RECHTLICHES

Vertrag über die Auftragsverarbeitung (AVV) nach Art. 28 DSGVO

Fassung vom 30. Oktober 2026 · wunschfund.de/avv.html

Zwischen

[Firma des Shops, Anschrift], im Folgenden „Verantwortlicher“,

und

purplebase, Inhaber Alexander Stepputt, Waldweg 25, 29323 Wietze, Deutschland, im Folgenden „Auftragsverarbeiter“.

---

§ 1 Gegenstand und Dauer

1. Der Auftragsverarbeiter betreibt für den Verantwortlichen die Produktsuche „wunschfund“ (Suchfeld, Suchseite, Empfehlungen im Onlineshop des Verantwortlichen sowie Kundenbereich) auf Grundlage des Hauptvertrags (AGB wunschfund und Bestellung vom [Datum]) oder, vor einer Bestellung, auf Grundlage der kostenlosen Demo nach § 2 Abs. 3 der AGB wunschfund. Dieser Vertrag regelt die dabei im Auftrag anfallende Verarbeitung personenbezogener Daten, in der Demo ebenso wie nach einer Bestellung.
2. Der Vertrag wird mit der Demo-Anmeldung geschlossen, spätestens mit der Bestellung. Bucht der Verantwortliche im Anschluss an die Demo einen Tarif, gilt dieser Vertrag ohne erneuten Abschluss fort; seine Laufzeit entspricht dann der des Hauptvertrags. Endet die Demo ohne Bestellung, endet auch dieser Vertrag; die Daten werden nach § 11 gelöscht. Pflichten, die über das Vertragsende hinauswirken (§§ 10, 11), gelten bis zur vollständigen Löschung.
3. Nicht Gegenstand dieses Vertrags ist die Verarbeitung der Daten, für die der Auftragsverarbeiter selbst verantwortlich ist (Vertragsverwaltung, Abrechnung, Zahlung über Stripe, Anmeldung und Protokoll im Kundenbereich; siehe Datenschutzhinweise Kundenbereich).

---

§ 2 Art, Zweck und Umfang der Verarbeitung

1. **Zwecke:**
   a) Beantwortung von Suchanfragen der Shop-Besucher über den Produktkatalog des Verantwortlichen, einschließlich Relevanzbewertung durch einen KI-Dienst (Anlage 2 Nr. 2);
   b) Anzeige von Produktempfehlungen (z. B. „zusammen gekauft“, „zuletzt angesehen“);
   c) Schutz der Suche vor Missbrauch und unkontrollierten Kosten (Rate-Limits, Kostendeckel);
   d) anonyme Tagesstatistik, damit die Suche für diesen Shop besser wird, und deren Auswertung für den Verantwortlichen (Kundenbereich, CSV-Export);
   e) Anonymisierung bzw. Aggregation von Nutzungsdaten nach § 4 Abs. 2.
2. **Art der Verarbeitung:** Erheben, flüchtiges Speichern im Arbeitsspeicher, Zwischenspeichern, Zählen, Auswerten, Übermitteln an Unterauftragsverarbeiter, Löschen.
3. **Kategorien betroffener Personen:**
   a) Besucher des Onlineshops, die Suche oder Empfehlungen nutzen;
   b) Käufer, soweit eine Bestellung (nur Produktnummern) gemeldet wird.

4. **Kategorien von Daten:**
   a) **Suchbegriffe** (Freitext; können unbeabsichtigt personenbezogene oder besondere Angaben enthalten);
   b) **IP-Adresse**, nur im Arbeitsspeicher, um einen täglich wechselnden, gesalzenen Hash für Rate-Limits zu bilden; nie im Klartext gespeichert oder protokolliert;
   c) nur bei **Einwilligung** des Besuchers (§ 25 Abs. 1 TDDDG): zufällige Sitzungskennung (128 Bit, im `sessionStorage` des Browsers, max. 7 Tage), serverseitig nur gehasht im Arbeitsspeicher, max. 24 Stunden, zusammen mit letztem Suchbegriff und bis zu 50 angeklickten Produktnummern;
   d) nur bei Einwilligung: Liste von bis zu 20 zuletzt angesehenen Produktnummern (`localStorage` im Browser, max. 30 Tage); sie wird zum Anzeigen an den Server geschickt, dort aber nicht gespeichert;
   e) Klicks auf Ergebnisse (Produktnummer, Position), Gerätetyp grob („mobil"/„Desktop"), Klicks auf Empfehlungen;
   f) gemeldete Bestellungen: nur Produktnummern und Mengen, optional Sitzungskennung;
   g) daraus gebildete **Tageszähler je Shop** (nach Einschätzung der Parteien anonym, siehe Datenkonzept und Anlage 1 Nr. 1).

   Nicht verarbeitet werden: Namen, Anschriften, E-Mail-Adressen, Telefonnummern, Kunden- oder Bestellnummern, Zahlungsdaten. Die Kaufschnittstelle weist solche Felder technisch ab. Besondere Kategorien (Art. 9 DSGVO) werden nicht gezielt verarbeitet; der Verantwortliche ist darauf hingewiesen, dass Besucher solche Angaben in das Suchfeld tippen können. Suchbegriffe, die wie E-Mail-Adresse, Telefon-, Kunden-, Bestell- oder Kontonummer, Web- oder IP-Adresse aussehen, werden beantwortet, aber nicht gespeichert, nicht zwischengespeichert und nicht protokolliert.

5. **Speicherdauer:** siehe Anlage 1 Nr. 6.
6. Die Beschreibung im Einzelnen ergibt sich aus dem Datenkonzept (Stand 30.09.2026, ergänzt um die Wunschliste vom 06.10.2026), das der Auftragsverarbeiter auf Anfrage aushändigt.

§ 3 Ort der Verarbeitung

1. Die Verarbeitung findet in einem Rechenzentrum der Hetzner Online GmbH in **Nürnberg (Deutschland)** statt (gemessen 09.10.2026). Ein Wechsel in ein anderes deutsches Rechenzentrum von Hetzner (z. B. Falkenstein) ist ohne gesonderte Zustimmung zulässig und wird mitgeteilt.
2. Zur Relevanzbewertung werden Suchbegriffe und Produktdaten an TypeSafe AI, Inc. in den **USA** übermittelt (Anlage 2 Nr. 2). Grundlage sind die EU-Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914), Modul 3 (Auftragsverarbeiter an Unterauftragsverarbeiter), die im Data Processing Addendum von TypeSafe vom 24.04.2026 vereinbart sind. TypeSafe ist (Stand 09.10.2026) **nicht** unter dem EU-US Data Privacy Framework zertifiziert. TypeSafe speichert Eingaben auf unsere Anweisung nicht (Zero Data Retention, von TypeSafe am 06.10.2026 bestätigt) und verwendet sie nicht zum Training.
3. Jede weitere Verlagerung in ein Drittland bedarf der vorherigen Information nach § 8 und der Voraussetzungen der Art. 44 ff. DSGVO.

§ 4 Weisungen

1. Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen. Weisungen sind dieser Vertrag, der Hauptvertrag und die Einstellungen, die der Verantwortliche im Kundenbereich vornimmt. Weitere Weisungen erteilt der Verantwortliche in Textform an anfragen@wunschfund.de. Eine Verarbeitung ohne Weisung ist nur zulässig, wenn das Recht der EU oder eines Mitgliedstaats sie verlangt; dann teilt der Auftragsverarbeiter dies vorher mit, soweit das Recht es nicht verbietet.
2. Der Auftragsverarbeiter nutzt **personenbezogene** Daten nicht für eigene Zwecke, nicht für andere Kunden und nicht zum Training von KI-Modellen. Der Verantwortliche weist den Auftragsverarbeiter an, Suchbegriffe, Bewertungen und Ergebnisse, Klicks und Käufe zu anonymisieren bzw. zu aggregieren (nach dem Personenfilter, Anlage 1 Nr. 1). Die so gewonnenen Daten ohne Personenbezug fallen nicht unter diesen Vertrag; der Auftragsverarbeiter darf sie nach § 12 Abs. 3 der AGB, auch shopübergreifend, zur Verbesserung von wunschfund und zum Training und Finetuning eigener KI-Modelle nutzen. Der Unterauftragsverarbeiter nach Anlage 2 Nr. 2 trainiert nicht mit den Eingaben.
3. Hält der Auftragsverarbeiter eine Weisung für datenschutzwidrig, teilt er dies unverzüglich mit und darf die Ausführung bis zur Bestätigung oder Änderung aussetzen.

§ 5 Pflichten des Verantwortlichen

1. Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung und die Wahrung der Betroffenenrechte verantwortlich.
2. Er holt die Einwilligung der Besucher nach § 25 Abs. 1 TDDDG für die Sitzungskennung und die Liste „zuletzt angesehen“ ein (z. B. Cookie-Banner) und schaltet sie nur bei erteilter Einwilligung ein (`wunschfund.consent(true)`), bei Widerruf aus (`wunschfund.consent(false)`). Ohne Aufruf bleiben beide aus.
3. Er informiert die Besucher in seiner Datenschutzerklärung über die Suche, die Einbindung des Auftragsverarbeiters und die Übermittlung von Suchbegriffen an TypeSafe in die USA.
4. Er übermittelt über die Kaufschnittstelle oder den Bestellabgleich nur Produktnummern, Mengen und die Sitzungskennung und hält sein Kunden-Token geheim (nur serverseitig).
5. Er teilt Fehler oder Unregelmäßigkeiten, die er bei der Prüfung der Ergebnisse feststellt, unverzüglich mit.

§ 6 Vertraulichkeit und Personal

1. Der Auftragsverarbeiter setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen. Derzeit hat ausschließlich der Inhaber Zugriff auf die Systeme.

§ 7 Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft die Maßnahmen nach Art. 32 DSGVO gemäß **Anlage 1**. Er darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt; wesentliche Änderungen teilt er mit.

§ 8 Unterauftragsverarbeiter

1. Der Verantwortliche genehmigt die in **Anlage 2** genannten Unterauftragsverarbeiter.

2. Über jede beabsichtigte Änderung (Hinzufügen oder Ersetzen) informiert der Auftragsverarbeiter mindestens **30 Tage** vorher in Textform (E-Mail oder Kundenbereich). Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund binnen **14 Tagen** widersprechen. Wird keine Lösung gefunden, kann jede Partei den Hauptvertrag zum Zeitpunkt der Änderung kündigen; im Voraus gezahlte Entgelte werden anteilig erstattet.
3. Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter vertraglich auf ein gleichwertiges Schutzniveau (Art. 28 Abs. 4 DSGVO) und haftet für sie.
4. Keine Unterauftragsverarbeitung sind Nebenleistungen wie Telekommunikation, Postdienste oder Wartung von Hardware, soweit dabei kein Zugriff auf personenbezogene Daten besteht.

§ 9 Betroffenenrechte, Unterstützung

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei der Erfüllung der Rechte Betroffener (Art. 12 bis 23 DSGVO). Anfragen, die direkt bei ihm eingehen, leitet er unverzüglich weiter.
2. Da keine Kennung dauerhaft gespeichert wird, lassen sich Tageszähler, Zwischenspeicher und Statistik keiner Person zuordnen. Auskunft oder Löschung zu einer einzelnen Person ist dort nicht möglich und nach Art. 11 DSGVO nicht geschuldet; die Daten in Browser-Speichern (Kennung, zuletzt angesehen) kann der Besucher selbst löschen bzw. per Widerruf entfernen.
3. Der Auftragsverarbeiter unterstützt bei Datenschutz-Folgenabschätzung und vorheriger Konsultation (Art. 35, 36 DSGVO), soweit erforderlich. Aufwand über eine Stunde je Jahr kann er nach Aufwand berechnen (100 € netto je Stunde).

§ 10 Meldung von Datenschutzverletzungen

1. Der Auftragsverarbeiter meldet eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens **24 Stunden** nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit bekannt, und liefert fehlende Angaben nach.
2. Er trifft unverzüglich Maßnahmen zur Eindämmung und dokumentiert den Vorfall.
3. Hinweis zur Kette: TypeSafe meldet uns Vorfälle binnen 72 Stunden (DPA 5.2). Wir leiten solche Meldungen unverzüglich nach Eingang weiter; die 24-Stunden-Frist läuft insoweit ab unserer Kenntnis.

§ 11 Löschung und Rückgabe bei Vertragsende

1. **Rückgabe und Löschung.** Nach Ende der Leistung löscht der Auftragsverarbeiter alle personenbezogenen Daten, die er im Auftrag des Verantwortlichen verarbeitet hat, innerhalb von **30 Tagen**, soweit keine gesetzliche Aufbewahrungspflicht besteht. Verlangt der Verantwortliche vor Vertragsende in Textform die Rückgabe statt der Löschung, stellt der Auftragsverarbeiter ihm die noch gespeicherten personenbezogenen Daten in einem gängigen maschinenlesbaren Format bereit (Art. 28 Abs. 3 lit. g DSGVO).
2. Anonyme Daten (insbesondere Tagessummen der Statistik) sind keine personenbezogenen Daten und nicht Gegenstand der Rückgabe. Die Löschung bestätigt der Auftragsverarbeiter auf Anfrage in Textform.

3. Datensicherungen: Daten in Sicherungskopien werden mit Ablauf der Aufbewahrungsfrist der Sicherung gelöscht, spätestens nach 90 Tagen; bis dahin sind sie gesperrt und werden nur zur Wiederherstellung verwendet.
4. Gesetzliche Aufbewahrungspflichten des Auftragsverarbeiters (z. B. Rechnungen) bleiben unberührt; sie betreffen keine Daten aus der Auftragsverarbeitung.

§ 12 Nachweise und Kontrollen

1. Der Auftragsverarbeiter stellt die zum Nachweis nötigen Informationen bereit (insbesondere diese TOM, das Datenkonzept, Testberichte).
2. Er ermöglicht Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer, nach Ankündigung mit mindestens 14 Tagen Vorlauf, grundsätzlich einmal je Kalenderjahr, während der Geschäftszeiten und ohne Störung des Betriebs. Ein Prüfer darf kein Wettbewerber des Auftragsverarbeiters sein.
3. Kosten: Die erste Prüfung im Kalenderjahr ist bis zu einem Aufwand von 4 Stunden kostenfrei; darüber hinaus trägt der Verantwortliche den Aufwand, es sei denn, die Prüfung deckt einen wesentlichen Verstoß auf. (100 € netto je Stunde)

§ 13 Haftung, Schlussbestimmungen

1. Für die Haftung gegenüber Betroffenen gilt Art. 82 DSGVO. Im Innenverhältnis haften die Parteien nach ihrem Verantwortungsanteil; im Übrigen gelten die Haftungsregeln des Hauptvertrags (§ 11 AGB), soweit Art. 82 DSGVO nicht entgegensteht.
2. Bei Widersprüchen geht dieser Vertrag in Datenschutzfragen dem Hauptvertrag vor.
3. Änderungen bedürfen der Textform. Unwirksame Bestimmungen berühren die übrigen nicht.
4. Es gilt deutsches Recht. Gerichtsstand ist, soweit zulässig, Celle.

Ort, Datum, Unterschriften bzw. elektronische Annahme im Bestellvorgang (Version, Zeitpunkt):

Anlage 1: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Stand 09.10.2026. Beschreibt den gemessenen Stand von Software (shopsuche `origin/main` 21854ba) und Server (pbadmin, Hetzner Nürnberg).

1. Datensparsamkeit, Pseudonymisierung, Anonymisierung

- Keine IP-Adresse im Klartext gespeichert oder protokolliert. Rate-Limits über SHA-256(IP + Zufallssalz); das Salz liegt nur im Arbeitsspeicher und wechselt täglich.
- Sitzungskennung nur bei Einwilligung, zufällig (128 Bit), im Browser `sessionStorage` (max. 7 Tage), auf dem Server nur gehasht im Arbeitsspeicher (max. 24 h), nie auf Platte, nie im Log.
- „Zuletzt angesehen“ nur bei Einwilligung, nur im Browser (`localStorage` , max. 20 Nummern, 30 Tage), serverseitig nicht gespeichert.

- Statistik nur als Tageszähler je Shop, keine Einzelereignisse, keine Uhrzeiten; je Zählertabelle höchstens 20.000 Schlüssel pro Tag.
- Personenähnliche Suchbegriffe (E-Mail, ≥ 6 Ziffern, IBAN, Web-/IP-Adresse) werden weder in der Statistik noch im Zwischenspeicher noch im Bremsprotokoll gespeichert (Test `test/pii-speicher.mjs`).
- Kaufschnittstelle nimmt nur Produktnummern, Mengen und Kennung an; Felder mit Personenbezug werden mit Fehler abgewiesen (Test `test/daten.mjs`).
- Auswertungen an den Shop mit Mindestzahl k = 5, auch in Handlungsvorschlägen und CSV-Export; Zeiträume für den Shop nur in festen Längen (7, 14, 30, 90, 365 Tage), damit keine Differenzbildung auf einzelne Tage möglich ist.
- Diensteprotokoll (Systemjournal) ohne IP, ohne Suchbegriff, ohne Kennung (automatischer Test; Stichprobe 09.10.2026 ohne Befund).
- Webserver (Caddy) schreibt für suche.wunschfund.de (Suche, Widget, Schnittstellen) kein Zugriffsprotokoll.

2. Vertraulichkeit: Zutritt, Zugang, Zugriff

- Zutritt: Rechenzentrum Hetzner Online GmbH (Nürnberg), Maßnahmen gemäß Hetzner-AVV Anlage 2 (TOM v1.2 vom 16.02.2026, liegt vor).
- Zugang zum Server: nur SSH mit Schlüssel, Passwort-Anmeldung und Root-Anmeldung abgeschaltet, nicht standardmäßiger Port, Firewall mit Standard „verwerfen“ (offen nur SSH, HTTP/HTTPS, WireGuard), fail2ban aktiv, automatische Sicherheitsupdates aktiv. Interne Verwaltung (CRM) nur über VPN (WireGuard).
- Dienst läuft als eigener Nutzer `wunschfund` ohne Root-Rechte, systemd-Härtung (NoNewPrivileges, ProtectSystem=strict, ProtectHome, PrivateTmp, PrivateDevices, PrivateUsers), schreibt nur nach `/srv/wunschfund` (Rechte 0700), Dateien 0600. Geheimnisse (Schlüssel, Tokens) über systemd-Credentials, nicht im Code.
- Dienst lauscht nur auf 127.0.0.1; Zugriff von außen nur über Caddy mit TLS, HSTS (inkl. Subdomains, preload), Content-Security-Policy.
- Mandantentrennung: eigener Ordner und eigene Dateien je Shop; Zuordnung einer Anfrage nur über den Widget-Schlüssel (Suche) bzw. Kunden-Token oder Anmeldung (Verwaltung). Kunden-Token nur als SHA-256 gespeichert, Vergleich in konstanter Zeit. Tests gegen Datenabfluss zwischen Mandanten (`test/mandanten.mjs` , `test/daten.mjs`).
- Widget im Shop: Shadow DOM, Texte nur über `textContent` , Bilder und Links nur `https` , Bilder ohne Referrer; Einwilligung per `postMessage` nur von der eingetragenen Shop-Herkunft angenommen.
- Je Shop eigener API-Schlüssel beim KI-Dienst (Alex, 09.10.2026), damit Kosten und Sperren getrennt bleiben.

3. Integrität

- Eingabeprüfung mit Feld-Allowlist, Größenlimits (1 KB Klick, 10 KB, 16 KB Kauf), Längenlimits, Rate-Limits je Besucher-Hash und je Shop; atomisches Schreiben (temporäre Datei + Umbenennen).
- Kundenbereich: CSRF-Schutz je Sitzung, gleiche Herkunft für Anmeldung, Rollenprüfung serverseitig (Inhaber/Mitarbeiter), Protokoll der Änderungen.

- Änderungen am Code über Git mit automatischen Tests vor dem Ausrollen, Sicherung vor jedem Ausrollen, Rückweg dokumentiert.

4. Verfügbarkeit und Belastbarkeit

- systemd mit automatischem Neustart; bei Störung des KI-Dienstes automatische Rückfallebene (einfache Suche); ist wunschfund nicht erreichbar, gibt das Widget die eigene Suche des Shops frei.
- Kostendeckel je Shop (Tag/Monat) mit Warnung ab 80 % und Rückfall auf einfache Suche.
- **Datensicherung:** Vor jedem Ausrollen Sicherung auf demselben Server.

5. Verfahren zur regelmäßigen Überprüfung

- Automatische Testsuiten (Sicherheit, Rollen, Mandanten, Datenschicht, Personenfilter, Widget/Consent) vor jedem Ausrollen.
- Interne Überwachung von Kosten und Fehlern mit Alarm an den Inhaber.

6. Löschfristen (automatisch, im Code umgesetzt, sofern nicht anders angegeben)

DATEN	FRIST
Sitzungskennung (Server, gehasht, Arbeitsspeicher)	24 h ohne Aktivität, nach Kaufmeldung, bei Neustart
Rate-Limit-Hashes und Salz	Arbeitsspeicher, Salz täglich neu
Suchergebnis-Zwischenspeicher	28 Tage
Bremsprotokoll (abgewiesene/gedrosselte Suchen)	30 Tage
Tageszähler / Statistik	25 Monate
Nutzung je Tag (Abrechnung, ohne Suchbegriffe)	400 Tage
Kostenbuch je Shop (ohne Suchbegriffe)	400 Tage / 36 Monate
Systemjournal	automatische Kürzung nach Größe
Sicherungen vor dem Ausrollen	90 Tage
Alle Daten bei Vertragsende	30 Tage (§ 11)

Anlage 2: Unterauftragsverarbeiter

#	UNTERNEHMEN	LEISTUNG	DATEN	ORT	GARANTIEN
1	Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland	Server (Hosting) der Suche, des Kundenbereichs und aller Auftragsdaten	alle unter § 2	Rechenzentrum Nürnberg (DE)	AVV mit Hetzner (Art. 28 DSGVO), TOM v1.2 vom 16.02.2026

#	UNTERNEHMEN	LEISTUNG	DATEN	ORT	GARANTIEN
2	TypeSafe AI, Inc., USA	Relevanzbewertung der Suche (System One, Modell „Jev“)	Suchbegriffe, Produktdaten des Shops (Name, Beschreibung, Kategorie, Hersteller, ggf. Preis); keine IP, keine Kennung, keine Kontaktdaten	USA (Hosting bei Amazon Web Services laut Trust Center)	Data Processing Addendum vom 24.04.2026 mit EU-SCC Modul 3 (Recht und Gerichte Irland), Meldung von Vorfällen binnen 72 h, kein Training auf Eingaben (Privacy Policy), Zero Data Retention vereinbart und aktiv; keine DPF-Zertifizierung (Stand 09.10.2026)
2a	Unterauftragsverarbeiter von TypeSafe	laut https://trust.typesafe.ai/subprocessors (u. a. Amazon Web Services; Cloudflare vor `api.typesafe.ai`)	wie Nr. 2	USA / weltweit	über DPA TypeSafe

Nicht eingesetzt: Analyse-, Werbe- oder Tracking-Dienste, Content-Delivery-Netzwerke für Widget oder Suchseite, externe Schriftarten, externe E-Mail-Versender für Besucherdaten. Der E-Mail-Versand (nur Kundenbereich, keine Besucherdaten) erfolgt über einen selbst betriebenen Mailserver.

Diese Seite und das PDF avv-2026-10-30.pdf geben dieselbe Fassung vom 30. Oktober 2026 wieder. Sie können beide speichern oder ausdrucken. Alle Fassungen finden Sie unter wunschfund.de/rechtliches.