Kundendaten nach Anhang III («Löschung»). Mit dem Kundenkonto löscht die Klarplan AG die Benutzerkonten, die zu keinem weiteren Kundenkonto gehören, samt Profilbild.

6. **Bestätigung.** Nach Abschluss der Löschung erhält der Inhaber automatisch eine Bestätigung per E-Mail. Ohne Inhaber gilt:

   6.1 Löscht die Klarplan AG auf Anfrage eines Admins (Ziffer 3.2), bestätigt sie ihm die Löschung nach Abschluss in Textform.

   6.2 Löscht sie nach Ablauf der Ruhephase, bestätigt sie die Löschung automatisch per E-Mail: an die Admins, ohne Admins an alle bisherigen Teammitglieder (Ziffer 2.3).

7. **Verbleibende Daten.** Nach der Löschung bestehen nur noch:

   7.1 Kopien in Datensicherungen bis zu deren Ablauf, spätestens 35 Tage nach der Löschung (Anhang III). Für Sicherungskopien der Testumgebung gilt abweichend Ziffer 7.3. Die Klarplan AG verwendet die Sicherungen nur für die Wiederherstellung des Gesamtsystems. Spielt sie eine Sicherung zurück, löscht sie die betroffenen Daten erneut, bevor sie diese wieder für den Betrieb oder für Tests verwendet.

   7.2 Einträge in Protokollen und technischen Warteschlangen: Anwendungsprotokolle bis 14 Tage, fehlgeschlagene Hintergrundaufträge in der Warteschlange bis 7 Tage, das Audit-Protokoll bis 365 Tage. Die Klarplan AG verwendet sie nur für Sicherheit, Nachweis und Fehlerbehebung.

   7.3 die Kopie auf der Testumgebung bis zu deren nächster Aktualisierung. Die Klarplan AG baut die Testumgebung mindestens alle 30 Tage neu auf, nach einer Löschung auf Anfrage spätestens innerhalb von 10 Arbeitstagen. Ab der Löschung des Kundenkontos führt sie für dessen Daten auf der Testumgebung keine Tests oder Anbieterabrufe mehr durch. Nach Entfernung aus der Testumgebung bestehen Kopien in automatischen Tagessicherungen höchstens 7 Tage, in manuellen Snapshots höchstens 30 Tage länger (Anhang III). Damit bestehen diese Sicherungskopien insgesamt höchstens 60 Tage nach der Löschung des Kundenkontos. Für ihre Verwendung und eine Wiederherstellung gilt Ziffer 7.1.

   7.4 die Freigabe des Zugriffs auf die Search Console und auf Google Analytics 4 im Google-Konto des Kunden. Die Löschung entfernt die Zugangsdaten in RankScan, widerruft die Freigabe bei Google aber nicht. Der Kunde kann sie im Google-Konto widerrufen. Trennt der Kunde die Search Console oder Google Analytics 4 vor der Löschung, widerruft RankScan die Freigabe selbst, sofern im Kundenkonto kein anderer Google-Zugang besteht.

8. Daten, für die die Klarplan AG selbst verantwortlich ist (Anhang II, Abschnitt 1), regelt die Datenschutzerklärung.

A.10 Export, einzelne Daten und Betroffenenanfragen (zu Klausel 8)

1. **Reporting-API.** Solange ein Tarif besteht, legt ein Admin ein Token des Kundenkontos an. Über die Reporting-API ruft der Kunde Auswertungen ab, zum Beispiel Scores, Rankings und KI-Sichtbarkeit. Sie liefert nicht alle Kundendaten.

2. **Vollständiger Export.** Auf Verlangen des Inhabers erstellt die Klarplan AG einen Export des Kundenkontos innerhalb von 10 Arbeitstagen. Der Export ist kostenlos, auch in der Ruhephase. Der Export ist eine ZIP-Datei mit einer JSONL-Datei je Tabelle, einer Übersicht (Manifest), den Profilbildern der Teammitglieder und den Screenshots der Support-Anfragen. Er enthält auch die interne Vorsortierung der Support-Anfragen (Kategorie, Dringlichkeit, Zusammenfassung, Antwortentwurf). Nicht enthalten sind:

   2.1 Zugangsdaten und Tokens, weil sie das Konto öffnen würden,

   2.2 Abrechnungsdaten und Kostenzähler, weil die Klarplan AG dafür selbst verantwortlich ist,

   2.3 die Nutzungsanalyse, weil die Klarplan AG dafür selbst verantwortlich ist (Datenschutzerklärung),

4. Arbeitsdaten laufender Crawls, weil sie nur bis zum Ende eines Laufs bestehen.

3. **Übergabe.** Die Klarplan AG sendet einen signierten Download-Link an die im Kundenkonto hinterlegte E-Mail-Adresse des Inhabers. Der Link gilt 7 Tage und braucht kein Login. Wer den Link besitzt, kann die Datei laden. Der Kunde hält ihn deshalb vertraulich. Die Klarplan AG löscht die Datei spätestens am Tag nach Ablauf des Links. Die Löschung des Kundenkontos löscht auch den Export.

4. **Berichtigung und Löschung durch den Kunden.** Solange ein Tarif besteht, ändert oder löscht der Kunde selbst:

   4.1 Teammitglieder, Einladungen und Empfänger von Benachrichtigungen (Admin),

   4.2 Websites und alle Scans einer Dimension (Admin),

   4.3 Topics, Keywords, Prompts, Wettbewerber und Kontakte für delegierte Massnahmen (alle Teammitglieder).

Mit einer Website, einem Keyword, einem Prompt oder einem Wettbewerber löscht RankScan die zugehörigen Ergebnisse. Sein eigenes Profil ändert und löscht jeder Nutzer selbst, auch ohne Tarif. Der Inhaber muss dafür zuerst das Kundenkonto übertragen oder löschen; ohne Tarif nach A.9 Ziffer 3.

5. **Inhalte ohne Einzellöschung; Support-Anfragen.**

   5.1 Einzelne gecrawlte Seiten, Suchergebnisse und KI-Antworten kann weder der Kunde noch die Klarplan AG mit einem vorgesehenen Verfahren einzeln löschen oder berichtigen. RankScan speichert sie so, wie die Quelle sie geliefert hat. Die Klarplan AG durchsucht diese Inhalte nicht gezielt nach einzelnen Personen.

   5.2 Diese Inhalte entfallen nach den Fristen in Anhang II oder mit der Löschung des Prompts, des Keywords, der Website oder des Kundenkontos. Diese Löschung nimmt der Kunde nach Ziffer 4 selbst vor. Ohne Tarif löscht die Klarplan AG auf Weisung nach A.9 Ziffer 3.

   5.3 Eine einzelne Support-Anfrage löscht ein Superadmin auf Weisung des Kunden innerhalb von 10 Arbeitstagen nach Eingang der Weisung. Die Weisung erteilt der Inhaber oder ein Admin in Textform an hello@rankscan.ai (A.5 Ziffer 3). Die Löschung umfasst Text, Verlauf, Screenshots und die interne Vorsortierung der Anfrage. Der Superadmin gibt dabei einen Grund an, den das Audit-Protokoll festhält. Kopien in Datensicherungen bestehen bis zu deren Rotation weiter, spätestens 35 Tage nach der Löschung (Anhang III). Die Klarplan AG verwendet sie nur für die Wiederherstellung des Gesamtsystems.

6. **Anfragen betroffener Personen.** Erhält die Klarplan AG eine Anfrage zu Kundendaten, leitet sie sie unverzüglich an den Inhaber weiter, spätestens innerhalb von 5 Arbeitstagen. Die Höchstfrist erlaubt keine Verzögerung, wenn eine frühere Weiterleitung möglich ist. Die Klarplan AG beantwortet die Anfrage nicht selbst, ausser der Kunde ermächtigt sie dazu. Anfragen zu Daten, für die die Klarplan AG selbst verantwortlich ist, beantwortet sie selbst.

A.11 Haftung

1. Die Haftung richtet sich nach den AGB, soweit zwingendes Recht und Teil B nicht entgegenstehen.

2. Der Ausschluss der Haftung für Drittanbieter in den AGB gilt nicht für die Unterauftragsverarbeiter nach Anhang IV. Für sie haftet die Klarplan AG nach Klausel 7.7 Buchstabe d.

3. Die Rechte betroffener Personen, insbesondere nach Art. 82 DSGVO, bleiben unberührt.

A.12 Anwendbares Recht, Gerichtsstand und Sprache

1. Für Teil A gilt Schweizer Recht. Gerichtsstand ist Luzern. Zwingende Gerichtsstände und die Rechte betroffener Personen und Aufsichtsbehörden nach DSGVO und DSG bleiben vorbehalten.
2. Dieser Vertrag liegt auf Deutsch und Englisch vor. Bei Abweichungen gilt die deutsche Fassung.

TEIL B

Standardvertragsklauseln

Durchführungsbeschluss (EU) 2021/915 der Kommission. Der Wortlaut ist unverändert übernommen.

Abschnitt I

Klausel 1: Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2: Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran, die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3: Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4: Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 – fakultativ: Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

Abschnitt II – Pflichten der Parteien

Klausel 6: Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7: Pflichten der Parteien

7.1. Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzliche Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 30 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8: Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9: Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

Abschnitt III – Schlussbestimmungen

Klausel 10: Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener

Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I

Liste der Parteien

Zu Klausel 1 Buchstabe b und Klausel 5.

Angabe	Verantwortlicher	Auftragsverarbeiter
Name	der Kunde, wie im Kundenkonto von RankScan angegeben	Klarplan AG (RankScan)
Anschrift	wie im Kundenkonto oder in der Rechnungsadresse angegeben	Sälihalde 11, 6005 Luzern, Schweiz
Kontaktperson	Inhaber des Kundenkontos (E-Mail-Adresse des Inhabers)	René Häfliger, Verwaltungsrat und Geschäftsführer, hello@rankscan.ai
Datenschutzberater / -beauftragter	–	keiner bestellt; Anfragen an hello@rankscan.ai
Vertreter in der EU nach Art. 27 DSGVO	–	keiner bestellt
Unterschrift und Beitrittsdatum	Annahme der AGB bei der Registrierung; bei Bestandskunden der Beginn nach A.2 Ziffer 8.2; bei unterzeichneter Fassung Unterschrift und Datum	Veröffentlichung dieses Vertrags; bei unterzeichneter Fassung Unterschrift und Datum

Handelt der Kunde nach A.4 Ziffer 4 im Auftrag eines Endkunden, ist er Auftragsverarbeiter des Endkunden. Die Rechte des Verantwortlichen nach diesen Klauseln übt er nach A.4 Ziffer 4.1 aus.

ANHANG II

Beschreibung der Verarbeitung

Zu Klausel 6.

1. Abgrenzung nach Vorgang

Vorgang	Rolle der Klarplan AG	Geregelt in
Inhalte und Auswertungen: Crawl der Websites des Kunden, Daten der Search Console und von Google Analytics 4, Suchergebnisse, KI-Sichtbarkeit, Wettbewerber, Massnahmen, Zusammenfassungen, Berichte, Wochenbericht, geteilte Reports, delegierte Massnahmen, Benachrichtigungen	Auftragsverarbeiter	dieser Vertrag
Teamverwaltung durch den Kunden: wer Zugang hat, Rollen, Einladungen, Empfänger von Benachrichtigungen und Reports, Kontakte für delegierte Massnahmen	Auftragsverarbeiter	dieser Vertrag
Benutzerkonto und Anmeldung: Registrierung, Login, Passwort, Schutz vor Missbrauch	Verantwortlicher	Datenschutzerklärung
Anwendungs- und Audit-Protokolle (Sicherheit, Nachweis)	Verantwortlicher	Datenschutzerklärung
Support: Inhalt der Anfrage und Screenshots, soweit sie Kundendaten enthalten	Auftragsverarbeiter	dieser Vertrag
Support: Austausch mit dem Kunden als Vertragspartner (Absender, Verlauf)	Verantwortlicher	Datenschutzerklärung
Abrechnung, Zahlungen, Provisionen an Vermittler	Verantwortlicher	Datenschutzerklärung
Nutzungsanalyse der Anwendung	Verantwortlicher	Datenschutzerklärung
Eigene E-Mails, Conversion-Messung, Website rankscan.ai	Verantwortlicher	Datenschutzerklärung

2. Kategorien betroffener Personen

- Teammitglieder des Kunden und eingeladene Personen
- Empfänger von Benachrichtigungen und geteilten Reports
- externe Kontakte, an die der Kunde Massnahmen delegiert, zum Beispiel Mitarbeitende einer Webagentur
- Personen, die in Support-Anfragen des Kunden genannt sind
- Personen, deren Name oder Kontaktdaten auf öffentlichen Websites stehen, die RankScan im Auftrag des Kunden verarbeitet: Websites des Kunden, seiner Wettbewerber und Seiten, die KI-Antworten zitieren (zum Beispiel Ansprechpersonen, Autoren, Inhaber von Einzelfirmen)
- Personen, die in Suchergebnissen, Antworten von KI-Assistenten oder Suchanfragen der Search Console genannt sind

- Personen, deren Namen der Kunde in Prompts, Wettbewerbern oder Notizen einträgt

3. Kategorien personenbezogener Daten

- Name, E-Mail-Adresse und Rolle von Teammitgliedern, eingeladenen Personen, Empfängern und externen Kontakten
- Inhalte öffentlicher Webseiten: Text, Überschriften, Titel, Links, Metadaten, Bild-URLs
- Daten der Google Search Console des Kunden: Seiten, Klicks, Impressionen, Klickrate, Position, die häufigsten Suchanfragen je Seite und Ergebnisse der URL-Prüfung. Die Werte sind aggregiert und enthalten keine Daten einzelner Besucher. Suchanfragen können Namen gesuchter Personen enthalten.
- Daten aus Google Analytics 4 des Kunden: Besuche, Seitenaufrufe, Verweildauer und Anzahl gewählter Ereignisse je Einstiegsseite, Tag und Quelle. Die Werte sind aggregiert und enthalten keine Daten einzelner Besucher.
- Prompts, Keywords, Wettbewerber, Positionierung und Antworten aus dem Strategie-Dialog, Notizen
- Suchergebnisse und Antworttexte von KI-Assistenten zu den Prompts des Kunden, mit den darin genannten Namen
- Freitext zu Massnahmen und Kommentare externer Kontakte
- Betreff, Text, Seiten-URL und Screenshots von Support-Anfragen

4. Sensible Daten (zu Klausel 7.5)

1. **Vorgesehen:** keine. RankScan ist nicht für die Verarbeitung sensibler Daten bestimmt.
2. **Wo sie zufällig anfallen können:** in Inhalten öffentlicher Webseiten, in Suchergebnissen, Antworten von KI-Assistenten und Suchanfragen der Search Console, in Prompts, Keywords und Notizen und in Support-Anfragen.
3. **Grenze der Technik:** RankScan erkennt sensible Daten nicht und filtert sie nicht heraus. Was der Kunde oder eine Website liefert, verarbeitet RankScan im Rahmen von Anhang II, auch die Weitergabe an Unterauftragsverarbeiter nach Anhang IV.
4. **Beschränkungen und Garantien, die bestehen:**

- RankScan wertet Inhalte nicht nach Personen aus und bildet keine Profile von Personen.
- RankScan crawlt nur öffentlich erreichbare Seiten und beachtet robots.txt.
- Den in RankScan gespeicherten Text gecrawlter Seiten sendet RankScan an kein Sprachmodell. Ausnahme ist der Seitentitel: für Vorschläge zur Meta-Description, in der Prüfung der Massnahmen und im Content-Brief. Für den Strategie-Dialog und die Prüfung zitierter Seiten ruft RankScan Seitentext eigens ab und sendet ihn an die Anbieter nach Anhang IV.
- Screenshots von Support-Anfragen gehen an kein Sprachmodell. Freitext der Nutzer zu übersprungenen Massnahmen geht nicht an die Prüfung der Massnahmen.
- Rohdaten der Crawls reduziert RankScan nach 14 Tagen auf zusammengefasste Werte.
- Zugriff des Personals der Klarplan AG nach Anhang III, mit Audit-Protokoll.

5. **Pflichten des Kunden:** Der Kunde gibt keine sensiblen Daten in Prompts, Keywords, Notizen, den Strategie-Dialog oder Support-Anfragen ein. Er lässt keine Seiten überwachen, deren Zweck die Veröffentlichung sensibler Daten einzelner Personen ist. In Keywords gibt er keine Personendaten ein, ebenso nicht in Prompts für eingeschränkte KI-Assistenten (A.4 Ziff. 6). Diese Pflichten sind vertragliche Regeln, keine technische Sperre.

6. **Hinweise in RankScan:** RankScan weist bei der Eingabe von Prompts und Keywords, im Strategie-Dialog, bei Notizen und im Support-Formular auf die Pflicht nach Ziffer 5 hin. Bei eingeschränkten KI-Assistenten weist RankScan bei der Auswahl und bei der Eingabe von Prompts auf A.4 Ziff. 6 hin. Eine automatische Erkennung sensibler Daten gibt es nicht. Auch Personendaten in Prompts oder Keywords erkennt RankScan nicht automatisch.

5. Art der Verarbeitung

Erheben (Crawl öffentlicher Webseiten, Abruf der Search Console und von Google Analytics 4, Abfrage von Suchdiensten und KI-Assistenten), Speichern, Auswerten, Zusammenfassen und Prüfen mit Sprachmodellen, Anzeigen, Bereitstellen über Reporting-API und MCP-Server, Versand an Empfänger auf Weisung des Kunden, Löschen.

6. Zwecke

Die Klarplan AG verarbeitet Kundendaten nur für diese Zwecke:

1. Überwachung von technischem Zustand, Suchsichtbarkeit und KI-Sichtbarkeit der Websites des Kunden, auch im Vergleich zu seinen Wettbewerbern
2. Einrichtung im Strategie-Dialog und Vorschläge für Prompts, Wettbewerber und Meta-Descriptions
3. Ableitung von Massnahmen, Zusammenfassungen, Berichte, Wochenbericht, geteilte Reports, delegierte Massnahmen und Benachrichtigungen
4. Bearbeitung von Support-Anfragen des Kunden, einschliesslich der Vorsortierung durch ein Sprachmodell
5. Bereitstellung über die Reporting-API und den MCP-Server
6. Betrieb und Sicherheit: Datensicherung, Fehleranalyse und Test neuer Versionen auf der Testumgebung (Anhang III)
7. Qualitätssicherung der Massnahmen: Ein Sprachmodell prüft Stichproben von abgeleiteten Massnahmen auf Richtigkeit, um die Prüfregeln von RankScan zu verbessern. Soweit dies über das einzelne Kundenkonto hinaus wirkt, erfolgt die Auswertung ausschliesslich anhand zuvor anonymisierter Daten ohne Personen- oder Kundenbezug.

Zweckbindung. Die Klarplan AG verwendet Kundendaten nur für die Zwecke 1 bis 7 und, ausser für Zweck 7, nur für den jeweiligen Kunden. Sie verwendet sie nicht für eigene Werbung, verkauft sie nicht, trainiert damit keine eigenen KI-Modelle und gibt sie nur an Unterauftragsverarbeiter nach Anhang IV und an Empfänger auf Weisung des Kunden weiter. Die Befugnis der AGB zur Verwendung aggregierter, anonymisierter Daten erfasst Kundendaten nur, soweit sie vorher so anonymisiert sind, dass weder ein Bezug zu einer natürlichen Person noch ein Rückschluss auf den Kunden möglich ist. Ob ein Unterauftragsverarbeiter Daten zum Training nutzt, steht in Anhang IV.

7. Dauer der Verarbeitung

Für die Laufzeit dieses Vertrags (A.2 Ziffer 3). Innerhalb der Laufzeit gelten diese Aufbewahrungsfristen:

Daten	Frist
Ergebnisse von Search und KI-Sichtbarkeit	alle Läufe 90 Tage, danach ein Lauf je Monat bis 365 Tage

Daten	Frist
Website-Health-Läufe je Tarif (alle Läufe / ein Lauf je Monat)	Starter 30/180, Pro 60/365, Enterprise 90/730 Tage, ohne Tarif 14/30 Tage
Rohdaten der Crawls (Seiteninhalte)	14 Tage, danach nur zusammengefasste Werte
Fehlgeschlagene Crawl-Läufe	30 Tage
Arbeitsdaten eines Crawls (Link- und Warteschlangen)	bis zum Ende des Laufs, bei Abbruch höchstens zwei Stunden länger
Zusammengefasste Werte (Tageswerte, Scores, Verläufe je Topic)	25 Monate
Kennzahlen der Search Console je Seite	180 Tage
Suchanfragen der Search Console je Seite	bei jeder Aktualisierung ersetzt, ohne Verlauf
Alle Daten der Search Console einer Website	beim Trennen der Search Console sofort gelöscht
Tagessummen von Google Analytics 4 je Seite und Quelle	365 Tage
Alle Daten von Google Analytics 4 einer Website	beim Trennen von Google Analytics 4 sofort gelöscht
Gelöste Hinweise zum technischen Zustand	180 Tage
Prüfungen von Seiten, die KI-Antworten zitieren	30 Tage nach der letzten Prüfung
Geteilte Reports	30 Tage ab Erstellung
Links für delegierte Massnahmen	90 Tage gültig; Inhalte bis zur Löschung der Website oder des Kundenkontos
Verworfene und gescheiterte Strategie-Dialoge	30 Tage
Export des Kundenkontos	7 Tage, Löschung spätestens am Folgetag
Ergebnisse der Prüfung von Massnahmen	bis zur Löschung des Kundenkontos
Support-Anfragen und Screenshots	bis zur Löschung auf Weisung (A.10 Ziffer 5) oder zur Löschung des Kundenkontos
Teammitglieder, offene Einladungen, Kontakte, Empfänger	bis zur Entfernung durch den Kunden oder zur Löschung des Kundenkontos
Abgelaufene Einladungen ins Team	30 Tage nach Ablauf
Kundenkonto ohne Tarif (Ruhephase)	12 Monate, Testkonto 3 Monate; Löschung frühestens 30 Tage nach der Erinnerung (A.9 Ziffer 2)

8. Verarbeitung durch Unterauftragsverarbeiter

Gegenstand, Art und Dauer stehen je Unterauftragsverarbeiter in Anhang IV. Die Dauer ist höchstens die Laufzeit dieses Vertrags. Beim Unterauftragsverarbeiter gelten zusätzlich die Fristen in Anhang IV.

ANHANG III

Technische und organisatorische Massnahmen

Einschliesslich der Massnahmen zur Gewährleistung der Sicherheit der Daten (zu Klausel 7.4, 8 und 9).

Verschlüsselung und Pseudonymisierung

- **Transport:** Alle Verbindungen zur Anwendung laufen über HTTPS. Die TLS-Verbindung endet bei Cloudflare (Anhang IV Nr. 10) und läuft von dort neu verschlüsselt zum Server. Das Session-Cookie ist nur über HTTPS gültig und verschlüsselt.
- **Geheimnisse:** OAuth-Tokens der Search Console und von Google Analytics 4 sind in der Datenbank verschlüsselt gespeichert. API-Tokens speichert RankScan nur als Hash.
- **Speicherung:** Die Datenbank (Amazon-Lightsail-Datenbank) ist verschlüsselt. Lightsail verschlüsselt ruhende Daten automatisch. Der Anwendungsserver (Amazon Lightsail) speichert Protokolle, Profilbilder, Screenshots von Support-Anfragen, Exporte und die Datenbank der Testumgebung auf verschlüsselten Datenträgern (Storage Volumes mit AWS-verwalteter Verschlüsselung).
- Passwörter speichert RankScan nur als Hash.

Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit

- **Mandantentrennung:** Jede Tabelle mit Kundendaten trägt die Kennung des Kundenkontos. Ein Zugriff ohne gesetzten Mandanten bricht mit einem Fehler ab. Zusammengesetzte Fremdschlüssel verhindern Daten im falschen Kundenkonto.
- Jeder Hintergrundauftrag setzt den Mandanten ausdrücklich, bevor er Daten liest oder schreibt.
- Lastbegrenzung für Anmeldung, Registrierung, Passwort-Reset, Reporting-API und MCP-Server.

Wiederherstellung nach Zwischenfällen

- Datenbank als Amazon-Lightsail-Datenbank mit automatischen Sicherungen. Aufbewahrung 7 Tage, Point-in-Time-Recovery innerhalb dieser Frist. Zusätzlich sichert die Klarplan AG die Datenbank jede Nacht verschlüsselt in Amazon S3. Diese Sicherungen werden spätestens 35 Tage nach ihrer Erstellung gelöscht. Manuelle Snapshots werden spätestens 30 Tage nach ihrer Erstellung gelöscht. Die Sicherungen liegen in Frankfurt (eu-central-1). Kopien in andere Regionen gibt es keine.
- Der Anwendungsserver wird täglich automatisch gesichert (Lightsail-Snapshots). Es bleiben die sieben neuesten. Manuelle Snapshots werden spätestens 30 Tage nach ihrer Erstellung gelöscht.

Überprüfung der Wirksamkeit

- Jede Änderung am Code durchläuft automatische Tests und statische Analysen, bevor sie live geht.
- **Testumgebung:** Sie läuft auf dem Anwendungsserver mit einer eigenen Datenbank. Sie nutzt eine Kopie der Produktion. Nutzer-, Konto-, Kontakt- und Support-Daten sowie Freitext aus Einrichtung, Kommentaren und Notizen sind pseudonymisiert, Nutzungsdaten und Zugangsdaten gelöscht. Inhaltsdaten wie Seiteninhalte, Keywords, Prompts, Wettbewerber und KI-Antworten bleiben unverändert. Anmelden können sich nur Superadmins. Scans starten dort nur Superadmins von Hand, für Tests. Dabei ruft die Testumgebung die Anbieter nach Anhang IV auf. Die Kopie wird bei jeder Aktualisierung ersetzt, mindestens alle 30 Tage; nach einer Löschung auf Anfrage spätestens innerhalb von 10 Arbeitstagen. Die Einschränkungen nach A.9 Ziffer 7.3 gelten auch für Tests und Anbieterabrufe.

- Die Klarplan AG überprüft diese Massnahmen mindestens jährlich und nach wesentlichen Änderungen an Infrastruktur oder Anbietern.

Identifizierung und Autorisierung der Nutzer

- Anmeldung mit E-Mail und Passwort. Die Verbindung mit Google dient nur dem Zugriff auf die Search Console und auf Google Analytics 4. RankScan fordert für Google Analytics 4 nur lesenden Zugriff an.
- Rollen im Kundenkonto: Inhaber, Admin und Mitglied. Nur Admins lösen kostenpflichtige Scans aus, verwalten das Team und löschen Websites. Nur der Inhaber löscht das Kundenkonto.
- Zugriff auf Reporting-API und MCP-Server nur mit einem Token des Kundenkontos. Ein Admin legt es an und widerruft es. Ein Token aus der Anwendung darf nur lesen und gilt bis zum Widerruf. Er endet auch, wenn sein Ersteller das Kundenkonto verlässt oder nicht mehr Admin ist. Schreib- und Löschrechte für den MCP-Server vergibt nur die Klarplan AG.

Zugriff durch Personal der Klarplan AG

- Zugriff auf Kundendaten haben nur wenige Superadmins, und nur, soweit Betrieb und Support es erfordern.
- Wechselt ein Superadmin in ein Kundenkonto, hat er dort die Rechte eines Admins. Jeder Wechsel schreibt einen Eintrag ins Audit-Protokoll.
- Meldet sich ein Superadmin im Namen eines Nutzers an, sind diese Aktionen gesperrt: Profil ändern oder löschen, API-Tokens anlegen, Einladungen versenden, Support-Anfragen anlegen oder beantworten und das Kundenkonto löschen.
- Superadmin-Zugänge zu RankScan erfordern einen zweiten Faktor (TOTP). Kontowechsel, auch per Link, und Anmeldung im Namen eines Nutzers verlangen eine Prüfung, die höchstens 15 Minuten alt ist.
- Exporte erstellt nur ein Superadmin auf dem Server, mit Angabe eines Grundes im Audit-Protokoll.
- Administrative AWS-Zugänge erfordern MFA.
- Alle Personen mit Zugriff auf Kundendaten sind vertraglich zur Vertraulichkeit verpflichtet.

Schutz bei der Übermittlung

- HTTPS für Anwendung, Reporting-API, MCP-Server und alle Aufrufe an Unterauftragsverarbeiter.
- An Sprachmodelle und Suchdienste gehen nur die Daten, die für die jeweilige Aufgabe nötig sind. Für die Sprachmodelle nennt Anhang IV sie je Anbieter.
- Geteilte Reports und delegierte Massnahmen öffnet ein Link mit einem zufälligen Token. Er gilt 30 bzw. 90 Tage.

Schutz bei der Speicherung

- Datenbank und Anwendungsserver bei Amazon Web Services, Region Frankfurt (eu-central-1).
- Die Datenbank ist nicht öffentlich erreichbar. Zugriff hat nur der Anwendungsserver.

Physische Sicherheit

Die Rechenzentren betreibt Amazon Web Services. Es gelten deren Zertifizierungen (unter anderem ISO 27001, SOC 2). Die Klarplan AG betreibt keine eigenen Server.

Protokollierung

- Anwendungsprotokolle mit Fehlern und Laufzeiten.
- Audit-Protokoll für Zugriffe von Superadmins auf Kundenkonten, Exporte, Löschungen, Schreibzugriffe über den MCP-Server, abgelehnte Aktionen, Treffer der Lastbegrenzung und fehlgeschlagene Anmeldungen. Es enthält Kennungen, E-Mail-Adressen der Handelnden und IP-Adressen. Bei fehlgeschlagenen Anmeldungen steht statt der eingegebenen E-Mail-Adresse nur deren Domain mit einem gekürzten Hash darin, bei einem bestehenden Benutzerkonto dessen Kennung.
- Die Protokolle sind nicht nach Mandanten getrennt. Zugriff haben nur Superadmins.
- Aufbewahrung: Anwendungsprotokolle 14 Tage, Audit-Protokoll 365 Tage.

Systemkonfiguration

- Server-Zugang nur per SSH-Schlüssel, über Cloudflare Zero Trust mit MFA. Port 22 ist öffentlich geschlossen.
- Sicherheits-Header für alle Antworten der Anwendung.
- Deploys nur von geprüften Versionen (Tag-Gate).

Interne Governance und Zertifizierung

- Verantwortlich für Datenschutz und IT-Sicherheit: René Häfliger, Verwaltungsrat und Geschäftsführer.
- Sicherheitslücken in Abhängigkeiten werden laufend geprüft und behoben.
- Die Klarplan AG hat keine eigene Zertifizierung.

Datenminimierung und Datenqualität

- RankScan crawlt nur öffentliche Seiten und beachtet robots.txt.
- Zwischenergebnisse eines Crawls werden am Ende des Laufs gelöscht. Rohdaten der Seiten werden nach 14 Tagen auf zusammengefasste Werte reduziert.
- Die Search Console und Google Analytics 4 liefern nur aggregierte Werte, keine Daten einzelner Besucher. RankScan speichert aus Google Analytics 4 nur Summen je Seite, Tag und Quelle.
- Ohne Tarif startet RankScan keine neuen Abrufe externer Dienste für das Kundenkonto (A.9 Ziffer 2).
- Solange ein Tarif besteht, kann der Kunde überwachte Websites, Keywords, Prompts, Wettbewerber und Teammitglieder selbst ändern (A.10 Ziffer 4).

Begrenzte Speicherung, Rechenschaft und Datenübertragbarkeit

- Automatische Löschung nach den Fristen in Anhang II, Abschnitt 7.
- Dieser Vertrag, die Liste der Unterauftragsverarbeiter und das Audit-Protokoll dienen als Nachweis.
- Export über die Reporting-API und vollständiger Export des Kundenkontos (A.10 Ziffer 1 bis 3).
- **Löschung:** Die Löschung eines Kundenkontos sperrt das Konto sofort und entfernt alle Teammitglieder. Danach löscht ein Hintergrundauftrag alle Websites, Scan-Ergebnisse, Daten und Zugangsdaten der Search Console und von Google Analytics 4, Support-Anfragen und Screenshots, Exporte, Nutzungsdaten und das Kundenkonto selbst. Benutzerkonten ohne weiteres Kundenkonto löscht er samt Profilbild. Scheitert der Auftrag, wiederholt RankScan ihn, und die Superadmins erhalten eine Meldung.
- **Trennen von Google Analytics 4:** Trennt der Kunde Google Analytics 4 bei einer Website, löscht RankScan sofort alle Daten von Google Analytics 4 dieser Website und danach die Zugangsdaten. Da-

nach widerruft RankScan die Freigabe bei Google, ausser im Kundenkonto besteht ein anderer Google-Zugang (Search Console oder Google Analytics 4). Die Daten sind in jedem Fall gelöscht.

- Verbleibende Daten: A.9 Ziffer 7.

Unterstützung des Verantwortlichen (Klausel 8 und 9)

- Anfragen betroffener Personen: A.10 Ziffer 6.
- Berichtigung und Löschung durch den Kunden: A.10 Ziffer 4 und 5.
- Löschung einzelner Support-Anfragen auf Weisung: A.10 Ziffer 5.
- Meldung von Verletzungen nach Klausel 9.2: unverzüglich, spätestens 48 Stunden nachdem der Klarplan AG die Verletzung bekannt wurde, per E-Mail an den Inhaber und die Admins des Kundenkontos. Die Höchstfrist erlaubt keine Verzögerung, wenn eine frühere Meldung möglich ist.
- Anlaufstelle für Datenschutzverletzungen: hello@rankscan.ai.

Massnahmen der Unterauftragsverarbeiter

Die Klarplan AG verlangt von jedem Unterauftragsverarbeiter mindestens diese Massnahmen: Verarbeitung nur zur Erbringung des Dienstes und auf Weisung; kein Training von KI-Modellen mit Kundendaten (ausser Anhang IV nennt etwas anderes); Verschlüsselung bei der Übertragung; Zugriff nur für befugtes, zur Vertraulichkeit verpflichtetes Personal; Löschung nach den Fristen in Anhang IV und am Vertragsende; Meldung von Verletzungen des Schutzes personenbezogener Daten; Unterstützung bei Anfragen betroffener Personen.

Die Verträge der Nummern 7 (cloro), 8 (Google Workspace), 9 (DataForSEO) und 10 (Cloudflare) in Anhang IV enthalten diese Punkte mit zwei Einschränkungen. Ein ausdrückliches Verbot des Trainings nennen sie nicht; sie beschränken die Verarbeitung auf die Erbringung des Dienstes. cloro schliesst Training nach eigener Angabe aus; vertraglich zugesichert ist das nicht. Der Vertrag von cloro sagt keine Verschlüsselung bei der Übertragung zu; die Klarplan AG ruft cloro nur über HTTPS auf.

ANHANG IV

Liste der Unterauftragsverarbeiter

Vereinbarte Liste nach Klausel 7.7 Buchstabe a (Option 2). Stand: 02.11.2026. Die geltende Fassung steht unter https://rankscan.ai/de/subprocessors.

Die Dauer der Verarbeitung ist höchstens die Laufzeit dieses Vertrags. «nicht angegeben» heisst: Der Vertrag des Anbieters macht dazu keine Angabe. «Aufbewahrung beim Anbieter» nennt die Fristen beim Anbieter; die Fristen der Klarplan AG stehen in Anhang II. «Eingeschränkt» bezeichnet einen eingeschränkten KI-Assistenten nach A.4 Ziff. 6 oder den Dienst, über den ein solcher abgefragt wird.

01 **Amazon Web Services EMEA SARL**
38 avenue John F. Kennedy, L-1855 Luxemburg

Tätigkeit	Datenbank, Anwendungsserver und Testumgebung (Lightsail), Sicherungen (S3), E-Mail-Versand (SES, Frankfurt)
Kundendaten	alle Kundendaten
Ort der Verarbeitung	EU, Frankfurt (eu-central-1)
Aufbewahrung beim Anbieter	nach den Fristen der Klarplan AG
Training mit Kundendaten	nein
Grundlage der Übermittlung	Verarbeitung in der EU; AWS Data Processing Addendum mit SCC 2021/914 und Swiss Addendum

02 **OpenAI Ireland Ltd.** NICHT EINGESCHRÄNKT

1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, Irland

Tätigkeit	Strategie-Dialog, Vorschläge, Content-Briefs, Mailentwürfe an zitierte Quellen, Zusammenfassungen, Vorsortierung von Support-Anfragen, KI-Sichtbarkeit
Kundendaten	Prompts; Topics, Keywords, Region; Positionierung, Markenbegriffe, Wettbewerbernamen; Text von bis zu 6 Seiten der Website des Kunden (je bis 3000 Zeichen) mit Seitentitel und Überschriften (bis 1000 Zeichen); Seitentitel für Vorschläge zur Meta-Description; für Content-Briefs Ausschnitte aus Antworten der KI-Assistenten (je bis 800 Zeichen) und deren Suchanfragen, URLs und Titel zitierter Seiten, Pfad und Seitentitel der gewählten Seite (bis 120 Zeichen); für Mailentwürfe Name, Adresse und Sprache der Website, URL und Art der zitierten Quelle sowie, ob die Quelle Plätze gegen Bezahlung vergibt, mit dem erkannten Wort aus einer festen Liste (zum Beispiel «Anzeige»), ohne Text der Quelle; in Zusammenfassungen die Inhalte der Massnahmen: Keywords mit Positionen, Prompts, Wettbewerber, URLs und Titel zitierter Seiten, Kennzahlen der Search Console je Seite (URL, Klicks, Impressionen, Klickrate, Position); Betreff und Text von Support-Anfragen mit Name und Domain der Website, Seiten-URL und Tarif, ohne Screenshots und ohne die Konto-Angaben des Absenders (Name, E-Mail). Angaben, die der Absender selbst in den Text schreibt, gehen mit.
Ort der Verarbeitung	USA und weitere Länder der Unterauftragsverarbeiter von OpenAI, ohne Datenresidenz in Europa
Aufbewahrung beim Anbieter	bis 30 Tage (Missbrauchsüberwachung)
Training mit Kundendaten	nein
Grundlage der Übermittlung	Vertragspartner für Kunden mit Sitz in der Schweiz ist OpenAI Ireland Ltd.; Irland bietet nach Anhang 1 DSV angemessenen Schutz. Daten nach dem Recht des EWR und der Schweiz verarbeitet OpenAI Ireland Limited. Weitergaben ausserhalb von EWR und Schweiz, etwa an OpenAI OpCo, LLC, stützt OpenAI auf SCC 2021/914 (DPA vom 1.1.2026, Ziff. 4.1). Eine Anpassung der SCC für die Schweiz nennt der DPA dafür nicht. OpenAI OpCo, LLC ist nicht unter dem Data Privacy Framework zertifiziert.

03 Google Cloud EMEA Limited NICHT EINGESCHRÄNKT

Velasco, Clanwilliam Place, Dublin 2, Irland

Tätigkeit	Gemini API (bezahlte Stufe): KI-Sichtbarkeit mit Google-Suche, Prüfung von Massnahmen, Prüfung eigener Nennungen
Kundendaten	Prompts; Auszüge aus KI-Antworten; Geschäftskontext (Marke, Domain, Topics, Keywords, Region); Name und Domain der Website; Text der Massnahme mit den häufigsten Suchanfragen, Impressionen, Klicks und Position je Seite aus der Search Console; Ergebnis der Messprüfung mit dem Seitentitel aus dem letzten Abruf (bis 120 Zeichen)
Ort der Verarbeitung	nicht angegeben
Aufbewahrung beim Anbieter	55 Tage (Missbrauchsüberwachung); mit Google-Suche 30 Tage, nicht abschaltbar
Training mit Kundendaten	nein
Grundlage der Übermittlung	Data Processing Addendum for Products Where Google is a Data Processor mit SCC 2021/914; der DPA erfasst auch Daten nach DSG. Google LLC ist unter dem EU-U.S. und dem Swiss-U.S. Data Privacy Framework zertifiziert.

04 Groq UK Limited NICHT ANWENDBAR

3 Hammersmith Grove, London W6 0ND, Vereinigtes Königreich

Tätigkeit	Auswertung von KI-Antworten: Marken, Relevanz, Eignung zitierter Seiten. Groq erhält keine Prompts der KI-Sichtbarkeit, sondern wertet Antworten aus.
Kundendaten	Antworttexte; Geschäftskontext (Marken- oder Website-Name, Domain, Topics, bis 60 Keywords, Region); Namen von Marken und Wettbewerbern; URL, Titel und bis 4000 Zeichen Text fremder Seiten, die eine KI-Antwort zitiert
Ort der Verarbeitung	USA (Google Cloud)
Aufbewahrung beim Anbieter	standardmässig keine; Protokolle bei Störung oder Missbrauch bis 30 Tage
Training mit Kundendaten	nein
Grundlage der Übermittlung	Groq Data Processing Addendum mit SCC 2021/914 (Module 2 und 3) und Anpassung für die Schweiz

05 Anthropic Ireland, Limited NICHT EINGESCHRÄNKT

6th Floor, South Bank House, Barrow Street, Dublin 4, Irland

Tätigkeit	KI-Sichtbarkeit, nur bei Auswahl durch den Kunden
Kundendaten	Prompts
Ort der Verarbeitung	weltweit nach Wahl des Anbieters
Aufbewahrung beim Anbieter	30 Tage; bei Verstoss gegen Nutzungsregeln bis 2 Jahre
Training mit Kundendaten	nein
Grundlage der Übermittlung	Anthropic Data Processing Addendum mit SCC 2021/914 (Module 2 und 3) und Swiss Addendum. Anthropic, PBC (USA) ist nicht unter dem Data Privacy Framework zertifiziert.

06 Perplexity AI, Inc. EINGESCHRÄNKT

115 Sansome Street, Suite 900, San Francisco, CA 94104, USA

Tätigkeit	KI-Sichtbarkeit, nur bei Auswahl durch den Kunden
Kundendaten	Prompts
Ort der Verarbeitung	USA. Perplexity und alle seine Unterauftragsverarbeiter sitzen in den USA.
Aufbewahrung beim Anbieter	Personendaten in Eingaben bis zur Löschung durch den Kunden, spätestens 30 Tage nach Ende der Leistung (DPA Annex 1). Für einzelne Dienste können eigene Regeln gelten.
Training mit Kundendaten	nein (DPA §5)
Grundlage der Übermittlung	Perplexity Data Processing Addendum (Stand 13.08.2026) mit SCC 2021/914 (Module 2 und 3) für Daten nach EU- und UK-Recht. Daten nach DSG erfasst der DPA nicht. Perplexity AI, Inc. ist nicht unter dem Data Privacy Framework zertifiziert. Die Klarplan AG hat eine Transferfolgenabschätzung erstellt und überprüft sie mindestens jährlich.

07 Cloro Incorporation Ltd. EINGESCHRÄNKT

168 Triq San Kristofru, Valletta VLT 1467, Malta

Tätigkeit	Abfrage von Microsoft Copilot, nur bei Auswahl durch den Kunden
Kundendaten	Prompts, Ländercode der Website
Ort der Verarbeitung	USA (Anwendung, Datenbank und Backups bei DigitalOcean) und Deutschland (Abfrage bei Hetzner). Die Anfrage an Copilot geht aus dem Land der Website. Weitere Unterauftragsverarbeiter von cloro mit Zweck und Ort: https://cloro.dev/our-commitment-to-security/ (Abschnitt «Subprocessors»).
Aufbewahrung beim Anbieter	Synchrone Anfragen und Ergebnisse nach der Antwort nicht gespeichert; asynchrone Aufträge und Ergebnisse etwa 24 Stunden; Telemetrie mit dem Text der Prompts 6 Monate; Anwendungsprotokolle 7 Tage; Datensicherungen 7 bis 14 Tage; Löschung auf Anfrage binnen 30 Tagen. Diese Fristen nennt cloro; vertraglich zugesichert sind sie nicht.
Training mit Kundendaten	nein nach Angabe von cloro, vertraglich nicht zugesichert; die Terms (§6.2) erlauben nur eine aggregierte, de-identifizierte Nutzung. Microsoft darf die Prompts zur Verbesserung von Copilot nutzen (A.4 Ziff. 5).
Grundlage der Übermittlung	Bekanntgabe an cloro (Malta): angemessener Schutz nach Art. 16 Abs. 1 DSG und Anhang 1 DSV; innerhalb der EU keine Übermittlung nach Kapitel V DSGVO. Weitergabe an DigitalOcean, LLC (USA): DigitalOcean ist unter dem EU-U.S. und dem Swiss-U.S. Data Privacy Framework zertifiziert. Zusätzlich gilt das cloro Data Protection Agreement mit SCC 2021/914 (Modul 2); Ziffer 6(a) stellt Übermittlungen aus der Schweiz unter die SCC; eine Anpassung an DSG und EDÖB enthält der DPA nicht. Für Better Stack (Logs; Deutschland und USA) und Snapshooter (Backups; USA) gilt der Vertrag zwischen cloro und dem Dienst. Die Klarplan AG kennt diesen Vertrag nicht. cloro haftet für beide nach DPA §5(c). Die Weitergabe an Microsoft Copilot erfolgt auf Weisung des Kunden (A.4 Ziff. 5; Klausel 8.8 des cloro Data Protection Agreement).

08 Google Cloud EMEA Limited: Google Workspace

Velasco, Clanwilliam Place, Dublin 2, Irland

Tätigkeit	Postfach hello@rankscan.ai: Support, Weisungen, interne Benachrichtigung zu Support-Anfragen
Kundendaten	Inhalt von E-Mails des Kunden; Auszüge aus Support-Anfragen
Ort der Verarbeitung	nicht angegeben
Aufbewahrung beim Anbieter	nach den Fristen der Klarplan AG
Training mit Kundendaten	nicht angegeben
Grundlage der Übermittlung	Google Cloud Data Processing Addendum, für das Konto rankscan.ai angenommen

09 DataForSEO OÜ

Vesivärava tn 50-201, 10152 Tallinn, Estland, Registernummer 14502291

Tätigkeit	Abruf von Suchergebnissen (SERP), Keyword-Kennzahlen und Suchsichtbarkeit
Kundendaten	Keywords, Domains, URLs, Sprach- und Ländereinstellungen (Personendaten nur, soweit Suchergebnisse sie enthalten)
Ort der Verarbeitung	EU (Estland, Deutschland bei Hetzner) und USA (Google Cloud, Microsoft Azure)
Aufbewahrung beim Anbieter	Auftragsdaten nach Abruf kurzzeitig zwischengespeichert; Protokolle nach den Fristen des Anbieters
Training mit Kundendaten	nein
Grundlage der Übermittlung	Bekanntgabe an DataForSEO OÜ (Estland): angemessener Schutz nach Art. 16 Abs. 1 DSG und Anhang 1 DSV; innerhalb der EU keine Übermittlung nach Kapitel V DSGVO. Weitergabe an Unterauftragsverarbeiter in den USA: DataForSEO Data Processing Agreement (Bestandteil der Privacy Policy) mit Standardvertragsklauseln (SCC).

10 Cloudflare, Inc.

101 Townsend Street, San Francisco, CA 94107, USA

Tätigkeit	Reverse-Proxy, DDoS-Schutz und Web Application Firewall für Anwendung, Reporting-API, MCP-Server und Testumgebung; Zugang zum Server (Zero Trust)
Kundendaten	alle Daten im Datenverkehr mit Anwendung, Reporting-API, MCP-Server und Testumgebung, auch IP-Adressen und Browserdaten der Nutzer. Die TLS-Verbindung endet bei Cloudflare (Anhang III).
Ort der Verarbeitung	weltweit, im Rechenzentrum von Cloudflare nächst beim Nutzer; auch ausserhalb von EWR und Schweiz (DPA Ziff. 6.1)
Aufbewahrung beim Anbieter	nicht angegeben; der DPA begrenzt die Verarbeitung auf die Laufzeit des Vertrags mit Cloudflare oder bis sie für den Dienst nicht mehr nötig ist (Annex 1)
Training mit Kundendaten	nicht angegeben; der DPA beschränkt die Verarbeitung auf die Erbringung des Dienstes (Ziff. 3.1 a)
Grundlage der Übermittlung	Cloudflare Data Processing Addendum (Version 6.4 vom 3.4.2026), Bestandteil des Self-Serve Subscription Agreement. Cloudflare, Inc. ist unter dem EU-U.S. und dem Swiss-U.S. Data Privacy Framework zertifiziert. Entfällt die Zertifizierung, gelten nach DPA Ziff. 6.2 die SCC 2021/914 (Module 2 und 3) mit Anpassung für die Schweiz.

Standardauswahl der KI-Assistenten. Ohne eigene Wahl des Kunden gehen die Prompts einer neuen Website an OpenAI und Gemini. Anthropic, Perplexity und cloro erhalten Prompts nur, wenn der Kunde sie auswählt. Eingeschränkte KI-Assistenten (A.4 Ziff. 6) gehören nie zur Standardauswahl.

Dienste ohne Auftragsverarbeitung

Diese Dienste setzt RankScan ein. Sie sind keine Unterauftragsverarbeiter.

Dienst	Einordnung	Begründung
Google LLC: Search Console API	eigenständig Verantwortlicher; Datenquelle des Kunden	Der Kunde verbindet seine Search Console. Google liefert Daten aus der eigenen Suche nach den Google APIs Terms mit Controller-Controller-Bedingungen. RankScan sendet nur die Zugangsdaten und Seiten-URLs.
Google LLC: Chrome UX Report API	Dienst ohne Personendaten	RankScan sendet nur Seiten-URLs und erhält aggregierte Ladezeiten.
Google LLC: Favicon-Dienst (S2)	Dienst ohne Personendaten im konkreten Einsatz	RankScan fragt den Dienst nur ab, wenn eine Website selbst kein Favicon liefert. Der Server sendet nur den Domainnamen, keine IP-Adresse oder Browserdaten der Nutzer.
Wikimedia Foundation, Inc.: Wikidata	Dienst ohne Personendaten im konkreten Einsatz	RankScan sendet nur die Domain der Website als Suchbegriff.
Serper (Serper.dev)	Dienst ohne Personendaten im konkreten Einsatz	RankScan sendet an Serper ausschliesslich sachbezogene Suchbegriffe (Keywords) sowie Länder- und Sprachcode, ohne Domain, Konto-, Nutzer- oder IP-Daten des Kunden, um öffentliche Google-Suchergebnisse abzurufen. Die Eingabe von Personendaten in Keywords ist nach Anhang II, Abschnitt 4 Ziff. 5 ausgeschlossen.
Websites Dritter	kein Empfänger	RankScan ruft öffentliche Seiten ab, auch Favicons von Wettbewerbern, und sendet dabei nur die Anfrage.
Google Tag Manager, Google Analytics 4, Google Ads, Pixel von OpenAI in der Anwendung	Verantwortungsbereich der Klarplan AG; nur mit Einwilligung	Messung von Registrierung und Abo nach der Datenschutzerklärung.
Stripe, Mautic (selbst betrieben)	Verantwortungsbereich der Klarplan AG	Abrechnung und eigene E-Mails.
Microsoft (Copilot)	Empfänger auf Weisung des Kunden (A.4 Ziff. 5); eigenständig Verantwortlicher ohne Vertrag mit der Klarplan AG	cloro stellt die Prompts an die Oberfläche für Verbraucher von Microsoft Copilot, nur bei Auswahl durch den Kunden. Microsoft verarbeitet sie nach eigenen Bedingungen und darf sie zur Verbesserung von Copilot nutzen.

Dienst	Einordnung	Begründung
Vom Kunden angebundene Dienste, zum Beispiel Looker Studio oder ein MCP-Client	Empfänger auf Weisung des Kunden	Der Kunde verbindet sie selbst. Sie sind nicht Unterauftragsverarbeiter der Klarplan AG.