v1.0.0

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

zwischen

Neext.code UG (haftungsbeschränkt)
Rötlensweg 1
71522 Backnang
Deutschland
E-Mail: contact@neextcode.com

– nachfolgend „Auftragsverarbeiter“ –

und

dem jeweiligen Kunden als Verantwortlichem

– nachfolgend „Verantwortlicher“ –

wird folgender Vertrag geschlossen:

———

1. Gegenstand und Dauer der Verarbeitung

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Zusammenhang mit der Bereitstellung und Nutzung der Software SchichtEasy.
2. Gegenstand der Verarbeitung ist die technische Bereitstellung einer webbasierten Anwendung zur Schichtplanung, Nutzerverwaltung, Mitarbeiterorganisation, Kommunikation und – soweit aktiviert – zur Nutzung optionaler KI-Funktionen.
3. Die Verarbeitung erfolgt für die Dauer des zugrunde liegenden Nutzungsverhältnisses sowie darüber hinaus nur insoweit, wie gesetzliche Aufbewahrungspflichten, berechtigte Nachweisinteressen oder technische Löschzyklen dies erfordern.
4. Weisungen des Verantwortlichen ergeben sich insbesondere aus der Nutzung der Plattform, den dort vorgenommenen Einstellungen sowie aus ergänzenden Weisungen in Textform.

———

2. Art und Zweck der Verarbeitung

1. Die Verarbeitung personenbezogener Daten erfolgt ausschließlich zur Erbringung der vom Verantwortlichen beauftragten Leistungen, insbesondere zur:
    * Verwaltung von Nutzerkonten und Rollen,
    * Organisation von Workspaces,
    * Verwaltung von Beschäftigten und sonstigen zugeordneten Personen,
    * Schicht-, Einsatz-, Zeit- und Planungsverwaltung,
    * Speicherung, Strukturierung, Anzeige und Übermittlung von Daten,
    * Kommunikation per E-Mail,
    * Verarbeitung von Kontakt-, Support-, Projekt- und sonstiger Kommunikation, soweit diese dem Verantwortlichen zuzurechnen ist,
    * Nutzung optionaler KI-Funktionen auf Veranlassung des Verantwortlichen,
    * Sicherstellung von Betrieb, Verfügbarkeit, Integrität und Sicherheit der Plattform.
2. Zusätzlich umfasst die Verarbeitung den Betrieb einer zentralen technischen Verarbeitungs- und Verwaltungsstelle mit der Bezeichnung NeextLink, soweit der Verantwortliche entsprechende Funktionen nutzt oder entsprechende Daten über die Plattform verarbeitet werden.
3. Hierzu gehört insbesondere die Verarbeitung von:
    * eingehenden und ausgehenden E-Mails,

* Kontakt-, Support-, Projekt- und sonstiger Kommunikation,
* Kommunikationsinhalten und Anhängen,
* Zustell-, Routing-, Bearbeitungs- und Metadaten,
* technischen Status-, Diagnose- und Systemdaten,
* Protokoll-, Fehler- und Sicherheitsdaten der Anwendung, Website und sonstiger verbundener Systeme.

4. Die Verarbeitung dient insbesondere:
* der Entgegennahme, Kategorisierung, Weiterleitung, Bearbeitung, Beantwortung und Dokumentation von Kommunikation,
* der technischen Zustellung und Steuerung von E-Mails,
* der Überwachung und Analyse des Systembetriebs,
* der Erkennung, Analyse und Behebung von Störungen, Softwarefehlern und Sicherheitsproblemen,
* der Sicherstellung von Betrieb, Integrität, Verfügbarkeit und Sicherheit der Plattform.

5. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten zu einer Verarbeitung verpflichtet ist.
6. Die Nutzung optionaler KI-Funktionen erfolgt nur, wenn der Verantwortliche oder von ihm autorisierte Nutzer diese Funktion tatsächlich verwenden.
7. Soweit der Verantwortliche KI-gestützte Funktionen nutzt oder entsprechende Prozesse aktiviert sind, umfasst die Verarbeitung auch die Analyse, Strukturierung, Zusammenfassung, Priorisierung oder sprachliche Aufbereitung von Kommunikationsinhalten, technischen Daten und Protokolldaten.
8. Technische Protokoll-, Fehler- und Statusdaten werden grundsätzlich für bis zu 30 Tage gespeichert und anschließend gelöscht, sofern nicht im Einzelfall eine längere Aufbewahrung zur Aufklärung konkreter Störungen, Sicherheitsvorfälle oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.
9. Der Verantwortliche stellt sicher, dass über die Plattform und insbesondere über optionale KI-Funktionen keine unzulässigen Inhalte oder Daten ohne erforderliche Rechtsgrundlage verarbeitet werden.

———

3. Kategorien personenbezogener Daten

Je nach Nutzung durch den Verantwortlichen können insbesondere folgende Kategorien personenbezogener Daten Gegenstand der Verarbeitung sein:

* Stammdaten,
* Kontaktdaten,
* Nutzer- und Rollendaten,
* Beschäftigten- und Organisationsdaten,
* Arbeitszeit-, Einsatz-, Schicht- und Planungsdaten,
* Verfügbarkeits- und Abwesenheitsdaten,
* vergütungsbezogene oder sonstige betriebliche Personaldaten,
* Login-, Protokoll- und Nutzungsdaten,
* Kommunikationsdaten,
* E-Mail-Inhalte, Kommunikations- und Supportdaten,
* Projektkommunikation und Anhänge,
* Header-, Versand-, Routing- und Zustelldaten,
* technische Status-, Diagnose- und Systemdaten,
* Protokoll-, Fehler- und Sicherheitsdaten,
* System- und Nutzungsmetadaten,
* nutzerinitiierte Eingaben im Rahmen optionaler KI-Funktionen.

Soweit besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO verarbeitet werden, erfolgt dies ausschließlich auf Veranlassung und in Verantwortung des Verantwortlichen.

———

4. Kategorien betroffener Personen

Von der Verarbeitung können insbesondere folgende Personengruppen betroffen sein:

* Mitarbeiter und sonstige Beschäftigte des Verantwortlichen,
* Nutzer und Administratoren,
* eingeladene Personen,
* Ansprechpartner des Verantwortlichen,
* Kunden, Interessenten oder sonstige Dritte, soweit deren Kommunikationsdaten durch den Verantwortlichen in SchichtEasy verarbeitet werden,
* sonstige Personen, deren Daten der Verantwortliche im Rahmen der Nutzung eingibt.

———

5. Verantwortlichkeit und Abgrenzung

1. Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten verantwortlich. Er stellt insbesondere sicher, dass die Voraussetzungen der Art. 6 und – soweit einschlägig – Art. 9 DSGVO erfüllt sind.
2. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur im Rahmen dieses Vertrags und der Weisungen des Verantwortlichen.
3. Soweit der Auftragsverarbeiter personenbezogene Daten zur Vertragsanbahnung, Vertragsdurchführung, Abrechnung, IT-Sicherheit, Support, Missbrauchsverhinderung oder zur Erfüllung gesetzlicher Pflichten verarbeitet, erfolgt dies in eigener datenschutzrechtlicher Verantwortlichkeit und nicht als Auftragsverarbeitung.
4. Zahlungsdienstleister und Zahlungsinfrastrukturanbieter wie Stripe werden zur Zahlungsabwicklung, Abrechnung, Rechnungsstellung, Verwaltung von Abonnements, Kündigungsabwicklung, Rückerstattung, Betrugsprävention, Streitfallbearbeitung und zur Erfüllung gesetzlicher Pflichten eingesetzt.
5. Soweit Stripe oder andere Zahlungsdienstleister personenbezogene Daten zu eigenen Zwecken verarbeiten, insbesondere zur Durchführung und Absicherung von Zahlungen, zur Betrugsprävention, zur Einhaltung gesetzlicher Pflichten, zur Durchsetzung eigener Rechte oder zur Bereitstellung eigener Zahlungsdienste, handeln diese insoweit als eigenständige Verantwortliche.
6. Soweit Stripe oder andere Zahlungsdienstleister personenbezogene Daten ausschließlich auf Weisung des Auftragsverarbeiters verarbeiten, erfolgt dies auf Grundlage der jeweils anwendbaren datenschutzrechtlichen Vereinbarungen mit dem jeweiligen Anbieter.

———

6. Pflichten des Verantwortlichen

Der Verantwortliche ist insbesondere verpflichtet,

1. personenbezogene Daten nur rechtmäßig verarbeiten zu lassen,
2. betroffene Personen ordnungsgemäß zu informieren, soweit ihn entsprechende Pflichten treffen,
3. erforderliche Einwilligungen oder sonstige Rechtsgrundlagen sicherzustellen,
4. Weisungen rechtzeitig, vollständig und rechtmäßig zu erteilen,
5. keine unzulässigen oder nicht erforderlichen sensiblen Daten einzugeben oder eingeben zu lassen,
6. die datenschutzkonforme Nutzung von Einladungs-, Kommunikations-, Log- und KI-Funktionen sicherzustellen.

———

7. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter ist verpflichtet,

1. personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen zu verarbeiten,
2. alle zur Verarbeitung befugten Personen auf Vertraulichkeit zu verpflichten,
3. den Verantwortlichen unverzüglich zu informieren, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt,
4. den Verantwortlichen bei der Wahrung von Betroffenenrechten im angemessenen Umfang zu unterstützen,
5. den Verantwortlichen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO im angemessenen Umfang zu unterstützen,
6. Verletzungen des Schutzes personenbezogener Daten unverzüglich mitzuteilen, soweit sie den Verantwortlichen betreffen,
7. nachzuweisen, dass die gesetzlichen Anforderungen an Auftragsverarbeiter eingehalten werden.

———

8. Technische und organisatorische Maßnahmen (TOMs)

1. Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
2. Hierzu gehören insbesondere:
   * Zugriffsschutz durch Authentifizierungsverfahren,
   * rollenbasierte Berechtigungssteuerung,
   * Verschlüsselung der Datenübertragung nach dem Stand der Technik,
   * Absicherung von Systemen gegen unbefugte Zugriffe,
   * Protokollierung sicherheitsrelevanter Ereignisse,
   * Maßnahmen zur Erkennung und Analyse unbefugter Zugriffe,
   * Datensicherungen und Wiederherstellungsverfahren,
   * logische Mandantentrennung,
   * Maßnahmen zur Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme,
   * Dokumentation rechtlich relevanter Zustimmungen und Versionsstände.
3. Soweit global verteilte Infrastrukturkomponenten, Netzwerkdienste, Sicherheitsdienste oder Edge-Infrastrukturen genutzt werden, stellt der Auftragsverarbeiter sicher, dass der Zugriff auf personenbezogene Daten auf das technisch erforderliche Maß beschränkt bleibt und geeignete datenschutzrechtliche Garantien bestehen.
4. Der Auftragsverarbeiter ist berechtigt, die TOMs weiterzuentwickeln, solange das Schutzniveau nicht abgesenkt wird.

———

9. Subauftragsverhältnisse

1. Der Verantwortliche erteilt seine allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern im Sinne dieses Vertrags.
2. Der Auftragsverarbeiter setzt zur Leistungserbringung insbesondere folgende Kategorien bzw. konkrete Anbieter ein:
   * Supabase für Datenbank- und Authentifizierungsfunktionen,
   * AWS, insbesondere AWS SES, Amazon SQS und Amazon S3,
   * Vercel für Hosting und Deployment,
   * OpenAI für optionale KI-Funktionen,
   * Hetzner für Infrastrukturleistungen,
   * Stripe für Zahlungsabwicklung, Abrechnung, Rechnungsstellung, Verwaltung von Abonnements, Rückerstattungen, Streitfallbearbeitung und zahlungsbezogene Sicherheits- und Betrugspräventionsmaßnahmen.
3. Im Zusammenhang mit NeextLink und der Verarbeitung von Kommunikations-, technischen und Protokolldaten setzt der Auftragsverarbeiter insbesondere AWS, Supabase und Hetzner ein.
4. Mit Supabase, AWS, Vercel, Hetzner, OpenAI und Stripe bestehen, soweit diese als Unterauftragsverarbeiter bzw. Auftragsverarbeiter tätig werden, Auftragsverarbeitungsverträge, Data Processing Addenda oder vergleichbare datenschutzrechtliche Vereinbarungen.

5. Zahlungsdienstleister wie Stripe handeln nicht in jedem Verarbeitungskontext als Unterauftragsverarbeiter. Soweit Stripe personenbezogene Daten zu eigenen Zwecken verarbeitet, insbesondere im Zusammenhang mit Zahlungsabwicklung, Betrugsprävention, regulatorischen Pflichten, Risikoprüfung, Streitfallbearbeitung, Rückerstattungen oder der Bereitstellung eigener Zahlungsdienste, handelt Stripe insoweit als eigenständiger Verantwortlicher.
6. Der Auftragsverarbeiter schließt mit Unterauftragsverarbeitern die erforderlichen Vereinbarungen gemäß Art. 28 DSGVO ab, soweit der jeweilige Anbieter als Auftragsverarbeiter eingesetzt wird.
7. Der Auftragsverarbeiter informiert den Verantwortlichen über wesentliche Änderungen bei eingesetzten Unterauftragsverarbeitern in angemessener Form.

———

10. Datenübermittlung in Drittländer

1. Die Verarbeitung personenbezogener Daten erfolgt überwiegend innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums.
2. Soweit Unterauftragsverarbeiter oder sonstige technische Leistungen zu einer Übermittlung personenbezogener Daten in Drittländer führen, stellt der Auftragsverarbeiter sicher, dass die Anforderungen der Art. 44 ff. DSGVO eingehalten werden.
3. Hierzu können insbesondere Angemessenheitsbeschlüsse, Standardvertragsklauseln oder sonstige gesetzlich zulässige Garantien eingesetzt werden.
4. Auf Anfrage stellt der Auftragsverarbeiter dem Verantwortlichen Informationen über die maßgeblichen Transfergrundlagen zur Verfügung, soweit dies rechtlich und vertraglich zulässig ist.

———

11. Unterstützungspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des Zumutbaren bei:

* Anfragen betroffener Personen,
* Meldungen und Bewertungen von Datenschutzverletzungen,
* Datenschutz-Folgenabschätzungen,
* Konsultationen mit Aufsichtsbehörden,
* Nachweisen über technische und organisatorische Maßnahmen.

———

12. Löschung und Rückgabe von Daten

1. Nach Beendigung des Nutzungsverhältnisses löscht der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen oder gibt diese auf Weisung zurück, sofern keine gesetzlichen Aufbewahrungspflichten, berechtigten Nachweisinteressen oder technischen Gründe für eine zeitlich verzögerte Löschung entgegenstehen.
2. Daten in Backups, Logsystemen oder Replikationssystemen können technisch bedingt erst zeitversetzt gelöscht werden.
3. Der Verantwortliche ist dafür verantwortlich, benötigte Daten rechtzeitig vor Beendigung des Nutzungsverhältnisses zu exportieren oder anderweitig zu sichern.

———

13. Kontrollrechte und Nachweise

1. Der Verantwortliche ist berechtigt, die Einhaltung der datenschutzrechtlichen Verpflichtungen in angemessenem Umfang zu überprüfen.
2. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zum Nachweis der Einhaltung seiner Pflichten zur Verfügung.

3. Audits sind mit angemessener Vorankündigung, unter Wahrung von Betriebs- und Geschäftsgeheimnissen sowie ohne unangemessene Beeinträchtigung des Geschäftsbetriebs durchzuführen.

———

14. Haftung

Die Haftung der Parteien richtet sich nach den gesetzlichen Vorschriften, insbesondere der DSGVO.

———

15. Schlussbestimmungen

1. Änderungen und Ergänzungen dieses Vertrags bedürfen mindestens der Textform.
2. Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
3. Soweit dieser Vertrag keine abweichenden Regelungen enthält, gelten ergänzend die vertraglichen Vereinbarungen zwischen den Parteien.