

Ergänzender Vertrag über die Auftragsverarbeitung

zwischen

im weiteren Verlauf **Auftraggeber** genannt

vertreten durch

und

OKIT GmbH
Weidenstraße 4a
45549 Sprockhövel

im weiteren Verlauf die **OKIT** genannt

vertreten durch

Olaf Krause

Stand: 4. März 2013
Revision: 11. Juli 2013
Revision: 4. Juli 2018
Revision: 17. Juli 2018
Revision: 20. Dezember 2018

1 Allgemeines zum Auftrag

1.1 Präambel

Die von der OKIT betriebenen Applikationen haben in der Regel Kooperation zum Zweck. Es liegt in der Verantwortung des Auftraggebers die an dem System teilnehmenden Personen darauf hinzuweisen, dass über die Applikationen auch mit anderen, nicht am Unternehmen des Auftraggebers beschäftigten Personenkreisen Daten und Informationen ausgetauscht werden können. Zu diesem Zweck sind die am System teilnehmenden Personen auch von anderen Personen identifizierbar, wenn nicht ausdrücklich etwas anderes vereinbart und konfiguriert ist. Die von den teilnehmenden Personen geschaffenen Artefakte und Vermerke zu deren Urheberschaft verbleiben auch über das Ausscheiden der jeweiligen Person hinaus in den einzelnen Applikationen verfügbar.

1.2 Einleitung, Geltungsbereich, Definitionen

1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
2. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter der OKIT personenbezogene Daten des Auftraggebers verarbeiten.
3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. In diesem Sinne ist der Auftraggeber der „Verantwortliche“, die OKIT der „Auftragsverarbeiter“. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der OKIT übernimmt folgende Verarbeitungen:

- Authentifizierung und Autorisierung
- Dokumentenspeicherung und Verwaltung
- Kalenderverwaltung
- E-Mail-Versand
- Tabellenkalkulationen
- Kundeninformations-Daten (CRM)
- Präsentationen

- Aufgaben- und Projektmanagement
- Wissensmanagement-Systeme
- Austausch von Dokumenten, Inhalten und Informationen mit bestimmten Empfängern oder Veröffentlichung von Inhalten und Webseiten, Formularen oder sonstiger Inhalte und Informationen
- Chats und Teilnahme an Audio- und Videokonferenzen
- Empfang und Verarbeitung von automatisch erfassten Daten
- Visualisierung und Datenexploration

Die Liste der angebotenen Verarbeitungen kann ergänzt oder auftraggeberspezifisch angepasst werden.

Im Rahmen der Nutzung öffentlich zugänglicher Dokumente, Webseiten oder sonstige Inhalte, kann OKIT Cookies auf den Rechner der Nutzer für Zwecke der Webanalyse oder um sich Einstellungen der Nutzer zu merken, speichern.

Wir nutzen die Dienste auf Grundlage unserer berechtigten Interessen gem. Art. 6 Abs. 1 lit. f DSGVO an effizienten und sicheren Verwaltungs- und Zusammenarbeitsprozessen.

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Dienstleistungsvertrag zur Nutzung der AgileAS-Plattform (im Folgenden „Hauptvertrag“).

2.2 Dauer

Die Verarbeitung beginnt jeweils am Tag, an dem ein Account angelegt wird, an dem der Hauptvertrag beginnt oder ab dem die Daten zur Verarbeitung bereit gestellt werden, je nach dem, welches dieser Ereignisse das früheste ist.

Die Verarbeitung erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

3 Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung

3.1 Art und Zweck der Verarbeitung AgileAS-Accounting

Die Verarbeitung der Daten dient vorwiegend der Authentifizierung und Autorisierung der einzelnen Anwender auf der Plattform, sowie der Bereitstellung kollaborativer Applikationen. Dazu werden strukturierte Daten erhoben. Das Erheben und die Pflege dieser Daten betreibt der Auftraggeber in Eigenregie. Der OKIT kann hierbei auf Anforderung des Auftraggebers unterstützen. Der OKIT kann hierbei unaufgefordert administrativ unterstützen, wenn dies offensichtlich im Sinne und Interesse des OKITs geschieht.

3.2 Art und Zweck der Verarbeitung AgileAS-Applikationen

Bei den einzelnen auf AgileAS angebotenen Applikationen liegt eine Verarbeitung

strukturierter und unstrukturierter Informationen vor. Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten.

Die Verarbeitung der Daten dient dem individuellen Zweck, den der Auftraggeber festlegt. Typische Verwendungen sind:

- Erfassen, organisieren und Abfragen unstrukturierter Daten in einem Wissenmanagement-System oder einer Datenablage. Dokumentieren von Veränderungen über die Zeit.
- Erfassen, organisieren und verändern von Aufgaben (Projektmanagement).
- Kommunikation mit Mitarbeitern des OKITs und Kommunikation mit externen Personen.
- Bereitstellung und kollaborative Bearbeitung von Daten für interne Zwecke bei Auftrag-nehmer.
- Bereitstellung und kollaborative Bearbeitung von Daten zusammen mit externen Personen.

3.3 Art der Daten

Es werden folgende strukturierte Daten verarbeitet:

- Name, Vorname, Anrede
- Adressen, E-Mail-Adressen, Telefonnummern, Fax-Nummern, Messenger-Adressen
- Eindeutige Logins
- Vom Anwender vergebene Passworte in einer nicht in den Klartext zurückführbaren Form

Es können zum Zweck der Absicherung des Betriebes der Dienstleistungen folgende strukturierte Daten verarbeitet werden:

- Zeitpunkt und Metadaten bei der Anmeldung/Abmeldung und Anwendung.
- Zeitpunkt und Metadaten erfolgloser Anmeldeversuche.
- Zeitpunkt und Umfang einer Nutzung der Dienste.
- Weitere Daten die der Fehlerdiagnose, der Verbesserung der Anwenderfreundlichkeit und der Sicherung der Anwendungen dienen.

Es werden unstrukturierte Daten verarbeitet. Deren Inhalt und der Kreis der zugriffsberechtigten Personen liegen im Ermessen des Auftraggebers.

3.4 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Authentifizierte und Autorisierte Anwender
- Administratoren zur Verwaltung der Anwender und deren Berechtigungen

des Auftraggebers

- Kommerzielle Administratoren zur Verwaltung der Buchung der einzelnen Anwendungen
- Anonyme Anwender, die von authentifizierten und autorisierten Anwendern eingeladen wurden
- Personen, deren Daten vom Auftraggeber für die Verarbeitung vorgesehen sind

4 Pflichten der Vertragsparteien

1. Die OKIT verarbeitet personenbezogene Daten wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, die OKIT ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für sie bestehen, teilt die OKIT diese dem Auftraggeber mit sobald sie davon Kenntnis erlangt, es sei denn, die Mitteilung ist ihr gesetzlich verboten. Die OKIT verwendet darüber hinaus die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
2. Der Auftraggeber und OKIT bestätigen sich gegenseitig, dass die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Die Grundsätze ordnungsgemäßer Datenverarbeitung werden beachtet.
3. Der OKIT verpflichtet sich, bei der Verarbeitung vertraulicher Daten die Vertraulichkeit streng zu wahren. Der Auftraggeber verpflichtet sich keine Aktivitäten zu entfalten, die die Vertraulichkeit beschädigen.
4. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
5. Die Parteien sichern sich gegenseitig zu, dass die bei zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Die Parteien tragen dafür Sorge, dass zur Verarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzerfordernisse laufend angemessen angeleitet und überwacht werden.
6. Im Zusammenhang mit der beauftragten Verarbeitung wird der OKIT den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung unterstützen. Erforderlichen Angaben und Dokumentationen werden gemäß Vorgabe durch den Auftraggeber vorgehalten und können dem Auftraggeber auf Anforderung zugeleitet werden. Abschnitt 8 gilt entsprechend.
7. Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer

Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich die OKIT den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist. Abschnitt 8 gilt entsprechend.

8. Auskünfte an Dritte oder den Betroffenen darf die OKIT nur nach vorheriger Zustimmung oder Weisung durch den Auftraggeber erteilen. Direkt an die OKIT gerichtete Anfragen wird sie an den Auftraggeber weiterleiten.
9. Soweit gesetzlich verpflichtet, bestellt die OKIT eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. In Zweifelsfällen kann sich der Auftraggeber direkt an die für den Datenschutz zuständige Person wenden.
10. Die Kontaktdaten der für den Datenschutz verantwortlichen Person können der Datenschutzerklärung der OKIT unter <https://www.okit.de/datenschutz/> entnommen werden.
11. Der Auftraggeber benennt der OKIT die für Weisungen und Beauftragungen berechtigten Personen und nennt Identifikationsmerkmale für diese. Über Änderungen der Zuständigkeiten informiert der Auftraggeber die OKIT unverzüglich.
12. Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb Deutschlands.
13. Die Verwendung der Daten durch die Nutzer des Auftraggebers kann weltweit erfolgen. Es obliegt dem Auftraggeber seinen Nutzern entsprechende organisatorische Einschränkungen aufzuerlegen und diese zu kontrollieren. Für die Verwendung der verarbeiteten Daten durch Nutzer des Auftraggebers außerhalb des Geltungsbereiches der einschlägigen Datenschutzgesetze ist der Auftraggeber verantwortlich.
14. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
15. Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen. Im Zweifel wird die Umsetzung bis zum Eintreffen der dokumentierten Weisung lediglich vorbereitet und erst nach Eintreffen der dokumentierten Weisung umgesetzt. OKIT ist bei unklarer Weisungslage berechtigt den Zugriff auf die verarbeiteten Daten in Teilen oder komplett zu unterbinden.
16. Der Auftraggeber informiert die OKIT unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

4.1 Technische und organisatorische Maßnahmen

1. Die in Abschnitt 6 beschriebenen Datensicherheitsmaßnahmen bilden den verfügbaren Maßnahmenkatalog.
2. Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Maßnahmen und

Änderungen werden unverzüglich umgesetzt. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

3. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftraggeber die OKIT unverzüglich.
4. Die OKIT macht den Auftraggeber ausdrücklich darauf aufmerksam, dass die im Auftrag verarbeiteten Daten, die dem Zweck der Kollaboration mit anderen Auftraggebern und von Auftraggebern autorisierten Dritten dienen, nicht von anderen Datenbeständen strikt getrennt werden.
5. Kopien oder Duplikate werden von OKIT erstellt, soweit es sich um technisch notwendige, temporäre Vervielfältigungen und Backups handelt, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
6. Der Auftraggeber ermöglicht seinen besonders geschulten Mitarbeitern die Verarbeitung von Daten in Privatwohnungen auf den durch den Auftraggeber abgesicherten IT-Ressourcen. Soweit eine solche Verarbeitung erfolgt, stellt der OKIT sicher, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.
7. Die OKIT lehnt die Annahme und Verarbeitung dedizierter Datenträger, die von Auftraggeber stammen prinzipiell ab.
8. Die OKIT lehnt die Überlassung von Datenträgern an den Auftraggeber prinzipiell ab.
9. Die OKIT und Auftraggeber führen jeweils den regelmäßigen Nachweis der Erfüllung ihrer Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit.
10. Der Auftraggeber kann sich von der Angemessenheit der technischen und organisatorischen Maßnahmen zur Einhaltung der getroffenen Vereinbarungen oder der Datenschutzgesetze sowie von der Einhaltung seiner Weisungen überzeugen. Hierfür kann er sachverständige Dritte oder Auskünfte der OKIT heranziehen oder soweit erforderlich sich nach Anmeldung während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufes in den Betriebsstätten von OKIT davon überzeugen. OKIT wird dem Auftraggeber entsprechend den Zugriff auf die exklusiven Daten des Auftraggebers bzw. soweit erforderlich den Zutritt den Betriebsstätten der OKIT gewähren. Die Ergebnisse der Kontrolle wird der Auftraggeber in Abstimmung mit der OKIT dokumentieren.
11. Der Auftraggeber und der OKIT werden sich gegenseitig unverzüglich über Abweichungen von den Bestimmungen der einschlägigen Datenschutzvorgaben oder den im Auftrag getroffenen Festlegungen sowie über Störungen informieren und bei der Beseitigung von Mängeln unterstützen.

5 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

1. Im Rahmen des Auftrags verarbeiteten exklusiv dem Auftraggeber zugeordneten Daten wird die OKIT entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
2. Gesetzliche Dokumentationspflichten können der Löschung entgegenstehen.
3. Einschränkungen bestehen bei der Löschung von Daten, die der Kollaboration dienen und an denen andere Auftraggeber beteiligt sind. Klar als exklusiv dem Auftraggeber zugeordnete Informationen sind von dieser Einschränkung nicht betroffen.
4. Den entsprechenden Weisungen des Auftraggebers wird der OKIT jederzeit und auch zur Abwicklung dieses Vertrages Folge leisten, soweit dies gesetzlich zulässig oder vorgeschrieben ist.

6 Sicherheitsmaßnahmen

Von OKIT zu treffende Maßnahmen können Folgendes umfassen:

1. Zutrittskontrolle:
Schlüssel und/oder elektronische Zutrittskontrolle (z. B. durch Ausweisleser) zu OKIT Lokationen
2. Zugangskontrolle:
Autorisierte Benutzerkennungen und individuelle Passwörter oder Schlüssel für den Zugang zu Datenverarbeitungssystemen
3. Zugriffskontrolle:
Abgestufte Zugriffskonzepte mit unterschiedlichen Kennungen und Passwörter für den Zugriff auf Datenverarbeitungssysteme; Einsatz von passwortgeschützten Schlüsseln
4. Weitergabekontrolle:
Technische Maßnahmen, um zu verhindern, dass Kundendaten bei der elektronischen Übertragung oder während ihres Transports unbefugt verarbeitet oder genutzt werden können (z. B. durch Verschlüsselung oder Schutz durch Passwörter)
5. Eingabekontrolle:
Aufzeichnung von Zugriffen der OKIT Mitarbeiter auf Kundendaten in Logfiles bei Verarbeitung auf OKIT Systemen
6. Auftragskontrolle:
Anweisung an OKIT Mitarbeiter über Umfang und Inhalt der vom Kunden erteilten Weisungen
7. Verfügbarkeitskontrolle:
Maßnahmen zum Brandschutz und bei Stromausfällen in OKIT Rechenzentren

8. Trennungskontrolle:
Personenbezogene Daten unterschiedlicher Kunden werden physikalisch getrennt gespeichert.

Maßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden.

Welche der vorgenannten Maßnahmen von OKIT getroffen werden, ist abhängig der Art der zu schützenden Kundendaten sowie vom Gegenstand des Auftrages und damit vom Verantwortungsbereich der OKIT bei der Verarbeitung der Kundendaten.

7 Mitteilung bei Verstößen

1. OKIT erstattet unverzüglich in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers, gegen die sich aus diesem Vertrag ergebenden Verschwiegenheitsverpflichtungen oder gegen die im Auftrag getroffenen Festlegungen verstoßen wurde.
2. Eine Meldung an den Auftraggeber enthält mindestens die folgenden Angaben:
 - (a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - (b) falls nicht der für den Datenschutz Zuständige der Ansprechpartner ist, den Namen und die Kontaktdaten einer Anlaufstelle für weitere Informationen;
 - (c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - (d) eine Beschreibung der vom OKIT ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
3. Der Auftraggeber erstattet in allen Fällen unverzüglich Meldung an die OKIT, wenn ihm entsprechende Vorgänge zur Kenntnis kommen oder die Integrität der Datenschutzmaßnahmen kompromittiert wurde und dies der OKIT nicht bekannt sein könnte.
4. Auftraggeber und OKIT unterstützen sich gegenseitig darin entsprechende Vorfälle zu klären und gesetzeskonform abzuwickeln.

8 Vergütung

1. Die Vergütung an die OKIT ist wesentlich im Hauptvertrag geregelt. Die OKIT ist berechtigt, für Leistungen die auf Anforderung des Auftraggebers erbracht werden vom Auftraggeber angemessene Pauschalen oder eine

angemessene aufwandsbezogene Vergütung zu verlangen. Die OKIT kann eine Anzahlung oder Vorauszahlung der zu erwartenden Vergütung verlangen.

2. Der Auftraggeber trägt seine Aufwände selbst.
3. Eine Erstattung von nur teilweise in Anspruch genommenen Leistungen erfolgt nicht. Regelungen zur Vergütung gelten auch über das Ende des Vertrages hinaus.

9 Sonstiges

1. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
2. Für Nebenabreden ist die Schriftform erforderlich. Das gilt auch für die Abschaffung des Schriftformerfordernisses.
3. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

10 Beendigung des Auftrags

Bei Beendigung des Auftrags wird OKIT je nach Vereinbarung oder mangels Vereinbarung gemäß Weisung des Auftraggebers die exklusiv dem Auftraggeber zugeordneten Daten löschen.

11 Abschluss

Unterschriften und Stempel

Ort, Datum

Ort, Datum

Auftraggeber

OKIT