retailflow

ART. 28 DSGVO

Vereinbarung zur Auftragsverarbeitung (AVV)

Anlage zum Vertrag über die Nutzung von retailflow (AGB retailflow, Stand November 2026)

Auftragnehmer	Version	Stand
Nordflow Software GmbH	1.0	November 2026

Vertragsparteien

Diese Vereinbarung wird geschlossen zwischen

dem Kunden, wie er im Vertragsdokument oder bei der Buchung angegeben ist (Einzelvertrag, Online-Buchung oder Buchung über eine App-Plattform),
– „Kunde“ (Auftraggeber) –

und

Nordflow Software GmbH, Schauenburgerstraße 116, 24118 Kiel, vertreten durch die Geschäftsführer Max Löhrer und Christoph von Trotha, Amtsgericht Kiel, HRB 25644 KI,
– „Nordflow“ (Auftragnehmer) –

über die Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO.

Präambel

Nordflow stellt dem Kunden die KI-Software retailflow als Software-as-a-Service bereit. Der Kunde bindet den KI-Assistenten als Chat in seinen Onlineshop ein oder setzt ihn als Web-App in seinen Geschäften („Stores“) ein und richtet ihn im Dashboard ein. Grundlage ist der Vertrag über die Nutzung von retailflow, bestehend aus dem Vertragsdokument, der Beschreibung des Abo-Plans und den AGB retailflow („Vertrag“).

Dabei verarbeitet Nordflow personenbezogene Daten im Auftrag des Kunden, vor allem die Chats seiner Endkunden. Diese Vereinbarung legt die Pflichten der Parteien dazu fest, nach der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, „DSGVO“) und dem Bundesdatenschutzgesetz (BDSG). Sie gilt für alle Tätigkeiten im Rahmen des Vertrags, bei denen Beschäftigte von Nordflow oder von Nordflow Beauftragte personenbezogene Daten im Auftrag des Kunden verarbeiten („Daten“).

Nicht unter diese Vereinbarung fallen Verarbeitungen, für die Nordflow selbst verantwortlich ist: das Kundenkonto und die Nutzer des Kunden, Vertragsschluss, Abrechnung und Kommunikation mit dem Kunden sowie die Website von Nordflow. Dafür gilt die Datenschutzerklärung von Nordflow.

„Endkunden“ sind die Besucher des Onlineshops oder der Stores des Kunden, die den Assistenten nutzen (§ 1.4 AGB).

§ 1 Gegenstand, Dauer und Ort der Verarbeitung

(1) Gegenstand ist die Bereitstellung und der Betrieb von retailflow für die Onlineshops und Stores des Kunden. Art und Zweck der Verarbeitung, die Arten der Daten und die Kategorien betroffener Personen stehen in Anlage 1. Diese Vereinbarung gilt für den Einsatz von retailflow in Onlineshops und als Web-App in Stores (Anlage 1 Nr. 2).

(2) Die Vereinbarung gilt für die Laufzeit des Vertrags. Pflichten, die über das Vertragsende hinaus bestehen, insbesondere zur Löschung (§ 3 Abs. 10) und zur Vertraulichkeit, gelten fort, bis sie erfüllt sind.

(3) Nordflow speichert die Daten in einer Datenbank in Frankfurt am Main (EU). Verarbeitungen und Speicherungen in Drittländern, etwa durch KI-Anbieter, finden nur nach § 8 und in dem in der Liste nach § 7 Abs. 4 beschriebenen Umfang statt.

§ 2 Verantwortlichkeit und Weisungen

(1) Der Kunde ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er allein beurteilt, ob die Verarbeitung zulässig ist und ob er die Daten an Nordflow weitergeben darf. Jede Partei ist für die Einhaltung des für sie geltenden Datenschutzrechts selbst verantwortlich.

(2) Nordflow verarbeitet die Daten nur auf dokumentierte Weisung des Kunden. Das gilt nicht, wenn Nordflow nach dem Recht der Union oder eines Mitgliedstaats, dem Nordflow unterliegt, zur Verarbeitung verpflichtet ist. In diesem Fall teilt Nordflow dem Kunden diese Pflicht vor der Verarbeitung mit, es sei denn, das betreffende Recht verbietet die Mitteilung wegen eines wichtigen öffentlichen Interesses.

(3) Die Weisungen des Kunden ergeben sich aus dem Vertrag und dieser Vereinbarung samt Anlagen. Dazu gehört, dass Nordflow die Daten so verarbeitet, wie der Kunde retailflow im Dashboard einrichtet (§ 3.1 AGB). Handlungen der Nutzer, denen der Kunde Zugang zum Dashboard gegeben hat, werden dem Kunden zugerechnet.

(4) **Variante der KI-Verarbeitung.** Für die KI-Verarbeitung gibt es die Varianten „Standard“ und „EU-Verarbeitung“ (Anlage 1 Nr. 5). Für den Kunden gilt die Variante, die die Parteien bei Vertragsschluss im Vertragsdokument oder in Textform (zum Beispiel per E-Mail) vereinbart haben. Ist nichts vereinbart, gilt „Standard“. Nordflow stellt die vereinbarte Variante ein, bevor Inhalte des Kunden aufbereitet werden und bevor der erste Chat stattfindet. Später kann der Kunde eine andere Variante im Dashboard beantragen. Der Antrag ist ein Wunsch nach einer Änderung der Leistung. Ob und wann Nordflow ihm folgt, entscheidet Nordflow. Nordflow stellt die Variante nur auf Antrag des Kunden um. Die vereinbarte Variante und, nach einer Umstellung, die beantragte Variante sind die dokumentierte Weisung des Kunden. Bis zu einer Umstellung gilt die bisherige Variante. Über die Umstellung informiert Nordflow den Kunden per E-Mail an den Kontakt nach § 4 Abs. 3. Lehnt Nordflow einen Antrag ab, teilt Nordflow ihm das mit. Das Dashboard zeigt immer die geltende Variante und den Zeitpunkt, seit dem sie gilt. Nordflow speichert zu jedem Antrag und jeder Umstellung den Zeitpunkt, den antragstellenden Nutzer sowie die alte und die neue Variante.

(5) Darüber hinaus kann der Kunde Einzelweisungen in Textform (zum Beispiel per E-Mail) an den Datenschutz-Kontakt von Nordflow (§ 3 Abs. 8) erteilen. Mündliche Weisungen bestätigt der Kunde unverzüglich in Textform. Weisungen, die im Vertrag nicht vorgesehen sind, behandelt Nordflow als Wunsch nach einer Änderung der Leistung.

(6) **Anonymisierung.** Der Kunde weist Nordflow an, Chats, Feedback und Auswertungen zu anonymisieren und die anonymisierten Daten zu nutzen, um retailflow zu verbessern und weiterzuentwickeln (§ 12.4 AGB). Die Anonymisierung betrifft nur die Daten, die Nordflow für diesen Zweck verwendet. Die Chats des Kunden bleiben unverändert gespeichert, bis sie nach Anlage 1 Nr. 6 gelöscht werden. Anonym sind Daten erst, wenn sie mit den Mitteln, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, weder einer Person noch dem Kunden noch einem einzelnen Chat zugeordnet werden können. Nordflow legt das Verfahren der Anonymisierung fest, dokumentiert es und stellt dem Kunden die Beschreibung auf Anfrage zur Verfügung. Anonymisierte Daten gibt Nordflow an Dritte nur in einer Form weiter, die keine Rückschlüsse auf den Kunden zulässt.

(7) **Kein KI-Training.** Nordflow verwendet die Daten nicht zum Training von KI-Modellen und gestattet auch den Unterauftragsverarbeitern nicht, die Daten dafür zu nutzen.

§ 3 Pflichten von Nordflow

(1) Nordflow verarbeitet die Daten nur im Rahmen des Vertrags und der Weisungen des Kunden, außer im Fall des § 2 Abs. 2 Satz 2. Für eigene Zwecke verarbeitet Nordflow die Daten nicht. § 2 Abs. 6 bleibt unberührt.

(2) Ist Nordflow der Ansicht, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften der Union oder der Mitgliedstaaten verstößt, informiert Nordflow den Kunden unverzüglich. Nordflow darf die Umsetzung der Weisung aussetzen, bis der Kunde sie bestätigt oder ändert. Eine umfassende rechtliche Prüfung schuldet Nordflow nicht. Mehrkosten, die durch eine zusätzliche oder abweichende Einzelweisung entstehen, trägt der Kunde, es sei denn, die Weisung ist nötig, damit gesetzliche Anforderungen erfüllt werden.

(3) Nordflow trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 2 beschrieben sind. Sie sollen die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste auf Dauer sicherstellen. Die Parteien sind sich einig, dass diese Maßnahmen ein dem Risiko angemessenes Schutzniveau bieten. Nordflow darf die Maßnahmen an den Stand der Technik anpassen und durch gleichwertige ersetzen. Das Schutzniveau der Anlage 2 darf dabei nicht sinken. Wesentliche Änderungen dokumentiert Nordflow und teilt sie dem Kunden auf Anfrage mit.

(4) Nordflow unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen nach Kapitel III DSGVO zu beantworten (§ 5).

(5) Nordflow unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der Nordflow vorliegenden Informationen bei den Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei einer Datenschutz-Folgenabschätzung. Dafür stellt Nordflow vor allem die Beschreibungen in den Anlagen 1 und 2, die Liste nach § 7 Abs. 4 und auf Anfrage weitere vorhandene Informationen bereit. Für Unterstützung, die darüber hinausgeht und nicht auf einen Verstoß von Nordflow zurückgeht, kann Nordflow eine angemessene Vergütung nach Aufwand verlangen, wenn Nordflow dies vorher ankündigt.

(6) Nordflow stellt sicher, dass alle Beschäftigten und sonstigen für Nordflow tätigen Personen, die mit den Daten arbeiten, zur Vertraulichkeit verpflichtet sind, auch über das Ende ihrer Tätigkeit und dieses Auftrags hinaus, und dass sie die Daten nur nach Weisung verarbeiten. Sie greifen auf die Daten nur zu, soweit es für Betrieb, Support, Fehlerbehebung, Qualitätssicherung (Anlage 1 Nr. 2) oder

Sicherheit von retailflow erforderlich ist. Fehler, die dabei auffallen, darf Nordflow für alle Kunden beheben. Darüber hinaus nutzt Nordflow Chats für die Weiterentwicklung von retailflow nur in anonymisierter Form (§ 2 Abs. 6).

(7) **Verletzungen des Schutzes der Daten.** Nordflow meldet dem Kunden eine Verletzung des Schutzes der Daten unverzüglich, spätestens 24 Stunden nachdem Nordflow von ihr Kenntnis erlangt hat. Die Meldung geht per E-Mail an den Kontakt des Kunden (§ 4 Abs. 3). Sie enthält, soweit bekannt:

- eine Beschreibung der Verletzung, möglichst mit der Art der Verletzung, den Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze,
- Name und Kontaktdaten einer Anlaufstelle bei Nordflow,
- die wahrscheinlichen Folgen der Verletzung,
- die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und zur Abmilderung möglicher nachteiliger Folgen.

Was zum Zeitpunkt der Meldung noch nicht bekannt ist, liefert Nordflow ohne unangemessene Verzögerung nach. Nordflow ergreift unverzüglich die erforderlichen Maßnahmen, um die Daten zu sichern und nachteilige Folgen für die betroffenen Personen zu mindern. Die Meldung an die Aufsichtsbehörde und die Benachrichtigung betroffener Personen (Art. 33, 34 DSGVO) sind Sache des Kunden. Nordflow gibt in seinem Namen nur auf seine Weisung Meldungen oder Benachrichtigungen ab.

(8) **Datenschutz-Kontakt.** Ansprechpartner für Datenschutzfragen im Rahmen dieser Vereinbarung ist: Nordflow Software GmbH, E-Mail: datenschutz@retailflow.app. Nordflow hat keinen Datenschutzbeauftragten benannt. Den jeweils aktuellen Kontakt nennt Nordflow in der Datenschutzerklärung auf retailflow.app.

(9) Nordflow führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

(10) **Vertragsende.** Nach dem Ende des Vertrags löscht Nordflow die Daten, spätestens 30 Tage nach Vertragsende. Bis dahin kann der Kunde verlangen, dass Nordflow ihm die Chats samt Feedback und Auswertungen in einem gängigen, maschinenlesbaren Format (JSON oder CSV) herausgibt. Besteht eine gesetzliche Pflicht zur Aufbewahrung, sperrt Nordflow die betroffenen Daten und löscht sie nach Ablauf der Frist. Kopien in Datensicherungen und Protokollen der Unterauftragsverarbeiter werden nach deren Fristen gelöscht (Anlage 1 Nr. 6). Nordflow bestätigt die Löschung auf Anfrage in Textform. Wünscht der Kunde die Herausgabe in einem anderen Format, trägt er die Mehrkosten.

Bei Buchung über eine App-Plattform (zum Beispiel Shopify) gilt als Vertragsende auch die Kündigung des Abos bei der Plattform oder die Deinstallation der App.

(11) Nordflow informiert den Kunden unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde, soweit sie diese Vereinbarung betreffen.

§ 4 Pflichten des Kunden

(1) Der Kunde ist dafür verantwortlich, dass die Verarbeitung gegenüber den Endkunden rechtmäßig ist. Er sorgt insbesondere für

- eine Rechtsgrundlage für den Einsatz des Assistenten,
- die Information der Endkunden in seiner Datenschutzerklärung. Nordflow stellt ihm dafür im Dashboard einen Textbaustein passend zur geltenden Variante bereit. Im Store sorgt der Kunde dafür,

dass Endkunden die Information vor der Nutzung der Web-App finden, zum Beispiel über einen Hinweis am QR-Code oder am Terminal,

- den Link zu seiner Datenschutzerklärung in den Einstellungen des Assistenten,
- die Einwilligungen, die für die Zuordnung von Bestellungen nötig sind, über sein Cookie-Banner (§ 6.3 AGB).

Wird die Variante umgestellt (§ 2 Abs. 4), passt der Kunde seine Datenschutzerklärung unverzüglich nach der Mitteilung von Nordflow an.

(2) Der Kunde informiert Nordflow unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

(3) Der Kunde nennt Nordflow einen Kontakt für Datenschutzfragen und hält ihn aktuell. Solange er keinen anderen nennt, gilt die bei der Buchung angegebene E-Mail-Adresse.

(4) Der Assistent ist nicht dafür bestimmt, besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) zu verarbeiten. Die Endkunden werden vor der ersten Nachricht gebeten, keine Gesundheitsdaten oder anderen sensiblen Angaben einzugeben. Lässt das Sortiment des Kunden erwarten, dass Endkunden solche Angaben dennoch machen, etwa bei Gesundheitsprodukten, prüft der Kunde, ob eine Datenschutz-Folgenabschätzung erforderlich ist.

(5) Wird eine Partei von einer betroffenen Person auf Schadensersatz nach Art. 82 DSGVO in Anspruch genommen, unterstützt die andere Partei sie im Rahmen ihrer Möglichkeiten bei der Abwehr des Anspruchs.

§ 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit einem Antrag nach Kapitel III DSGVO an Nordflow, verweist Nordflow sie an den Kunden und leitet den Antrag unverzüglich an ihn weiter, soweit Nordflow ihn dem Kunden zuordnen kann. Nordflow beantwortet den Antrag nicht selbst.

(2) Nordflow unterstützt den Kunden bei der Beantwortung. Auf Weisung des Kunden erteilt Nordflow innerhalb von 5 Werktagen Auskunft über einen Chat (Herausgabe der gespeicherten Daten), berichtigt die Daten, löscht sie oder schränkt ihre Verarbeitung ein. Beim Löschen entfernt Nordflow den Chat samt Feedback, Auswertung und Bestellzuordnung. Damit Nordflow den Chat findet, nennt der Kunde die Chat-ID oder den ungefähren Zeitpunkt und Inhalt des Gesprächs.

(3) Anfragen zu einzelnen Endkunden, die über Shopify eingehen (Datenanfrage oder Löschung), behandelt Nordflow als Weisung des Kunden. Bei einer Löschung entfernt Nordflow die Bestellzuordnungen und die Tracking-Kennung zu dem Endkunden. Bei einer Datenanfrage teilt Nordflow dem Kunden mit, welche Daten zu den genannten Bestellungen gespeichert sind.

(4) Die Unterstützung bei einzelnen Anträgen ist mit der Vergütung nach dem Vertrag abgegolten. Bei ungewöhnlich vielen Anträgen kann Nordflow nach vorheriger Ankündigung eine angemessene Vergütung nach Aufwand verlangen.

(5) Auskünfte an Dritte erteilt Nordflow nur mit vorheriger Zustimmung des Kunden in Textform oder wenn Nordflow nach dem Recht der Union oder eines Mitgliedstaats dazu verpflichtet ist. Im zweiten Fall informiert Nordflow den Kunden vorher, soweit das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

§ 6 Nachweise und Kontrollen

(1) Nordflow weist dem Kunden die Einhaltung dieser Vereinbarung mit geeigneten Mitteln nach und stellt ihm auf Anfrage die dafür nötigen Informationen zur Verfügung, insbesondere zur Umsetzung der Maßnahmen nach Anlage 2.

(2) Als Nachweis dienen insbesondere

- aktuelle Selbstauskünfte und Berichte von Nordflow zu den Maßnahmen nach Anlage 2,
- Berichte oder Testate unabhängiger Prüfer,
- Zertifizierungen, auch die der Unterauftragsverarbeiter (zum Beispiel ISO/IEC 27001 oder SOC 2),
- genehmigte Verhaltensregeln (Art. 40 DSGVO) oder Zertifizierungen nach Art. 42 DSGVO.

(3) Der Kunde kann die Einhaltung dieser Vereinbarung in angemessenen Abständen prüfen, außerdem jederzeit bei Anhaltspunkten für einen Verstoß. Er kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen, der zur Verschwiegenheit verpflichtet ist und nicht im Wettbewerb mit Nordflow steht. Bei der Entscheidung über eine Prüfung berücksichtigt der Kunde die Nachweise nach Abs. 2.

(4) Prüfungen umfassen Auskünfte, die Einsicht in Unterlagen und, soweit nötig, Inspektionen vor Ort. Eine reguläre Inspektion vor Ort findet höchstens einmal im Kalenderjahr statt, mit angemessener Ankündigung (in der Regel mindestens 14 Tage), während der üblichen Geschäftszeiten und ohne vermeidbare Störung des Betriebs. Anlassbezogene Prüfungen, etwa nach einer Verletzung des Schutzes der Daten, bleiben davon unberührt. Die Sicherheits- und Vertraulichkeitsinteressen von Nordflow und anderer Kunden sind zu wahren. Nordflow kann dazu eine Verschwiegenheitsvereinbarung verlangen. Sie darf den Kunden nicht daran hindern, die Ergebnisse gegenüber der Aufsichtsbehörde zu verwenden.

(5) Die Systeme, auf denen die Daten verarbeitet werden, betreiben die Unterauftragsverarbeiter in ihren Rechenzentren. Diese Systeme werden über die Zertifikate und Prüfberichte der Unterauftragsverarbeiter geprüft. Nordflow macht sie dem Kunden auf Anfrage zugänglich, soweit die Unterauftragsverarbeiter dies erlauben.

(6) Jede Partei trägt ihre eigenen Kosten der Prüfungen, auch bei Nachprüfungen.

(7) Prüfungen der zuständigen Aufsichtsbehörde ermöglicht Nordflow ohne die Beschränkungen des Abs. 4.

§ 7 Unterauftragsverarbeiter

(1) Die Unterauftragsverarbeiter, die bei Abschluss dieser Vereinbarung in der Liste nach Abs. 4 stehen, gelten als genehmigt. Für Unterauftragsverarbeiter, die die Liste nur für eine Variante vorsieht, gilt die Genehmigung nur, solange diese Variante für den Kunden gilt (§ 2 Abs. 4). Nordflow setzt für den Kunden nur die Unterauftragsverarbeiter ein, die die Liste für beide Varianten und für seine Variante vorsieht. Eine Umstellung der Variante auf Antrag des Kunden ist keine Änderung im Sinne von Abs. 2.

(2) Darüber hinaus erteilt der Kunde Nordflow eine allgemeine Genehmigung, weitere Unterauftragsverarbeiter hinzuzuziehen oder bestehende zu ersetzen. Nordflow informiert den Kunden darüber mindestens 14 Kalendertage vorher in Textform (zum Beispiel per E-Mail an den Kontakt nach § 4

Abs. 3) und aktualisiert die Liste nach Abs. 4. Der Kunde kann der Änderung innerhalb dieser Frist aus einem wichtigen datenschutzrechtlichen Grund in Textform widersprechen. Widerspricht er nicht, gilt die Änderung als genehmigt. Widerspricht er, suchen die Parteien gemeinsam eine Lösung. Kann Nordflow den neuen Unterauftragsverarbeiter für den Kunden nicht vermeiden, können beide Parteien den Vertrag zu dem Zeitpunkt kündigen, zu dem die Änderung wirksam werden soll. Fällt ein Unterauftragsverarbeiter ersatzlos weg, aktualisiert Nordflow nur die Liste nach Abs. 4.

(3) Muss Nordflow einen Unterauftragsverarbeiter kurzfristig ersetzen, etwa bei einem dringenden Sicherheitsrisiko oder einem unvorhergesehenen Ausfall, darf Nordflow die Frist nach Abs. 2 unterschreiten. Nordflow informiert den Kunden dann unverzüglich. Das Widerspruchsrecht nach Abs. 2 gilt ab dieser Information.

(4) Die aktuelle Liste der Unterauftragsverarbeiter steht unter www.retailflow.app/retailflow-subprocessors und ist Teil dieser Vereinbarung. Sie nennt mindestens Name und Anschrift, die übernommene Leistung, die verarbeiteten Daten, den Ort der Verarbeitung und die Grundlage für Übermittlungen in Drittländer. Sie verweist außerdem auf die Listen der weiteren Unterauftragsverarbeiter. Nordflow prüft die Liste mindestens einmal im Jahr und aktualisiert sie bei jeder Änderung. Nordflow bewahrt frühere Fassungen der Liste mit Datum auf und stellt sie dem Kunden auf Anfrage zur Verfügung.

(5) Nordflow wählt die Unterauftragsverarbeiter sorgfältig aus und verpflichtet sie vertraglich nach Art. 28 Abs. 4 DSGVO auf die Datenschutzpflichten dieser Vereinbarung, insbesondere auf hinreichende Garantien für geeignete technische und organisatorische Maßnahmen. Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet Nordflow gegenüber dem Kunden in vollem Umfang für die Einhaltung der Pflichten dieses Unterauftragsverarbeiters (Art. 28 Abs. 4 Satz 2 DSGVO).

(6) Keine Unterauftragsverarbeitung sind Nebenleistungen, die Nordflow bei Dritten in Anspruch nimmt, etwa Telekommunikation oder allgemeine Netzdienste. Shopify ist für die Verarbeitung auf seiner Plattform selbst verantwortlich und kein Unterauftragsverarbeiter von Nordflow. Das gilt auch für Daten, die über den Shop des Kunden bei Shopify laufen, etwa Warenkorb-Attribute und das Web Pixel.

§ 8 Übermittlung in Drittländer

(1) Nordflow übermittelt Daten in Länder außerhalb der EU und des EWR (Drittländer) nur auf dokumentierte Weisung des Kunden und nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Mit dieser Vereinbarung und der für ihn geltenden Variante (§ 2 Abs. 4) weist der Kunde die Übermittlungen an, die die Liste nach § 7 Abs. 4 für beide Varianten und für seine Variante beschreibt.

(2) Das angemessene Schutzniveau wird je Unterauftragsverarbeiter (Liste nach § 7 Abs. 4) gewährleistet durch

- einen Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO), insbesondere für das Vereinigte Königreich und für Unternehmen in den USA, die nach dem EU-US Data Privacy Framework zertifiziert sind, oder
- Standardvertragsklauseln der EU-Kommission (Art. 46 Abs. 2 lit. c DSGVO) in der jeweils geltenden Fassung, bei Bedarf mit zusätzlichen Maßnahmen.

Stützt sich eine Übermittlung auf Standardvertragsklauseln ohne Angemessenheitsbeschluss, bewertet Nordflow die Rechtslage und Praxis im Empfängerland (Transfer Impact Assessment), dokumentiert das Ergebnis und ergreift bei Bedarf zusätzliche technische, organisatorische oder vertragliche Maßnahmen. Nordflow stellt dem Kunden die Bewertung auf Anfrage zur Verfügung. Fällt eine Grundlage weg, etwa weil ein Angemessenheitsbeschluss aufgehoben wird oder eine Zertifizierung endet, stützt Nordflow die Übermittlung auf eine andere Grundlage nach Art. 46 DSGVO oder stellt sie ein und informiert den Kunden unverzüglich.

(3) **Variante „EU-Verarbeitung".** Alle Aufrufe von KI-Modellen laufen über Microsoft Azure in Rechenzentren in der EU: Sprachmodelle, Spracheingabe, Such-Vektoren und die Sortierung der Suchtreffer, für den Chat, für die Auswertung und für die Aufbereitung der Inhalte des Kunden. Chatinhalte, Spracheingaben, Auswertungen, Bestelldaten und Inhalte des Kunden werden in Rechenzentren in der EU verarbeitet. Ausnahmen, die in der Liste nach § 7 Abs. 4 beschrieben sind:

- IP-Adressen, Browserangaben und Kennungen beim Ausliefern des Chat-Fensters über das weltweite Netz von Vercel,
- Protokolle und Stichproben zur Fehlersuche bei Fly.io in den USA, die IP-Adressen enthalten können,
- Zugriffe von Supabase von außerhalb der EU im Einzelfall, etwa bei Support oder Sicherheitsvorfällen,
- E-Mails zu Anfragen von Endkunden, die über Shopify eingehen (Resend, Google).

Einige Unterauftragsverarbeiter mit Rechenzentren in der EU gehören zu Unternehmen mit Sitz in den USA. Fällt die Verarbeitung in der EU aus, verarbeitet Nordflow die Daten nicht ersatzweise in der Variante „Standard". Der betroffene Dienst ist dann vorübergehend nicht verfügbar.

(4) **Variante „Standard".** OpenAI Ireland Ltd verarbeitet Chatinhalte, Spracheingaben und Inhalte des Kunden für Antworten, Produktsuche, Spracheingabe, Auswertung und die Aufbereitung der Inhalte. OpenAI Ireland Ltd gibt die Daten an verbundene Unternehmen und eigene Unterauftragsverarbeiter in den USA und in weiteren Drittländern weiter (Liste nach § 7 Abs. 4). OpenAI ist nicht nach dem EU-US Data Privacy Framework zertifiziert. Grundlage dieser Übermittlungen sind Standardvertragsklauseln. Nordflow bewertet sie nach Abs. 2.

(5) Neue Übermittlungen in Drittländer führt Nordflow nur nach dem Verfahren des § 7 ein. Die Information nach § 7 Abs. 2 nennt dann das Drittland und die Grundlage der Übermittlung. Die Genehmigung nach § 7 gilt auch als Genehmigung nach diesem § 8.

§ 9 Haftung

(1) Die im Vertrag vereinbarte Haftungsregelung (§ 11 AGB) gilt auch für diese Vereinbarung.

(2) Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt.

§ 10 Schlussbestimmungen

(1) Werden die Daten bei Nordflow durch Pfändung, Beschlagnahme, ein Insolvenzverfahren oder sonstige Maßnahmen Dritter gefährdet, informiert Nordflow den Kunden unverzüglich. Nordflow teilt allen Beteiligten unverzüglich mit, dass die Hoheit über die Daten allein beim Kunden als Verantwortlichem liegt.

(2) Diese Vereinbarung wird zusammen mit dem Vertrag geschlossen: bei einer Online-Buchung und bei einer Buchung über eine App-Plattform durch Bestätigung im Bestellprozess, beim Einzelvertrag durch Bezugnahme im Vertragsdokument. Die elektronische Form genügt (Art. 28 Abs. 9 DSGVO). Nordflow speichert Zeitpunkt und Version der Zustimmung. Auf Wunsch erhält der Kunde die Vereinbarung als PDF.

(3) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform und eines ausdrücklichen Hinweises, dass es sich um eine Änderung dieser Vereinbarung handelt. Das gilt auch für einen Verzicht auf dieses Formerfordernis. Nordflow kann diese Vereinbarung außerdem nach dem Verfahren des § 13.2 AGB ändern (Mitteilung mindestens 30 Tage vorher, Widerspruch, Kündigungsrecht), wenn sich Rechtslage, Rechtsprechung, Vorgaben der Aufsichtsbehörden oder retailflow ändern und das Schutzniveau nicht sinkt. Änderungen bei den Unterauftragsverarbeitern richten sich allein nach § 7.

(4) Bei Widersprüchen geht diese Vereinbarung dem Vertrag und den AGB vor (§ 12.2 AGB). Ist ein Teil dieser Vereinbarung unwirksam, bleibt der Rest wirksam.

(5) Jede Partei darf Informationen aus dieser Vereinbarung nutzen, um Ansprüche Dritter abzuwehren und um nachzuweisen, dass sie für einen eingetretenen Schaden nicht verantwortlich ist.

(6) Es gilt deutsches Recht. Der Gerichtsstand richtet sich nach § 14.3 AGB.

Anlage 1: Einzelheiten der Verarbeitung

1. Verantwortlicher

Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist der Kunde.

2. Gegenstand, Art und Zweck der Verarbeitung

Nordflow betreibt für den Kunden einen KI-gestützten Chat-Assistenten in dessen Onlineshop und als Web-App in dessen Stores (Software-as-a-Service). Die Verarbeitung umfasst:

Leistung	Zweck	Was Nordflow dafür tut
Beratung im Chat	Endkunden zu den Produkten des Kunden beraten	Nachrichten entgegennehmen, Produkte und Wissensbasis durchsuchen, Antworten mit KI-Modellen erzeugen, den Chat speichern, damit der Endkunde ihn fortsetzen kann
Web-App im Store	Endkunden im Store beraten	Die Web-App bereitstellen. Sie ist das Chat-Fenster als eigene Seite. Endkunden öffnen sie über einen QR-Code auf ihrem eigenen Gerät oder nutzen sie auf einem Terminal im Store. Jeder QR-Code und jedes Terminal gehört zu einer festen Filiale.
Spracheingabe	Nachrichten per Sprache ermöglichen	Die Aufnahme in Text umwandeln. Die Aufnahme wird nicht gespeichert.
Feedback	Beratung bewerten lassen	Bewertung und Freitext am Chat speichern
Dashboard	Der Kunde sieht seine Chats und wertet sie aus	Chats, Feedback und Statistiken im Dashboard bereitstellen
Auswertung der Chats	Beratung und Sortiment des Kunden verbessern	Chats automatisch mit KI nach Anliegen, Service-Themen, Ergebnis und fehlenden Produkten auswerten und dem Kunden im Dashboard zeigen
Zuordnung von Bestellungen (nur im Onlineshop, nur wenn der Kunde sie einrichtet und der Endkunde einwilligt)	Auswerten, ob Beratungen zu Bestellungen führen	Eine Bestellung, die innerhalb von 14 Tagen nach einem Chat aufgegeben wird, diesem Chat zuordnen. In Shopify-Shops über das Web Pixel der App, in anderen Shops über die Bestelldaten, die der Shop auf der Bestellbestätigung für die Webanalyse bereitstellt.
Aufbereitung der Inhalte des Kunden	Grundlage für Suche und Antworten schaffen	Produktdaten importieren, Website-Inhalte abrufen, Texte übersetzen und zusammenfassen, Such-Vektoren erzeugen
Schutz und Betrieb	Missbrauch abwehren, Fehler beheben, Support leisten	Anfragen je IP-Adresse begrenzen, Protokolle mit Metadaten führen, im Einzelfall Support leisten
Qualitätssicherung	Funktion und Antworten des Assistenten für den Kunden prüfen	Berechtigte Beschäftigte von Nordflow sehen Chats im Dashboard ein: bei Supportanfragen, bei Fehlermeldungen und in Stichproben, um Fehler in Antworten, Einrichtung oder Wissensbasis zu erkennen und zu beheben

Leistung	Zweck	Was Nordflow dafür tut
Anfragen von Endkunden	Den Kunden bei den Rechten betroffener Personen unterstützen	Anfragen nach § 5 bearbeiten, auch solche, die über Shopify eingehen
Anonymisierung	retailflow weiterentwickeln	Daten nach § 2 Abs. 6 anonymisieren

Art der Verarbeitung: Erheben, Erfassen, Speichern, Ordnen, Auslesen, Abfragen, Verwenden, Übermitteln an Unterauftragsverarbeiter, Bereitstellen im Dashboard, Anonymisieren, Löschen.

Endkunden nutzen den Chat ohne Konto und ohne Angabe ihres Namens. Der Assistent kann keine Bestellungen auslösen und hat keinen Zugriff auf Kundenkonten oder Zahlungsdaten. Eine automatisierte Entscheidung im Sinne des Art. 22 DSGVO findet nicht statt.

3. Kategorien betroffener Personen

- **Endkunden:** Besucher des Onlineshops und der Stores des Kunden, die den Assistenten nutzen (Interessenten und Kunden des Kunden), einschließlich Kunden des Kunden, die über Shopify Auskunft oder Löschung verlangen
- **In den Inhalten des Kunden genannte Personen:** zum Beispiel Ansprechpartner im Impressum, auf Kontaktseiten oder in Produktdaten

4. Arten personenbezogener Daten

Kategorie	Daten	Hinweis
Chatinhalte	Nachrichten der Endkunden (bis 600 Zeichen), Antworten, gezeigte Produkte, Quellen, Suchphrasen, Sprache, Eingabeart, Zeitpunkte, im Store die Filiale	Freitext. Endkunden können darin beliebige Angaben machen, etwa Namen, Kontaktdaten, Bestellnummern oder Gesundheitsangaben.
Spracheingaben	Audioaufnahme (bis 20 Sekunden)	Wird nur umgewandelt, nicht gespeichert.
Feedback	Bewertung, Freitext, Bewertung einzelner Produkte, Zeitpunkt	
Kennungen	Zufällige Chat-ID. Nur mit Einwilligung: pseudonyme Browser-Kennung (Tracking-Kennung), Einwilligungsstatus, Zeitpunkt der letzten Nutzung	
Technische Daten	IP-Adresse, Angaben zu Browser und Gerät, Zugriffsprotokolle	Keine Standortermittlung, kein Fingerprinting
Bestelldaten (nur im Onlineshop, nur mit Einwilligung)	Bestellnummer, Gesamtsumme, Währung, je Artikel Nummer, Name, Variante, Menge und Preis, Zeitpunkt	Keine Namen, Anschriften, E-Mail-Adressen, Telefonnummern oder Zahlungsdaten
Auswertungen	Je Chat: Anliegen, Service-Thema, Ergebnis, fehlende Produkte mit Produktart, Eigenschaften, Marke, Preisrahmen, Größe und Menge	Aus den Chatinhalten abgeleitet

Kategorie	Daten	Hinweis
Inhalte des Kunden	Namen und Kontaktdaten in Website-Inhalten (Impressum, Kontaktseiten), in Produktdaten und in Textdokumenten	Personenbezug nur ausnahmsweise
Anfragen über Shopify	E-Mail-Adresse und Shopify-Kennung des Endkunden, Bestellnummern	

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO): Die Verarbeitung ist dafür nicht bestimmt. Im Freitext können solche Angaben dennoch vorkommen (§ 4 Abs. 4).

5. Varianten der KI-Verarbeitung

Es gilt die bei Vertragsschluss vereinbarte Variante, sonst „Standard“. Später kann der Kunde eine andere Variante im Dashboard beantragen. Ob und wann Nordflow umstellt, entscheidet Nordflow (§ 2 Abs. 4). Das Dashboard zeigt immer die geltende Variante und den Zeitpunkt, seit dem sie gilt.

Aufgabe	Standard	EU-Verarbeitung
Antworten im Chat und Such-Vektoren	OpenAI	Microsoft Azure, Rechenzentren in der EU
Spracheingabe	OpenAI	Microsoft Azure, Rechenzentren in der EU
Auswertung der Chats	OpenAI	Microsoft Azure, Rechenzentren in der EU
Aufbereitung der Inhalte des Kunden (Produkttexte, Übersetzungen, Such-Vektoren für Produkte und Wissensbasis)	OpenAI	Microsoft Azure, Rechenzentren in der EU
Datenbank, Server, Hintergrundaufgaben, Auslieferung des Chat-Fensters	Supabase, Fly.io, Trigger.dev, Vercel	wie Standard

In der Variante „EU-Verarbeitung“ laufen alle Aufrufe von KI-Modellen über Microsoft Azure in der EU, auch die Sortierung der Suchtreffer (§ 8 Abs. 3).

Eine Umstellung gilt ab ihrem Zeitpunkt für alle weiteren Verarbeitungen, auch für Chats, die vorher begonnen haben. Bereits gespeicherte Daten bleiben in der Datenbank in Frankfurt am Main. Zum Ausfall der Verarbeitung in der EU siehe § 8 Abs. 3.

6. Speicherdauer und Löschung

Daten	Speicherdauer
Chats, Feedback, Auswertungen, Bestellzuordnungen	Für die Dauer des Vertrags. Der Kunde kann einzelne Chats früher löschen lassen (§ 5 Abs. 2). Löschung spätestens 30 Tage nach Vertragsende (§ 3 Abs. 10).
Vollständige Modell-Eingabe eines Chats (einschließlich Suchergebnissen)	72 Stunden nach der letzten Nachricht
Spracheingaben	Nicht gespeichert

Daten	Speicherdauer
IP-Adresse	Zum Schutz vor Missbrauch nur im Arbeitsspeicher. Protokolliert nur, wenn die zulässige Zahl von Anfragen überschritten wird. In Zugriffsprotokollen von Vercel einen Tag, in Protokollen und Stichproben zur Fehlersuche von Fly.io bis zu 60 Tage.
Tracking-Kennung	Bis zum Widerruf der Einwilligung durch den Endkunden. Dann wird sie im Browser und am Chat gelöscht.
Inhalte des Kunden	Bis der Kunde sie löscht, spätestens 30 Tage nach Vertragsende
E-Mails zu Anfragen über Shopify	Im Postfach von Nordflow bis 30 Tage nach Erledigung der Anfrage. Bei Resend 30 Tage nach dem Versand.
Bei den KI-Anbietern	Je nach Variante halten OpenAI oder Microsoft Eingaben zur Erkennung von Missbrauch in der Regel bis zu 30 Tage vor.
Datensicherungen der Datenbank	7 Tage. Die Datenbank wird täglich gesichert. Gelöschte Daten sind spätestens nach 7 Tagen auch aus den Sicherungen entfernt.

Anlage 2: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Nordflow betreibt keine eigenen Server oder Rechenzentren. retailflow läuft bei den Unterauftragsverarbeitern nach § 7 Abs. 4. Die Maßnahmen bestehen deshalb aus eigenen Maßnahmen von Nordflow und den Maßnahmen der Anbieter. Deren Nachweise (zum Beispiel ISO/IEC 27001, SOC 2) prüft Nordflow vor der Beauftragung und bei Änderungen.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

- Die Daten werden in Rechenzentren der Unterauftragsverarbeiter verarbeitet, vor allem in Frankfurt am Main. Deren physische Schutzmaßnahmen sind durch Zertifizierungen nachgewiesen.
- Nordflow speichert die Daten nicht auf eigenen Servern. Kopien auf Arbeitsgeräten entstehen nur im Einzelfall, soweit sie für Support oder Herausgabe nötig sind, und werden danach gelöscht.

1.2 Zugangskontrolle

- Ein Konto für das Dashboard entsteht nur bei einer Buchung (zum Beispiel über Shopify) oder per Einladung. Der Nutzer erhält einen einmal gültigen Link an seine E-Mail-Adresse und setzt darüber sein Passwort. Ein Konto aus einer Buchung erhält immer eine neue, eigene Organisation. Zugang zu einer bestehenden Organisation gibt es nur per Einladung.
- Passwörter haben mindestens 8 Zeichen mit Großbuchstabe, Ziffer und Sonderzeichen. Die Regel wird auf dem Server geprüft. Passwörter werden nur als Hashwert gespeichert.
- Sitzungen sind zeitlich begrenzt und werden mit rotierenden Erneuerungstoken verlängert.
- Admin-Zugänge zum Dashboard sowie alle Zugänge zu den Konten bei den Unterauftragsverarbeitern und zum Quellcode sind mit Zwei-Faktor-Anmeldung geschützt.
- Arbeitsgeräte sind verschlüsselt, sperren sich automatisch und erhalten Sicherheitsupdates.
- Zugänge werden beim Ausscheiden von Beschäftigten sofort entzogen.

1.3 Zugriffskontrolle

- Nutzer des Kunden sehen nur die Daten ihrer eigenen Organisation. Das setzen Zugriffsregeln in der Datenbank durch (Row Level Security).
- Admin-Rechte haben nur namentlich festgelegte Beschäftigte von Nordflow. Nordflow führt eine Liste dieser Personen. Sie greifen auf Daten des Kunden nur zu, soweit es für Betrieb, Support, Fehlerbehebung, Qualitätssicherung oder Sicherheit erforderlich ist. Ihre Zugriffe werden protokolliert.
- Serverkomponenten mit erweiterten Rechten nutzen ihre Schlüssel nur in der Serverumgebung. Die Shopify-App nutzt eine eigene, eingeschränkte Datenbankrolle ohne Zugriff auf Chatinhalte.
- Schlüssel und Zugangsdaten liegen nur in geschützten Umgebungsvariablen der Plattformen, nicht im Quellcode. Kompromittierte oder offengelegte Schlüssel werden sofort ersetzt.
- Zugangsdaten zu Shops und Produktfeeds werden verschlüsselt gespeichert und im Dashboard nicht im Klartext angezeigt.

- Die öffentlichen Schnittstellen des Chats sind auf das Nötigste beschränkt: Sitzungen sind an den Assistenten gebunden, Kennungen werden zufällig erzeugt, Anfragen werden je IP-Adresse begrenzt, auch bei Spracheingabe und Feedback.

1.4 Trennungskontrolle

- Jeder Datensatz ist einer Organisation zugeordnet. Zugriffsregeln der Datenbank und Prüfungen in den Serverkomponenten verhindern den Zugriff auf Daten anderer Kunden. Die Trennung wird regelmäßig getestet.
- Entwicklung, Test und Produktion sind getrennt. Für Entwicklung und Test werden keine Produktivdaten verwendet.
- Für die Variante „EU-Verarbeitung“ nutzt Nordflow eigene KI-Ressourcen bei Microsoft Azure in der EU. Die Variante gilt je Organisation. Nur Nordflow stellt sie um, auf Antrag des Kunden.

1.5 Pseudonymisierung und Datensparsamkeit

- Der Chat funktioniert ohne Konto und ohne Namen. Die Chat-ID ist eine zufällige Kennung. Die Tracking-Kennung ist pseudonym und wird nur mit Einwilligung gesetzt.
- An die KI-Anbieter gehen keine Nutzer-, Sitzungs- oder IP-Kennungen. Die Auswertung der Chats erhält keine Kennungen.
- Spracheingaben werden nicht gespeichert. Die vollständige Modell-Eingabe eines Chats wird nach 72 Stunden geleert.
- Die Zuordnung von Bestellungen erfolgt ohne Namen, Anschriften, Kontaktdaten und Zahlungsdaten. Die Shopify-App hat keine Berechtigung für Kunden- oder Bestelldaten des Shops.
- Der Assistent setzt keine Cookies. Nachrichten sind auf 600 Zeichen begrenzt.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

- Alle Übertragungen sind verschlüsselt (HTTPS mit TLS).
- Gespeicherte Daten verschlüsseln die Anbieter (Verschlüsselung ruhender Daten).
- Webhooks von Shopify werden anhand ihrer Signatur geprüft. Interne Schnittstellen sind durch geheime Schlüssel geschützt.
- Daten gehen nur an die Unterauftragsverarbeiter nach § 7 Abs. 4. Bei den KI-Anbietern ist die Speicherung von Antworten abgeschaltet, soweit der Anbieter das anbietet. Das Training mit den Daten ist vertraglich ausgeschlossen.
- Protokolle der Chat-API, der Hintergrundaufgaben und der Serverfunktionen enthalten keine Chatinhalte und keine Kennungen der Endkunden, sondern nur Metadaten wie Zeit, Dauer, Kosten und Fehlerart. IP-Adressen werden nur protokolliert, wenn die zulässige Zahl von Anfragen überschritten wird.

2.2 Eingabekontrolle

- Chats werden mit Zeitpunkt gespeichert.
- Anträge auf eine andere Variante und jede Umstellung werden mit Zeitpunkt, antragstellendem Nutzer sowie alter und neuer Variante gespeichert.
- Zugriffe von Admins auf Daten des Kunden werden protokolliert.

- Änderungen am Quellcode laufen über eine Versionsverwaltung und sind nachvollziehbar.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Der Betrieb läuft bei Anbietern mit redundanten Rechenzentren und Schutz vor Überlastungsangriffen.
- Chat-API und Shopify-App laufen dauerhaft.
- Anfragen werden je IP-Adresse begrenzt. Für jeden Assistenten gilt ein Monatslimit.
- Die Datenbank wird täglich gesichert. Die Sicherungen werden 7 Tage aufbewahrt.
- Fällt die Verarbeitung in der EU aus, gibt es keinen Rückfall auf die Variante „Standard“.

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- **Organisation:** Verantwortlich für den Datenschutz bei Nordflow ist die Geschäftsführung. Alle Beschäftigten sind auf Vertraulichkeit verpflichtet und werden zum Datenschutz geschult. Nordflow führt ein Verzeichnis nach Art. 30 Abs. 2 DSGVO.
- **Vorfälle:** Es gibt einen dokumentierten Ablauf: erkennen, bewerten, eindämmen, den Kunden binnen 24 Stunden informieren, nachbereiten.
- **Unterauftragsverarbeiter:** Nordflow beauftragt nur Anbieter mit einem Vertrag nach Art. 28 DSGVO und einer Grundlage für Übermittlungen in Drittländer. Nordflow prüft ihre Nachweise vor der Beauftragung und bei Änderungen und verfolgt ihre Mitteilungen über eigene Unterauftragsverarbeiter.
- **Löschung:** Es gibt einen dokumentierten Ablauf für das Vertragsende und für einzelne Chats.
- **Überprüfung:** Nordflow überprüft diese Maßnahmen mindestens einmal im Jahr und bei wesentlichen Änderungen. Bei Änderungen am Code wird geprüft, dass keine Chatinhalte oder Kennungen in Protokolle oder in Daten von Hintergrundaufgaben gelangen.
- **Datenschutzfreundliche Voreinstellungen:** Vor der ersten Nachricht weist der Chat auf den Einsatz von KI hin und bittet, keine sensiblen Angaben einzugeben. Bestellungen werden nur nach Einwilligung zugeordnet.