

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

Produkt: SubCheck

Stand: September 2026

Vertragsparteien

Auftraggeber (Verantwortlicher im Sinne der DSGVO):

Der jeweilige **Kunde** (in der Regel ein Generalunternehmer bzw. Bauunternehmen), der mit BHO Systems eine **Testvereinbarung**, einen **Hauptvertrag** (Abonnement von SubCheck) oder eine vergleichbare Auftragsbestätigung abschließt.

Firma, Anschrift, Vertretung und E-Mail des Auftraggebers ergeben sich aus der vom Kunden unterzeichneten **Testvereinbarung** bzw. dem **Hauptvertrag** / der Registrierung auf subcheck.online (nicht aus diesem AVV-Dokument).

Auftragsverarbeiter:

BHO Systems UG (haftungsbeschränkt)

Betreiber der Marke / des Produkts **SubCheck**

Registergericht: Amtsgericht Aschaffenburg · HRB 18704

USt-IdNr.: DE465543479

Geschäftsanschrift gemäß aktuellem Impressum unter <https://subcheck.online/impressum>
nachfolgend gemeinsam auch „**Parteien**“ genannt.

Präambel

Der Auftraggeber nutzt die B2B-Software **SubCheck** (<https://subcheck.online>) zur digitalen Verwaltung von Subunternehmer-Nachweisen und zur Unterstützung der Nachunternehmer-Compliance. Dabei verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Auftraggebers. Die Parteien schließen diesen Vertrag zur Regelung der Auftragsverarbeitung gemäß Art. 28 DSGVO.

Es gelten ergänzend die **Allgemeinen Geschäftsbedingungen** des Auftragsverarbeiters (<https://subcheck.online/agb>) sowie die **Datenschutzerklärung** (<https://subcheck.online/datenschutz>), soweit diese nicht diesem AVV widersprechen.

§ 1 Gegenstand und Dauer

(1) Gegenstand ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Auftraggebers im Zusammenhang mit der Nutzung der Plattform **subcheck.online** und des gebuchten SubCheck-Abonnements (einschließlich Testphase). Dazu gehören insbesondere:

- Anlegen und Verwalten von Subunternehmer-Stammdaten
- Anfordern, Empfangen, Speichern und Versionieren von Nachweisen (z. B. § 48b, SOKA-BAU, BG BAU)
- Versand von Upload-Links, Erinnerungen und Statusmitteilungen per E-Mail im Namen des Auftraggebers
- KI-/OCR-Vorprüfung hochgeladener Dokumente mit anschließender manueller Freigabe durch den Auftraggeber
- Dashboard, Archiv, Aktivitäten- und E-Mail-Verlauf sowie Export (CSV/PDF)
- Teamzugänge mit Rollen (Admin, Vollzugriff, Leserecht)

(2) Die Dauer dieses AVV entspricht der Dauer des zugrunde liegenden Hauptvertrags (SaaS-/Abonnementvertrag für SubCheck). Er endet automatisch mit Beendigung des Hauptvertrags, vorbehaltlich gesetzlicher Aufbewahrungspflichten und der in § 10 geregelten Rückgabe/Löschung.

§ 2 Art und Zweck der Verarbeitung

(1) **Art der Verarbeitung:** Erheben, Speichern, Organisieren, Abfragen, Übermitteln, Auslesen (einschließlich OCR), Löschen und sonstige Verarbeitung im Rahmen des SaaS-Betriebs.

(2) **Zweck der Verarbeitung:**

- Bereitstellung und Betrieb von SubCheck
- Authentifizierung und Mandanten-/Teamverwaltung
- Speicherung und Verarbeitung vom Auftraggeber bzw. dessen Subunternehmern eingegebener Compliance- und Nachweisdaten
- Versand transaktionaler E-Mails (Anforderungen, Erinnerungen, Freigabe-/Ablehnungshinweise) über den technischen Absender von SubCheck mit Anzeigenname und Reply-To des Auftraggebers
- Support, Fehleranalyse und IT-Sicherheit

(3) Der Auftragsverarbeiter verarbeitet Daten **nur auf dokumentierte Weisung** des Auftraggebers, es sei denn, eine Verarbeitung ist nach Unionsrecht oder dem Recht der Mitgliedstaaten vorgeschrieben (Art. 28 Abs. 3 lit. a DSGVO). Weisungen ergeben sich insbesondere aus der Nutzung der Plattform (z. B. Anlegen von Subunternehmern, Versand von Upload-Links, Freigabe oder Ablehnung von Dokumenten).

§ 3 Kategorien betroffener Personen und Datenarten

Kategorien betroffener Personen	Kategorien personenbezogener Daten
Mitarbeiter und Beauftragte des Auftraggebers	Name, E-Mail, Rolle/Berechtigung (Admin, Vollzugriff, Leserecht), Nutzungs- und Protokolldaten
Subunternehmer / Nachunternehmer und deren Ansprechpartner	Firmenname, Kontaktdaten (z. B. Name, E-Mail), optionale Projekt-/Baustellenbezüge
Ggf. weitere in Nachweisen erkennbare Personen	Inhalte und Metadaten hochgeladener Dokumente (z. B. Freistellungsbescheinigungen, Sozialkassen- und BG-Nachweise), OCR-Auszüge, Prüfstatus, Versionen, E-Mail-Verlauf

Der Auftraggeber ist dafür verantwortlich, dass die Verarbeitung dieser Daten eine Rechtsgrundlage hat und betroffene Personen informiert werden, soweit erforderlich.

§ 4 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich insbesondere:

1. personenbezogene Daten nur im Rahmen der Weisungen und dieses AVV zu verarbeiten;
2. sicherzustellen, dass zur Verarbeitung befugte Personen Vertraulichkeit zugesichert haben;
3. geeignete technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO umzusetzen (siehe Anlage 1);
4. den Auftraggeber bei der Erfüllung von Betroffenenrechten nach Möglichkeit zu unterstützen (Art. 28 Abs. 3 lit. e DSGVO);
5. Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Kenntnis zu melden (Art. 33, 34 DSGVO);
6. dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung von Art. 28 DSGVO bereitzustellen und Audits zu ermöglichen, soweit zumutbar;
7. Unterauftragsverarbeiter nur gemäß § 5 einzusetzen.

§ 5 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt eine **allgemeine schriftliche Genehmigung** zum Einsatz von Unterauftragsverarbeitern.

(2) Aktuell eingesetzte Kategorien von Unterauftragsverarbeitern für SubCheck:

Kategorie	Zweck	Standort	Standard-DPA (Art. 28)
Hosting / Cloud-Infrastruktur (Vercel)	Betrieb der Webanwendung	EU (Irland)	vercel.com/legal/dpa
Datenbank, Authentifizierung und Dateispeicher (Supabase)	Mandantendaten, Login, Nachweisdateien	Deutschland (EU)	supabase.com/legal/.../data-processing-addendum
E-Mail-Dienst (Resend)	Transaktionale E-Mails (Anforderungen, Erinnerungen)	EU / EWR	resend.com/legal/dpa
Zahlungsdienst (Stripe)	Abonnement und Abrechnung	EU / EWR	stripe.com/legal/dpa
Automatisierung und OCR (n8n)	Workflow-Automatisierung und Vorprüfung hochgeladener Nachweise	Deutschland / EU	n8n.io/legal/data-processing-agreement

(2a) Die Verarbeitung personenbezogener Daten erfolgt **innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums**. Soweit ein Unterauftragsverarbeiter gleichwohl eine Übermittlung in Drittländer ermöglicht, erfolgt diese nur, sofern geeignete Garantien (insbesondere EU-Standardvertragsklauseln) im jeweiligen Standard-DPA vorliegen.

(3) Der Auftragsverarbeiter informiert den Auftraggeber über **wesentliche Änderungen** der Liste (neue Unterauftragsverarbeiter oder Ersatz). Der Auftraggeber kann innerhalb von **30 Tagen** widersprechen. Bei berechtigtem Widerspruch bemühen sich die Parteien um eine einvernehmliche Lösung.

(4) Mit den Unterauftragsverarbeitern bestehen Verträge gemäß Art. 28 DSGVO in Form der **öffentlich hinterlegten Standard-DPAs** der jeweiligen Anbieter. Diese DPAs sind Bestandteil der Nutzungsbedingungen des Dienstleisters und gelten mit Nutzung des Dienstes — **ohne gesonderte Annahme und ohne individuellen Vertrag** zwischen BHO Systems und dem jeweiligen Anbieter. Die jeweils aktuelle Fassung ist über die Links in der Tabelle sowie in der Datenschutzerklärung (<https://subcheck.online/datenschutz>) einsehbar.

§ 6 Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher und stellt die Rechtmäßigkeit der Datenverarbeitung, einschließlich Weisungen an den Auftragsverarbeiter, sicher.

(2) Der Auftraggeber informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Rechtsverstöße bei der Verarbeitung feststellt.

(3) Der Auftraggeber sichert Zugangsdaten und sorgt für berechtigte Nutzung durch seine Mitarbeiter (einschließlich der Vergabe von Teamrollen).

§ 7 Weisungsrecht

(1) Weisungen erfolgen in Textform (E-Mail an info@subcheck.online oder info@bho-systems.de genügt) oder durch Nutzung der vorgesehenen Funktionen in SubCheck.

(2) Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies dem Auftraggeber unverzüglich mit.

§ 8 Kontrollrechte

(1) Der Auftraggeber kann nach vorheriger Ankündigung in angemessenem Umfang Nachweise über die Einhaltung dieses AVV anfordern (z. B. TOM-Beschreibung, Unterauftragsverarbeiterliste).

(2) Vor-Ort-Inspektionen sind nach Abstimmung zu üblichen Geschäftszeiten möglich, höchstens einmal jährlich, sofern nicht Anlass aus einem Datenschutzvorfall besteht. Der Auftraggeber trägt eigene Kosten; übermäßige Kosten des Auftragsverarbeiters können dem Auftraggeber in Rechnung gestellt werden.

§ 9 Geheimhaltung

Die Parteien und ihre Mitarbeiter behandeln alle im Rahmen der Zusammenarbeit bekannt gewordenen vertraulichen Informationen und personenbezogenen Daten vertraulich.

§ 10 Rückgabe und Löschung nach Vertragsende

(1) Nach Beendigung des Hauptvertrags löscht der Auftragsverarbeiter die im Auftrag verarbeiteten personenbezogenen Daten innerhalb von **90 Tagen**, sofern keine gesetzliche Aufbewahrungspflicht

entgegensteht.

(2) Auf Wunsch des Auftraggebers stellt der Auftragsverarbeiter vor Löschung einen **Export** in einem gängigen Format bereit (CSV und/oder PDF, soweit in SubCheck vorgesehen).

(3) Dokumentationspflichten nach DSGVO und gesetzliche Aufbewahrungsfristen bleiben unberührt.

§ 11 Haftung

Die Haftung der Parteien richtet sich nach dem Hauptvertrag (AGB von SubCheck) und den gesetzlichen Vorschriften. Soweit der Auftragsverarbeiter gegen diesen AVV verstößt, haftet er gegenüber dem Auftraggeber nach den gesetzlichen Bestimmungen.

§ 12 Schlussbestimmungen

(1) Änderungen dieses AVV bedürfen der Textform.

(2) Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

(3) Es gilt deutsches Recht.

(4) Der **Auftragsverarbeiter** nimmt diesen AVV bereits mit **Bereitstellung** in der jeweils aktuellen Fassung an. Eine **gesonderte Unterschrift von BHO Systems** ist **nicht erforderlich**.

(5) Der AVV kommt mit dem Auftraggeber zustande, sobald dieser den AVV **unterschreibt** oder durch **Unterzeichnung der Testvereinbarung bzw. des Hauptvertrags** (einschließlich Abschluss eines SubCheck-Abonnements) dem beigefügten AVV **zustimmt**. In letzterem Fall ist **keine separate Unterschrift auf diesem AVV-Dokument** erforderlich.

Unterschrift Auftraggeber (optional)

Der Auftragsverarbeiter hat diesen AVV bereits angenommen (§ 12 Abs. 4).

Nur wenn Sie den AVV nicht bereits über die Testvereinbarung oder den Hauptvertrag angenommen haben, unterschreibt der Auftraggeber hier:

Ort, Datum: _____

Auftraggeber

(Firma / Vertretungsberechtigter)

Anlage 1 – Technische und organisatorische Maßnahmen (TOM)

Der Auftragsverarbeiter setzt unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art der Verarbeitung insbesondere folgende Maßnahmen um:

Zutritts- und Zugangskontrolle

- Hosting in professionellen Rechenzentren mit physischer Zugangskontrolle
- Zugriff auf Produktionssysteme nur für autorisierte Administratoren

Zugriffskontrolle

- Mandantentrennung in der Anwendung (Daten einer Kundenfirma sind von anderen Firmen getrennt)
- Rollenbasierte Berechtigungen in SubCheck (Admin, Vollzugriff, Leserecht)
- Authentifizierung über Supabase Auth, sichere Session-Verwaltung

Weitergabekontrolle

- Verschlüsselte Übertragung (TLS/HTTPS)
- E-Mail-Versand über den Dienstleister Resend
- Upload-Links ohne eigenes Subunternehmer-Konto, zeitlich bzw. vorgangbezogen begrenzt

Eingabekontrolle

- Protokollierung sicherheitsrelevanter und fachlicher Ereignisse (Uploads, Freigaben, Anforderungen, Erinnerungen)
- Nachvollziehbarkeit über Aktivitäten-Feed und E-Mail-Verlauf, soweit in SubCheck vorgesehen

Verfügbarkeits- und Belastbarkeitskontrolle

- Regelmäßige Backups der Datenbank
- Monitoring und Fehlerbehandlung

Verfahren zur regelmäßigen Überprüfung

- Aktualisierung von Abhängigkeiten und Sicherheitspatches nach Möglichkeit zeitnah
- Anpassung der TOM bei wesentlichen Änderungen der Verarbeitung

Detaillierte Angaben können auf Anfrage aktualisiert werden.

Anlage 2 – Weisungskontakt

Rolle	Kontakt
Auftraggeber (Weisungen)	Ansprechpartner gemäß Testvereinbarung, Hauptvertrag bzw. SubCheck-Konto
Auftragsverarbeiter	info@subcheck.online / info@bho-systems.de