# Scodex

# Vereinbarung zur Auftragsverarbeitung

### Version 1.0 vom 15. November 2026

**Hinweise zur Verwendung: Kundenbezogene Felder und die als offen markierten Angaben sind vor Abschluss auszufüllen. Die beschriebenen Maßnahmen beruhen auf Angaben des Auftragnehmers, nicht auf einer technischen Prüfung.**

## Vertragsparteien

Auftragnehmer (Auftragsverarbeiter): Philipp Walter, Scodex, Wilhelm-von-Capitaine Straße 18, 50858 Köln. Kontakt: info@scodex.de, Telefon +49221-99875711. Anschrift und allgemeine Kontaktdaten wurden dem öffentlich abrufbaren Impressum entnommen und sind vor Verwendung zu bestätigen.

Auftraggeber (Verantwortlicher): [Firma/Name, vollständige Anschrift und vertretungsberechtigte Person].

Hauptauftrag/Angebot: [Bezeichnung, Datum, Auftragsnummer]. Beginn: [Datum]. Ende bzw. Beendigungsregel: [Datum oder Laufzeit des Hauptauftrags]. Weisungsberechtigte Person des Auftraggebers: [Name und E-Mail]. Datenschutz-/Vorfallkontakt des Auftraggebers: [Name, E-Mail, Telefon]. Anlaufstelle des Auftragnehmers: Philipp Walter über die vorgenannten Kontaktdaten. Die Benennung als Anlaufstelle ist keine Aussage über die Bestellung oder Erforderlichkeit eines Datenschutzbeauftragten.

## 1. Geltungsbereich und Dauer

Diese Vereinbarung ergänzt den Hauptauftrag, soweit Scodex personenbezogene Daten im Auftrag des Kunden verarbeitet. Sie betrifft Webdesign, WordPress-Entwicklung und -Wartung sowie gesondert beauftragten IT-Support ohne Fernwartung. Nicht jede gestalterische Tätigkeit ist automatisch eine Auftragsverarbeitung; ausschlaggebend ist der tatsächlich vereinbarte Umgang mit personenbezogenen Daten.

Eigenes Hosting, Fernwartung von Kundenendgeräten und KI-Automatisierungen sind nicht Gegenstand dieser Vereinbarung. Eine gesondert beauftragte Administration der Kundenwebsite, beispielsweise über das WordPress-Backend, ist davon zu unterscheiden und in Anlage 1 konkret zu beschreiben. Diese AVV begründet selbst keine Zugriffsberechtigung für Produktivsysteme. Sie erlaubt insbesondere keine Weitergabe von Auftragsdaten an KI-Dienste. Eine Erweiterung der Verarbeitung erfordert eine vorherige dokumentierte Vereinbarung und Prüfung der erforderlichen Schutzmaßnahmen.

Die Verarbeitung beginnt mit dem in Anlage 1 bestimmten Auftrag und endet mit dessen Abschluss einschließlich der vereinbarten Rückgabe und Löschung. Vertraulichkeit und sonstige nachwirkende Pflichten gelten über das Auftragsende hinaus. Für rein eigene Zwecke von Scodex, etwa die gesetzlich erforderliche Rechnungsführung, gilt diese Vereinbarung nicht; diese Verarbeitung ist rechtlich gesondert zu beurteilen.

## 2. Verantwortung, Weisungen und Vertraulichkeit

Der Auftraggeber bestimmt Zwecke und zulässigen Umfang der Verarbeitung, sorgt für deren Rechtsgrundlage und die erforderlichen Informationen an betroffene Personen. Er stellt Scodex nur die für den Auftrag benötigten Daten und Berechtigungen bereit und kontrolliert die Eignung der vereinbarten Maßnahmen.

Scodex verarbeitet Auftragsdaten ausschließlich entsprechend dokumentierten Weisungen. Hauptauftrag, diese Vereinbarung und ausgefüllte Anlagen bilden die anfänglichen Weisungen. Ergänzungen werden in

Textform, beispielsweise per E-Mail, festgehalten. Dringliche mündliche Weisungen sind unverzüglich zu dokumentieren. Weisungen zur Übermittlung in Drittländer unterliegen zusätzlich Abschnitt 5.

Verpflichtet Unionsrecht oder das Recht eines Mitgliedstaats Scodex zu einer abweichenden Verarbeitung, informiert Scodex den Auftraggeber vorher, soweit das betreffende Recht eine Information nicht aus wichtigem öffentlichen Interesse untersagt. Hält Scodex eine Weisung für datenschutzwidrig, informiert Scodex den Auftraggeber unverzüglich und setzt ihre Ausführung bis zur rechtlichen Klärung aus. Eine bloße Bestätigung des Auftraggebers legitimiert keine rechtswidrige Verarbeitung.

Zugang zu Auftragsdaten erhalten nur zur Aufgabenerfüllung befugte Personen. Vor einem solchen Zugang ist deren Verpflichtung zur Vertraulichkeit oder eine angemessene gesetzliche Verschwiegenheitspflicht sicherzustellen. Scodex nutzt Auftragsdaten weder für eigene Werbung noch für eigene Trainings-, Analyse- oder andere vom Auftrag losgelöste Zwecke.

## 3. Sicherheit der Verarbeitung

Scodex trifft die nach Artikel 32 DSGVO erforderlichen, dem Risiko angemessenen technischen und organisatorischen Maßnahmen. Anlage 2 unterscheidet bestätigte Maßnahmen, offene Ausgestaltungen und künftig umzusetzende Vertragspflichten. Offene Punkte sind vor Beginn der betroffenen Verarbeitung zu klären; sie gelten durch die Unterschrift nicht rückwirkend als umgesetzt.

Bei wesentlichen Änderungen der Risiken oder Verarbeitung sind Maßnahmen und Anlagen zu überprüfen. Technische Weiterentwicklungen dürfen das vereinbarte Schutzniveau nicht unterschreiten. Ein für den konkreten Auftrag unzureichendes Schutzniveau ist vor Beginn bzw. Fortsetzung der betroffenen Verarbeitung zu beheben; eine bloße Risikoakzeptanz ersetzt notwendige Maßnahmen nicht.

## 4. Unterstützung, Vorfälle und Kontrolle

Scodex leitet Anfragen betroffener Personen unverzüglich an den Auftraggeber weiter und beantwortet sie inhaltlich nur auf dessen Weisung, soweit keine eigene gesetzliche Pflicht besteht. Unter Berücksichtigung der Art der Verarbeitung unterstützt Scodex mit geeigneten Maßnahmen bei Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und weiteren Betroffenenrechten.

Unter Berücksichtigung der verfügbaren Informationen unterstützt Scodex den Auftraggeber außerdem bei Datensicherheit, Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen nach Artikeln 32 bis 36 DSGVO. Dazu gehören das Auffinden betroffener lokaler Dateien und Sicherungen, die Bereitstellung verfügbarer Verarbeitungsinformationen und die Ausführung dokumentierter Schutz- und Löschweisungen.

Scodex meldet dem Auftraggeber eine bekannt gewordene Verletzung des Schutzes von Auftragsdaten unverzüglich, ohne eine eigene 72-Stunden-Frist auszuschöpfen. Die Meldung enthält, soweit verfügbar, Art und Umfang des Vorfalls, betroffene Daten- und Personenkategorien, ungefähre Zahlen, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Maßnahmen und eine Kontaktstelle. Fehlende Informationen werden ohne unangemessene Verzögerung nachgereicht. Scodex sichert verfügbare Nachweise und unterstützt bei der Eindämmung; gesetzliche Meldepflichten des Auftraggebers bleiben unberührt.

Scodex stellt dem Auftraggeber alle zum Nachweis der Pflichten nach Artikel 28 DSGVO erforderlichen Informationen bereit, ermöglicht Überprüfungen einschließlich Inspektionen durch den Auftraggeber oder dessen beauftragte Prüfer und wirkt daran mit. Prüfungen werden unter Wahrung fremder Daten und berechtigter Geheimhaltungsinteressen organisiert. Soweit der Prüfzweck es zulässt, werden Termin und Ablauf vorab abgestimmt; dringliche Anlassprüfungen und behördliche Befugnisse bleiben unberührt. Eine Zertifizierung wird nicht zugesichert.

## 5. Weitere Auftragsverarbeiter, Kundenhoster und Verarbeitungsorte

Die Beauftragung weiterer Auftragsverarbeiter durch Scodex bedarf der vorherigen gesonderten schriftlichen oder elektronisch dokumentierten Genehmigung des Auftraggebers. Vor einer Genehmigung legt Scodex Identität, Tätigkeit, Verarbeitungsorte und Schutzmaßnahmen offen. Genehmigte Anbieter werden in Anlage 3 erfasst. Dem weiteren Auftragsverarbeiter werden durch einen Vertrag oder ein anderes einschlägiges Rechtsinstrument nach Unionsrecht oder dem Recht eines Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die Scodex in dieser Vereinbarung übernommen hat, insbesondere die Pflicht, hinreichende Garantien für geeignete technische und organisatorische Maßnahmen zu bieten. Scodex bleibt für die Erfüllung der Pflichten des weiteren Auftragsverarbeiters gegenüber dem Auftraggeber verantwortlich.

Ein vom Kunden selbst unmittelbar beauftragter Website-Hoster ist nicht allein deshalb ein Unterauftragsverarbeiter von Scodex, weil Scodex dort Wartungsarbeiten ausführt. Vertrags- und Verantwortungsbeziehungen sowie tatsächliche Datenflüsse sind pro Auftrag festzuhalten. Scodex übernimmt durch diese Vereinbarung weder Hosting noch die Sicherung der beim Kundenhoster betriebenen Website, sofern eine konkrete Sicherungsleistung nicht gesondert vereinbart ist.

Lokale Verarbeitungsorte und gegebenenfalls Zugriffe auf Kundensysteme werden in Anlage 1 festgelegt. Eine Übermittlung in Drittländer oder ein entsprechender Zugriff ist nur auf dokumentierte Weisung und unter Erfüllung von Kapitel V DSGVO zulässig. Eine bloße Weisung oder diese AVV stellt für sich keine ausreichende Drittlandgarantie dar. Nicht geklärte Übermittlungen sind vor ihrer Durchführung zu stoppen und zu prüfen.

## 6. Auftragsende, Rückgabe und Löschung

Nach Abschluss der Verarbeitung gibt Scodex nach Wahl des Auftraggebers die Auftragsdaten zurück oder löscht sie und löscht vorhandene Kopien einschließlich lokaler Sicherungskopien. Eine gewünschte Rückgabe ist mit dem Auftraggeber so abzustimmen, dass keine benötigten Daten vor deren Übergabe vernichtet werden. Ohne Rückgabeweisung ist die Löschung bei Auftragsende vorgesehen.

Die Löschung umfasst insbesondere lokale Projektdateien, Datenbankexporte, Downloads, Sicherungskopien und gespeicherte Kundenzugangsdaten. Auf Wunsch bestätigt Scodex die Durchführung. Als Freigabebedingung sind vor Beginn der betroffenen Verarbeitung Verfahren, Zuständigkeiten und Löschzeitpunkte für sämtliche Kopien einschließlich Sicherungskopien festzulegen und ihre technische Umsetzbarkeit sicherzustellen. Eine ausschließlich zeitversetzte Bereinigung von Sicherungskopien ist bislang nicht vereinbart.

Soweit Unionsrecht oder das Recht eines Mitgliedstaats die Aufbewahrung bestimmter Auftragsdaten zwingend verlangt, werden nur diese Daten für die erforderliche Dauer zweckgebunden aufbewahrt, gegen anderweitige Nutzung geschützt und anschließend gelöscht. Der Auftraggeber wird über Rechtsgrundlage, Umfang und Dauer informiert, soweit rechtlich zulässig. Eigene Rechnungsunterlagen sind von solchen Auftragsdaten zu unterscheiden.

## 7. Abschluss und Änderungen

Diese Vereinbarung einschließlich der ausgefüllten Anlagen wird schriftlich oder in dokumentierter elektronischer Form geschlossen. Der Download einer Vorlage allein bewirkt keinen Vertragsschluss. Eine spätere Veröffentlichung einer neuen Fassung auf der Website ersetzt keine bereits vereinbarte Version. Änderungen bedürfen der Vereinbarung beider Parteien. Bei Widersprüchen zum Hauptauftrag geht diese Vereinbarung hinsichtlich der Auftragsverarbeitung vor; zwingendes Recht bleibt unberührt.

Für den Auftraggeber: [Name/Funktion, Ort, Datum, Unterschrift oder dokumentierte elektronische Annahme].

Für den Auftragnehmer: Philipp Walter, Scodex – [Ort, Datum, Unterschrift oder dokumentierte elektronische Annahme].

# Anlage 1 – Auftragsbezogene Beschreibung

Vor Abschluss je Kundenauftrag ausfüllen. Nur tatsächlich benötigte Kategorien auswählen; Beispiele sind keine pauschale Freigabe.

## A. Auftrag und Verarbeitung

Projekt/Website/System: [Bezeichnung und URL]. Beauftragte Tätigkeiten: [konkrete Webdesign-, WordPress-Entwicklungs-/Wartungs- oder IT-Supportleistungen ohne Fernwartung]. Zeitraum und Zugriffshäufigkeit: [Angaben].

Zweck: [z. B. Umsetzung und Pflege der Kundenwebsite, Fehlerbehebung, Funktionsprüfung]. Vorgänge: [zutreffend auswählen: Einsehen, Empfangen, lokales Speichern, Ordnen, Ändern, Testen, Übertragen, Rückgeben, Löschen]. Lokale Datenkopien sind auf das Erforderliche zu begrenzen. Tests sollen möglichst ohne Echtdaten erfolgen.

## B. Betroffene Personen und Daten

Betroffene Personen: [zutreffend auswählen/ergänzen: Websitebesucher, Interessenten, Kunden, Ansprechpartner, Beschäftigte, registrierte Nutzer].

Datenarten: [zutreffend auswählen/ergänzen: Namen und Kontaktdaten, Inhalte von Kontaktanfragen, Benutzer-/Berechtigungsdaten, veröffentlichte personenbezogene Inhalte, IP-Adressen und technische Protokolldaten]. Datenbankkopien können mehrere Kategorien umfassen und sind vor Übernahme zu prüfen.

Besondere Kategorien nach Artikel 9 DSGVO sowie Daten über strafrechtliche Verurteilungen und Straftaten nach Artikel 10 DSGVO sind in dieser Grundfassung nicht zur Verarbeitung vorgesehen. Sind sie im konkreten Projekt enthalten oder zu erwarten, sind vor Übernahme Umfang, Rechtsgrundlagen und zusätzliche Schutzmaßnahmen gesondert festzulegen.

## C. Systeme, Orte und Übergabe

Lokale Verarbeitungsorte (Ort/Land): [ergänzen]. Geräte/Speicherorte: [ergänzen]. Zugriffsberechtigte Personen: [ergänzen]. Übertragungsweg für Dateien und Zugangsdaten: [ergänzen; Schutzbedarf berücksichtigen].

Kundenseitig beauftragter Hoster/Systemanbieter: [Name, Vertragsrolle, Server-/Zugriffsorte oder nicht zutreffend]. Erlaubte Website-Administrationszugriffe: [Umfang und Zugangsweg]. Keine Fernwartung von Kundenendgeräten.

Rückgabe vor Löschung gewünscht: [ja/nein; Format und Übergabeweg]. Löschverantwortlicher und Nachweis: [ergänzen]. Abweichende zwingende Aufbewahrungspflicht: [konkret oder keine bekannt].

# Anlage 2 – Technische und organisatorische Maßnahmen

## A. Vom Auftragnehmer bestätigter Stand

1. Arbeitsgeräte sind durch Passwortschutz, automatische Bildschirmsperre und Festplattenverschlüsselung geschützt.
2. Zugangsdaten werden mit KeePassXC lokal verwaltet. Nach Angabe des Auftragnehmers wird der Passwortmanager lokal und ohne Cloud-Synchronisation eingesetzt.
3. Geräte und eingesetzte Software werden regelmäßig aktualisiert. Konkrete Patchfristen und Prüfprotokolle sind nicht bestätigt.
4. Kundendaten werden lokal gespeichert. Backups werden nach Angabe des Auftragnehmers lokal auf verschlüsselten Festplatten abgelegt. Eine Cloud-Sicherung wird für diese Backups nicht angegeben. Eine räumlich getrennte oder dauerhaft vom Arbeitsgerät getrennte Aufbewahrung wird damit nicht zugesichert.
5. Lokale Kundendaten sollen bei Auftragsende gelöscht werden. Löschmethoden, Einbeziehung von Sicherungen und Nachweise sind noch zu konkretisieren.
6. Scodex bietet kein eigenes Hosting und keine Fernwartung an. KI-Automatisierungen gehören nicht zum vereinbarten Leistungsumfang.

Diese Bestandsbeschreibung ist keine technische Sicherheitsprüfung und kein Nachweis, dass die Maßnahmen für jeden denkbaren Auftrag ausreichen.

## B. Vor Verwendung zu konkretisieren

Verfügbarkeit: Bestätigt sind lokale Backups auf verschlüsselten Festplatten. Sicherungsfrequenz, Aufbewahrungs- und Anschlusskonzept, Wiederherstellungstests und Wiederherstellungsziele sind noch zu konkretisieren. Die Verschlüsselung allein ist kein Nachweis einer wirksamen Wiederherstellbarkeit. Vor Einsatz ist für den konkreten Auftrag festzulegen und gegebenenfalls umzusetzen, wie erforderliche Verfügbarkeit und Wiederherstellbarkeit gewährleistet werden. Eine räumlich getrennte oder offline aufbewahrte Sicherung und geprüfte Wiederherstellbarkeit werden nicht behauptet.

Berechtigungen: Getrennte Kundenzugänge, Zwei-Faktor-Anmeldung, Rechtebegrenzung und regelmäßige Rechtekontrollen sind bislang nicht bestätigt. Verfügbarkeit und notwendige Umsetzung je Kundensystem sowie Umgang mit nicht unterstützten Schutzfunktionen sind zu dokumentieren.

Weitere Ausgestaltung: Physischer Schutz des Arbeitsplatzes, logische Trennung von Kundenprojekten, sichere Übertragung, Schadsoftware-Schutz, Nachweis der Löschung einschließlich Sicherungskopien, Verfahren für Vorfälle sowie regelmäßige Wirksamkeitskontrollen sind vor Verwendung risikogerecht festzulegen. Sie werden nicht als bereits eingeführte Maßnahmen dargestellt.

## C. Mit Abschluss zu erfüllende organisatorische Pflichten

Nur erforderliche Daten und Rechte verwenden; berechtigte Personen und deren Vertraulichkeitsbindung festhalten; Weisungen nachvollziehbar dokumentieren; Vorfälle unverzüglich an den Kunden melden; Betroffenenanfragen zuordnen und weiterleiten; Rückgabe und Löschung koordinieren; Maßnahmen bei geänderten Risiken und in festzulegenden Abständen auf Wirksamkeit überprüfen. Diese Pflichten sind umzusetzen und nicht durch diese Aufzählung allein erfüllt.

# Anlage 3 – Weitere Auftragsverarbeiter

Status: nicht abschließend erhoben. Es wurden bislang keine konkreten Unterauftragsverarbeiter zur Genehmigung benannt; dies ist keine Bestätigung, dass tatsächlich keine eingesetzt werden. Vor Vertragsabschluss ist diese Anlage zu vervollständigen oder das Ergebnis „keine“ nach Prüfung ausdrücklich zu bestätigen.

KeePassXC wird nach Angabe des Auftragnehmers ausschließlich lokal und ohne Cloud-Synchronisation eingesetzt; hierfür wird kein Cloud-Passwortmanager-Anbieter in die Liste aufgenommen. Zu prüfen bleiben Datenübermittlungen durch gegebenenfalls eingesetzte Support-/Projektwerkzeuge sowie andere von Scodex für Auftragsdaten eingesetzte Dienste. Die eigene Website-Infrastruktur von Scodex wird nicht automatisch als Verarbeitungskette eines Kundenauftrags eingestuft.

Je genehmigtem Anbieter festhalten: [vollständiger Name/Anschrift, konkrete Tätigkeit, betroffene Daten, Verarbeitungs-/Zugriffsorte, gegebenenfalls Drittlandgrundlage, Datum und Nachweis der Kundengenehmigung].

Bestätigtes Ergebnis für diesen Auftrag: [keine / beigefügte konkret ausgefüllte Liste]. Bestätigung durch Scodex und Genehmigung durch den Auftraggeber: [Datum und dokumentierte Erklärung].