

Datenschutzkonzept i&k Premium Cloud®

der

i&k Software GmbH

Neuer Wall 3

24782 Büdelsdorf

1. Verantwortliche Stelle

Unternehmen: i&k Software GmbH Neuer Wall 3 24782 Büdelsdorf Vertretungsberechtigter Geschäftsführerin: Dipl. Informatikerin Diana Pabst Tel.: 04331 / 843 993 - 0 E-Mail: info[at]iuk-software.de	Datenschutzbeauftragter: Unseren Datenschutzbeauftragten und die Datenschutzabteilung erreichen Sie wie folgt: i&k Software GmbH Datenschutzabteilung Neuer Wall 3 24782 Büdelsdorf Tel.: 04331 / 843 993 - 0 E-Mail: datenschutz[at]iuk-software.de
--	---

2. Präambel

Die i&k Software GmbH verfügt als unabhängiges Softwareunternehmen über eine exzellente und langjährige Erfahrung in der Entwicklung und Implementierung von Softwareprodukten für Reisekostenabrechnungen und die Buchung von Geschäftsreisen im In und Ausland.

WinTrip® SaaS wird als Kernprodukt samt Ergänzungsbausteinen in der i&k Premium Cloud® auf Servern in deutschen Rechenzentren gehostet. Diese Rechenzentren sind insbesondere nach ISO 27001 zertifiziert und erfüllen sämtliche Anforderungen an den sicheren Betrieb von Serversystemen nach dem Stand der Technik. Die i&k Software GmbH erfüllt alle erforderlichen Anforderungen an den Datenschutz und die Datensicherheit. Weitere Einzelheiten zu den getroffenen technisch organisatorischen Maßnahmen (TOM) können Kunden und Interessenten der Vereinbarung zur Auftragsverarbeitung gemäß Art 28 DSGVO (AVV) entnehmen.

3. Grundsätze der Verarbeitung personenbezogener Daten

Die Europäische Datenschutz-Grundverordnung (nachfolgend DSGVO) regelt die allgemeinen Grundsätze für die Verarbeitung von personenbezogenen Daten (Art. 5 DSGVO), welche von der i&k Software GmbH als Auftragsverarbeiter konsequent umgesetzt werden.

Nach Art. 4 Nr. 1 DSGVO sind Personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen. Identifizierbar ist eine natürliche Person, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung (wie Name, Reisedaten, Adresse, Telefonnummer, E-Mail-Adresse, IP-Adresse, Standortdaten) identifiziert werden kann.

Dabei sind die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten in Art. 5 Abs. 1 DSGVO festgelegt:

- Rechtmäßigkeit der Verarbeitung
- Verarbeitung nach Treu und Glauben
- Grundsatz der Transparenz
- Grundsatz der Zweckbindung
- Grundsatz der Datenminimierung
- Grundsatz der Richtigkeit der Datenverarbeitung
- Speicherbegrenzung
- Grundsatz der Integrität und Vertraulichkeit

Die i&k Software GmbH als verantwortliche Stelle nach Art. 4 Nr. 7 DSGVO beachtet die Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art. 5 DSGVO.

Die Architektur von WinTrip® SaaS, der Ergänzungsbausteine sowie der Schnittstellen ermöglicht es, dass die Anwendung und die enthaltenen (personenbezogenen) Daten so verschlüsselt sind, dass Sie nichtberechtigten Personen (hierzu zählen auch Mitarbeiter der i&k Software GmbH) nicht ohne ausdrückliche Weisung bekannt

und verarbeitet werden können. Mit jedem Kunden vereinbart die i&k Software GmbH vor Beginn der Auftragsverarbeitung eine Vereinbarung zur Auftragsverarbeitung gemäß Art 28 DSGVO, welche die Rechte und Pflichten zum Datenschutz und zur Datensicherheit regelt. Sämtliche getroffenen TOM sind in der Anlage Technische und organisatorische Maßnahmen dokumentiert.

Eine Verarbeitung von personenbezogenen Daten durch die i&k Software GmbH erfolgt somit ausschließlich weisungsbezogen und auf Basis des vereinbarten AVV.

Weiterhin prüft der Datenschutzbeauftragte der i&k Software GmbH in regelmäßigen Abständen, ob alle personenbezogenen Daten gemäß den Grundsätzen der DSGVO und nach den weiteren datenschutzrechtlichen Vorschriften, insbesondere gem. BDSG, verarbeitet werden.

In diesem Zusammenhang werden die Mitarbeiter der i&k Software GmbH in regelmäßigen Abständen umfassend zum Datenschutz geschult und sensibilisiert sowie neue Mitarbeiter vor Aufnahme Ihrer Tätigkeit umfassend geschult und auf die Pflichten zum Datenschutz und als Auftragsverarbeiter geschult.

4. Bestellung eines Datenschutzbeauftragten

Gem. § 38 BDSG haben Unternehmen, in denen mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, einen Datenschutzbeauftragten zu benennen. Als pflichtbewusster Auftragsverarbeiter hat die i&k Software GmbH ordnungsgemäß einen Datenschutzbeauftragten bestellt.

Dieser prüft im Rahmen seiner Tätigkeit die Einhaltung sämtlicher gesetzlicher und vertraglicher Vorschriften zum Datenschutz und stellt die hiernach erforderlichen Dokumentationen sicher.

a) Unterauftragsverarbeiter und Datenübermittlung

Mit einer Auftragsverarbeitung gemäß Art. 28 DSGVO ist die Hinzuziehung externer oder interner Dienstleister zur Verarbeitung personenbezogener Daten zu verstehen. Die von der i&k Software beauftragten Unterauftragsverarbeiter sind in dem AVV entsprechend genannt. Sofern die Nutzung weiterer oder eines anderen Auftraggebers erforderlich werden, so informiert die i&k Software GmbH seine Kunden vorab mit der Bitte um Zustimmung. Eine solche Information regelt auch transparent die Möglichkeiten zur Zustimmung.

b) Internationale Datenübermittlung

Ein internationaler Datentransfer erfolgt durch die i&k Software GmbH als Auftragsverarbeiter nicht. Sämtliche personenbezogenen Daten werden auf Servern in deutschen Rechenzentren, die ISO 27001 zertifiziert sind, gehostet.

5. Unternehmensrichtlinien zum Datenschutz & zur IT-Nutzung

Bei der i&k Software GmbH bestehen verbindliche Vorgaben zur datenschutzkonformen Verarbeitung von personenbezogenen Daten sowie zur sicheren Nutzung der jeweiligen IT-Systeme. So werden alle Mitarbeiter vor tatsächlicher Tätigkeitsaufnahme auf die Regelungen zum Datenschutz sowie der IT-Sicherheit verpflichtet. Weiterhin finden regelmäßig Schulungen zum Datenschutz und der IT-Sicherheit statt.

6. Wichtige Richtlinien

a) Compliance Vorgaben

Die i&k Software GmbH legt höchste Maßstäbe an die Einhaltung gesetzlichen und sonstiger geltender rechtlicher Bestimmungen des Gesetzgebers. Hierbei sind die Vorgaben des Datenschutzes und die Bestimmungen im Rahmen der Auftragsverarbeitung von zentraler Bedeutung. Die einschlägigen Bestimmungen und Regelungen werden den Mitarbeitern im jeweils erforderlichen Umfang bereitgestellt.

b) Leitlinien zum Datenschutz

Alle für WinTrip® SaaS und die Ergänzungsbausteine relevanten Regelungen werden jedem Mitarbeiter vor tatsächlicher Tätigkeitsaufnahme zur Verfügung gestellt. Weiterhin werden diese Regelungen regelmäßig hinsichtlich Aktualität und Wirksamkeit überprüft und bei Bedarf entsprechend angepasst.

Im Allgemeinen hat die i&k Software GmbH folgende Ziele und Vorgaben zum Datenschutz definiert:

- Stellenwert des Datenschutzes und der IT-Sicherheit für das Unternehmen im Allgemeinen
- Verpflichtung zur Umsetzung rechtlicher Vorgaben im Bereich Datenschutz
- Regelung und Definition von Zuständigkeiten im Bereich Datenschutz
- Hinweis auf Konsequenzen bei Nichtbeachtung

7. Löschkonzept

Im Rahmen des geltenden Datenschutzrechts und der Begrenzung der Speicherdauer für die Dauer, für die die Verarbeitung tatsächlich erforderlich und zulässig ist, haben Unternehmen ein Löschkonzept zu erarbeiten und zu implementieren.

Bei Nutzung von WinTrip® SaaS und die Ergänzungsbausteine erfolgt die Verarbeitung von personenbezogenen Daten ausschließlich weisungsgebunden. Insoweit obliegt die Pflicht zur Löschung dem jeweiligen Auftraggeber. Die i&k Software GmbH wird den Kunden bei Bedarf in angemessenen Umfang im Rahmen einer bestehenden Auftragsverarbeitung bei der Umsetzung unterstützen.

8. Privacy by Default & Design

Nach den Anforderungen des Art. 25 DSGVO sollen datenschutzfreundliche Voreinstellungen (Privacy by Default) und durch Technikgestaltung (Privacy by Design) bereits ab Entwicklung umgesetzt werden.

Diese Grundsätze werden bereits vor Entwicklung einer Software im Rahmen des Planungs- und Designprozess umgesetzt. So kann die Einhaltung der DSGVO und der ergänzenden datenschutzrechtlichen Vorgaben softwareseitig dahingehend sichergestellt werden.

Dabei ist das Ziel, dass nur solche Verfahren eingesetzt werden, die sicherstellen können, dass nur solche personenbezogenen Daten verarbeitet werden, die zweckgebunden für die Verarbeitung erforderlich sind. Die Architektur von WinTrip® SaaS und der Ergänzungsbausteine stellt sicher, dass personenbezogene Daten nur berechtigten Personen bekannt werden können.

9. Umsetzung der Transparenz- und Informationspflichten nach Art 12- 14 DSGVO

Gemäß den Transparenzvorschriften (nach Art. 12 bis 14 DSGVO) sind betroffene Personen umfassend sowie in nachvollziehbarer Weise (leicht zugänglich, verständlich sowie in klarer und einfacher Sprache) darüber zu informieren, ob und wie deren personenbezogenen Daten verarbeitet werden.

Die Erfüllung der Informationspflichten (Art. 13, 14 DSGVO) umfasst insbesondere:

- Rechtsgrundlage der Datenverarbeitung
- Darstellung der berechtigten Interessen
- Festlegung der Dauer der Speicherung

Im Rahmen der Auftragsverarbeitung werden personenbezogene Daten lediglich nach Maßgabe der Weisungen durch die i&k Software GmbH verarbeitet. In der Regel obliegen die vorgenannten Pflichten dem Auftraggeber selbst. Soweit erforderlich stellt die i&k Software GmbH Informationen an geeigneter Stelle bereit und unterstützt den Auftraggeber im angemessenen Umfang.

10. Gewährleistung Rechte von Betroffenen

Die i&k Software GmbH gewährleistet die Rechte von Betroffenen im Rahmen ihrer Pflichten als Auftragsverarbeiter.

Die i&k selbst verarbeitet lediglich im Rahmen der Auftragsverarbeitung personenbezogenen Daten. Insoweit ist die i&k Software GmbH insbesondere nicht für die Sicherstellung folgender Betroffenenrechte von Softwarenutzern (den Nutzern selbst) zuständig:

- Auskunftsrecht (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung (Art. 17 DSGVO)

- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Recht auf Widerspruch (Art. 21 DSGVO)
- Widerruf einer zur Datenverarbeitung erteilten Einwilligung (soweit überhaupt erforderlich)

Die i&k Software unterstützt den Auftraggeber selbst (Unternehmen oder Einrichtungen in öffentlicher Trägerschaft) hierbei jedoch in angemessenem Umfang.

11. Einwilligungen nach Artt. 6 Abs. 1 lit. a, 7 DSGVO

Die Einwilligung gem. Artt. 6 Abs. 1 lit. a, 7 DSGVO stellt eine Rechtmäßigkeitsvoraussetzung für die Verarbeitung personenbezogener Daten dar. Soweit erforderlich ist diese nur wirksam, wenn sie die Anforderungen an die Freiwilligkeit und die erforderlichen Informationen für den Verarbeitungszweck und zum Umfang der Verarbeitung enthält sowie hinreichend dokumentiert wird.

Da in WinTrip® SaaS personenbezogene Daten lediglich weisungsgebunden im Rahmen der bestehenden Auftragsverarbeitung verarbeitet werden, ist die i&k Software für die Einholung etwaiger erforderlicher Einwilligungen beim Nutzer selbst nicht zuständig. Weiterhin erfolgt die Verarbeitung personenbezogener Daten im Rahmen eines Beschäftigtenverhältnisses zur Reisekostenabrechnung zur Erfüllung gesetzlicher Vorschriften (u.a. HGB, AO, GoBD).

12. Verpflichtung auf den Datenschutz und zur Einhaltung der DSGVO

Diese Verpflichtung beinhaltet die Pflicht zur Einhaltung der datenschutzrechtlichen Anforderungen (u.a. gem. DSGVO) jedes einzelnen Mitarbeiters zur Beachtung des gesetzlichen Verbots unbefugter Datenverarbeitung. *(Für die Verpflichtung auf das Datengeheimnis besteht gem. DSGVO und den ergänzenden gesetzlichen Bestimmungen keine unmittelbare Verpflichtung. Diese wird jedoch von den Aufsichtsbehörden insb. aus den Artt. 5 Abs. 1 und 2, 28 Abs. 3 Satz 2 lit. b, 32 Abs. 4 für nichtöffentliche Stellen abgeleitet. Für öffentliche Stellen gilt § 53 BDSG, der gemäß § 1 Abs. 5 BDSG aufgrund der Nichtregelung in der DSGVO zur Anwendung kommt.)*

Die Verarbeitung personenbezogener Daten darf nur erfolgen, sofern dies durch eine Rechtsvorschrift erlaubt oder angeordnet oder der Betroffene seine Einwilligung erteilt hat. Weiterhin besteht für Auftragsverarbeiter eine gesetzliche Verpflichtung zur Vertraulichkeit gem. Art. 28 Abs. 3 lit. b DSGVO.

Ferner verlangt das Gesetz, dass die Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen der DSGVO bereits bei der Aufnahme der Tätigkeit erfolgt. Daher sollte möglichst bereits bei Unterzeichnung des, spätestens unmittelbar vor Aufnahme der Tätigkeit, erfolgen. Die Verpflichtung besteht auch nach Beendigung des Arbeitsverhältnisses entsprechend fort. Weiterhin hat jeder Mitarbeiter Arbeitsanweisungen zum Datenschutz und zur IT-Sicherheit entsprechend umzusetzen

Alle bei der i&k Software beschäftigten Personen wurden auf die Einhaltung der datenschutzrechtlichen Anforderungen insbesondere der DSGVO verpflichtet.

13. Datenschutzzschulungen

Bei der i&k Software GmbH wird regelmäßig eine Datenschutzzschulung der Mitarbeiter durch den Datenschutzbeauftragten oder entsprechend qualifizierte sowie geeignete Personen durchgeführt. Die Teilnahme an solchen Schulungen ist verbindlich. Neue Mitarbeiter werden vor tatsächlicher Tätigkeitsaufnahme in den Datenschutz eingewiesen.

14. Technische und organisatorische Maßnahmen (TOM – Datensicherheit)

Die TOM (Technische und organisatorische Maßnahmen i.S.d. Art 32 DSGVO) halten die bei der i&k Software getroffenen Maßnahmen entsprechend fest. Unter Datensicherheit ist zu verstehen, dass Daten vor unbefugter Einsicht, Verfälschung, Änderung, Missbrauch oder Verlust geschützt werden.

Die getroffenen TOM müssen so sicher sein, dass Betroffene (und deren personenbezogene Daten) vor allen Risiken geschützt sind, welche durch Datenverlust und Datenmissbrauch entstehen oder eintreten könnten.

Unter Berücksichtigung des Stands der Technik (sowie u.a. der anfallen Kosten, der Art, des Umfangs und des Zweckes der Verarbeitung, der jeweiligen Wahrscheinlichkeit des Schadenseintritts, der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen) sind geeignete technische und organisatorische Maßnahmen (i.S.d. Art. 32 DSGVO) zu treffen, um ein dem jeweiligen Risiko angemessenes Schutzniveau zu gewährleisten.

Die TOM sollen dabei u.a. Folgendes gewährleisten:

- Pseudonymisierung und Verschlüsselung
- Vertraulichkeit der Daten und Informationen
- Datenintegrität
- Verfügbarkeit
- Belastbarkeit
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Die i&k Software GmbH hat geeignete Technische und organisatorische Maßnahmen getroffen, um die Datensicherheit entsprechend sicherzustellen. Die getroffenen TOM werden in der Anlage zur Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO (AVV) entsprechend dokumentiert.

Stand: 07.2022

© i&k Software GmbH