

Bedingungen zur Auftragsverarbeitung (AVV)

personenbezogener Daten gemäß Art. 28 DSGVO

Stand: 25.10.2021

1. VORBEMERKUNG

- 1.1. Die iComply GmbH, geschäftsansässig Große Langgasse 1a, 55116 Mainz, eingetragen unter HRB 49894 Amtsgericht Mainz (Auftragnehmer), stellt auf Grundlage der Nutzungsvereinbarung nebst Nutzungsbedingungen (Hauptvertrag) die digitale Hinweisgebersystem-Software iWhistle cloudbasiert als individualisierbare Software-as-a-Service (SaaS) an Kunden (Auftraggeber) bereit.
- 1.2. Auftraggeber und Auftragnehmer vereinbaren mit Abschluss des Hauptvertrages ausdrücklich auch nachfolgende Bedingungen zur Auftragsverarbeitung und schließen damit eine Vereinbarung zur Auftragsverarbeitung (AVV), mit welcher die damit verbundenen datenschutzrechtlichen Verpflichtungen geregelt werden.

2. UMFANG DER BEAUFTRAGUNG

- 2.1. Dieser AVV gilt für Zugang und Zugriff des Auftragnehmers zu personenbezogenen Daten (Daten), für die der Auftraggeber verantwortlich ist, im Rahmen der hauptvertraglichen Leistungserbringung des Auftragnehmers. Der Auftragnehmer verarbeitet Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn für die Einhaltung der datenschutzrechtlicheren Vorgaben, insbesondere der DSGVO, und der gesetzlichen Betroffenenansprüche im Hinblick auf die Daten.
- 2.2. Zweck, Art und Umfang der Verarbeitung, Art der Daten und Kategorien der betroffenen Personen sind:
 - Art und Zweck der Verarbeitung: Bereitstellung der digitalen Hinweisgebersystem-Software iWhistle, um Mitarbeitern und Dritten anonyme Meldungen von Rechtsverstößen zu ermöglichen.
 - Arten personenbezogener Daten: Verarbeitungsgegenstand personenbezogener Daten sind folgende Datenarten/-kategorien: Personenstammdaten (voraussichtlich Name, Vorname, Titel / akademischer Grad), Kommunikationsdaten (Telefon, E-Mail), Daten aus Meldungen (Hinweise auf Straftaten, Rechtsverstöße).
 - Kategorien der betroffenen Personen: Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen: Mitarbeiter (Zugriffsberechtigte), Meldende Personen, Betroffene Personen.
- 2.3. Der Auftragnehmer darf Daten anonymisieren oder aggregieren, so dass Identifizierung einzelner betroffener Personen nicht möglich ist, und in dieser Form für die bedarfsgerechte Gestaltung, Weiterentwicklung und Optimierung sowie die Leistungserbringung gemäß Hauptvertrags verwenden. Anonymisierte oder aggregierte Daten gelten nicht als Daten im Sinne dieses AVV.
- 2.4. Die Verarbeitung findet grundsätzlich innerhalb der Europäischen Union (EU) oder dem Europäischen Wirtschaftsraum (EWR) statt.

3. WEISUNGSBEFUGNIS

- 3.1. Der Auftragnehmer verarbeitet die Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, soweit er nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In einem solchen Fall teilt er dem Auftraggeber die rechtlichen Anforderungen vor der Verarbeitung mit, sofern sich dies nicht aufgrund wichtigen öffentlichen Interesses verbietet.

- 3.2. Die Weisungen des Auftraggebers sind grundsätzlich abschließend in diesem AVV und dem Hauptvertrag geregelt. Einzelweisungen, die hiervon abweichen oder zusätzliche Anforderungen aufstellen, bedürfen vorheriger Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des im Hauptvertrag festgelegten Änderungsverfahrens.
- 3.3. Die weisungsbefugte Person benennt der Auftraggeber im Hauptvertrag mit dem Hauptverantwortlichen (Administrator). Der Auftraggeber kann die weisungsberechtigte Person jederzeit unter Mitteilung an den Auftragnehmer in Textform auswechseln.
- 3.4. Der Auftraggeber erteilt Weisungen klar und nachvollziehbar. Weisungen dürfen nicht gegen geltendes Recht verstoßen. Ist eine Weisung aus der Sicht des Auftragnehmers unklar, weist er unverzüglich darauf hin und erbittet Klarstellung. Hält der Auftragnehmer eine Weisung für einen Verstoß gegen diese AVV oder geltendes Recht, kann er nach Mitteilung an den Auftraggeber die Ausführung bis zu einer Bestätigung durch den Auftraggeber aussetzen. Die alleinige Verantwortung für die weisungsgemäße Verarbeitung liegt beim Auftraggeber.

4. VERANTWORTLICHKEIT DES AUFTRAGGEBERS

Der Auftraggeber ist im Verhältnis zum Auftragnehmer für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte der Betroffenen allein verantwortlich. Der Auftraggeber informiert den Auftragnehmer unverzüglich und vollständig über festgestellte Fehler oder Unregelmäßigkeiten im Hinblick auf datenschutzrechtliche Bestimmungen oder Weisungen. Der Auftraggeber stellt dem Auftragnehmer auf Verlangen die in Art. 30 Abs. 2 DSGVO genannten Angaben bereit, soweit sie diesem nicht vorliegen. Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Daten des Auftraggebers zu erteilen oder mit solchen Stellen anderweitig zusammenzuarbeiten, unterstützt ihn der Auftraggeber auf erstes Anfordern bei der Erteilung von Auskünften und der Erfüllung anderweitiger Verpflichtungen.

5. ANFORDERUNG AN PERSONAL

Der Auftragnehmer setzt ausschließlich Personen ein, die zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen.

6. TECHNISCH-ORGANISATORISCHE MASSNAHMEN

Der Auftragnehmer ergreift gemäß Art. 32 DSGVO die nachfolgenden erforderlichen und geeigneten Maßnahmen, die unter Berücksichtigung des Standes der Technik, Implementierungskosten, Art, Umfang, Umständen und Zwecken der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein angemessenes Schutzniveau für die Daten des Auftraggebers zu gewährleisten (technisch-organisatorische Maßnahmen). Der Auftragnehmer darf diese während der Verarbeitung ändern und anpassen, solange sie weiterhin den gesetzlichen Anforderungen genügen.

6.1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen. Die deutschen Rechenzentren sind umfassend durch Einlasskontrollen und Sicherungsmechanismen gesichert, um einen unbefugten Zutritt zu Datenverarbeitungsanlagen zu verhindern (u.a. Alarmanlage, Wachdienst, Protokollierung des Zutritts usw.). Ein Zutritt ist nur autorisierten Mitarbeitern gestattet. Darüber hinaus sind die Büroräume des Auftragnehmers gesichert u.a. durch Schlüssel.
- Zugangskontrolle: Keine unbefugte Systembenutzung. Der Auftragnehmer setzt sichere und komplexe Passwörter ein, um eine unbefugte Systembenutzung auszuschließen. Die Inhalte werden durch AES-GCM mit 256 verschlüsselt. Backend-User erhalten neben einem Passwort einen

persönlichen Secret Key. 2-Faktor-Authentifizierung. Es wird eine Firewall eingesetzt und es besteht ein umfassender Malware-Schutz auf Arbeitsplatzrechnern und Servern. Verschlüsselung der Festplatten. Technische Sperre des Arbeitsplatzes bei Nicht-Aktivität. TLS-Verschlüsselung.

- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern, Entfernen innerhalb des Systems durch ein entsprechendes Berechtigungskonzept. Protokollierung von Zugriffen.
- Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben werden. Mehr-Mandantenfähigkeit. Trennung von Entwicklungs-, Test- und Produktivsystem.
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) Die Daten in iWhistle werden verschlüsselt. Dadurch können die verschlüsselten Daten nicht mit Daten Dritter de-pseudonymisiert bzw. es kann kein Personenbezug hergestellt werden.

6.2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern, Entfernen bei elektronischer Übertragung oder Transport durch eine industrieübliche SSL-Verschlüsselung.
- Eingabekontrolle: Veränderungen, Einfügungen und Löschungen werden durch die Protokollierung der Server-Logfiles erfasst. Derartige Veränderungen, Einfügungen und Löschungen durch Mitarbeiter des Auftraggebers werden umfassend und identifizierbar in iWhistle protokolliert.

6.3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle: Es werden täglich Back-ups angefertigt, um einen Verlust der Daten zu minimieren. Wir setzen einen industrieüblichen Virenschutz ein. Die Open Telekom Cloud (ISO/IEC 27001 Zertifiziert) setzt eine umfassende USV ein und weitere Schutzmaßnahmen um (Firewall, Meldewege und Notfallpläne).
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO): Eine Wiederherstellung der Daten aus dem Backup kann binnen weniger Minuten erfolgen. Dokumentation im Ticket-System.
- Widerstandsfähigkeit- und Ausfallsicherheitskontrolle: Es sind u.a. redundante Datenanbindungen und Ausweichserver vorhanden. Es werden regelmäßige Penetrationstests durchgeführt.

6.4. Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d; Art. 25 Abs. 1 DSGVO)

- Der Auftragnehmer hat ein umfassendes Datenschutz-Management-System implementiert, insbesondere eine Governance zur DSGVO, Verarbeitungsverzeichnis, einen für den Datenschutz Verantwortlichen benannt, Schulung und Sensibilisierung der Mitarbeiter.
- Incident-Response-Management entsprechend den Vorgaben der DSGVO wurde implementiert.
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO).
- Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen.
- Auftragskontrolle: Der Auftragnehmer evaluiert regelmäßig sein Datenschutz-Management-System und vergewissert sich regelmäßig von der datenschutzrechtlichen Zuverlässigkeit seiner Unterauftragnehmer.

7. UNTERAUFTRAGSVERARBEITER

7.1. Der Auftragnehmer darf Unterauftragsverarbeiter zur Verarbeitung hinzuziehen (Subunternehmer), soweit sichergestellt ist, dass diese die Voraussetzungen von Art 28 DSGVO und Ziffer 2.4 erfüllen.

7.2. Subunternehmer ist, wer Leistungen in direktem Zusammenhang mit Verarbeitung des Auftragnehmers erbringt. Wer lediglich Nebenleistungen erbringt, wie etwa Prüfung oder Wartung von Verarbeitungsverfahren oder -anlagen durch andere Stellen, Telekommunikationsleistungen, Post- und Transportdienstleistungen oder Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Verarbeitungsanlagen, ist kein Subunternehmer.

7.3. Derzeit eingesetzte Subunternehmer sind (nach Unternehmen, Anschrift, Zweck, Ort der Verarbeitung):

- Telekom Deutschland GmbH, Landgrabenweg 151, DE-53227 Bonn, Datenhaltung, Deutschland
- rapidmail GmbH, Wentzingerstraße 21, DE-79106 Freiburg, E-Mail Versand, Deutschland
- LINK Mobility Austria GmbH, Brauquartier 5/13, AT-8055 Graz, SMS Versand, Österreich

7.4. Der Auftragnehmer darf Subunternehmer jederzeit austauschen, soweit er die Übertragung der Pflichten aus diesem AVV sicherstellt. Der Auftragnehmer teilt dem Auftraggeber jeden neuen Subunternehmer vorab in Textform mit. Soweit der Auftraggeber innerhalb von 30 Tagen nach Benachrichtigung kein Widerspruch erhebt, gilt das Einverständnis als erteilt. Erhebt der Auftraggeber aus wichtigem, dem Auftragnehmer nachgewiesenen Grund Widerspruch, darf der Auftragnehmer die Zusammenarbeit mit einer Frist von 3 Monaten kündigen.

8. RECHTE DER BETROFFENEN

8.1. Der Auftragnehmer unterstützt den Auftraggeber mit technisch-organisatorischen Maßnahmen in Zumutbarem Maß, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der betroffenen Personen zustehenden Rechte nachzukommen. Soweit eine betroffene Person einen Anspruch auf Wahrnehmung ihrer zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer erhebt, leitet der Auftragnehmer das Ersuchen zeitnah weiter.

8.2. Der Auftragnehmer teilt dem Auftraggeber Informationen über gespeicherte Daten, Empfänger auftragsgemäßer Weitergabe von Daten und Zweck der Speicherung mit, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.

8.3. Der Auftragnehmer ermöglicht dem Auftraggeber, in erforderlichem und zumutbarem Maß Daten des Auftraggebers zu berichtigen, zu löschen, ihre weitere Verarbeitung einzuschränken oder auf Verlangen die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

8.4. Soweit eine betroffene Person gegenüber dem Auftraggeber nach Art. 20 DSGVO Übertragung von Daten des Auftraggebers fordert, unterstützt der Auftragnehmer dem Auftraggeber in erforderlichem und zumutbarem Maß bei der Bereitstellung in gängigem und maschinenlesbarem Format, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

9. MITTEILUNGEN UND UNTERSTÜTZUNG

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorheriger Konsultationen. Hierzu gehören die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen. Die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden. Dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen. Die Unterstützung des Auftraggebers für dessen Datenschutz-Folgeabschätzung und die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

10. DATENLÖSCHUNG

10.1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen

Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

- 10.2. Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Auftraggeber, spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger ausdrücklicher Zustimmung des Auftraggebers datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- 10.3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

11. NACHWEISE UND ÜBERPRÜFUNG

Der Auftragnehmer stellt dem Auftraggeber auf Anforderung alle erforderlichen und vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem AVV zur Verfügung. Der Auftraggeber darf die Einhaltung der Regelungen dieses AVV, insbesondere die Umsetzung der technischen-organisatorischen Maßnahmen, überprüfen. Dabei gilt was folgt:

- 11.1. Überprüfungen finden zu üblichen Geschäftszeiten ohne Störung des Betriebsablaufs beim Auftragnehmer sowie unter Beachtung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers statt. Der Auftraggeber informiert den Auftragnehmer in der Regel mindestens 14 Tage vorher über alle mit der Durchführung zusammenhängenden Umstände. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.
- 11.2. Der Auftragnehmer darf nach eigenem Ermessen unter Berücksichtigung gesetzlicher Verpflichtungen Informationen zurückhalten, (i) welche sensibel im Hinblick auf seine Geschäfte sind, oder (ii) deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstößt. Der Auftraggeber erhält keinen Zugang zu Daten oder Informationen über (i) andere Kunden des Auftragnehmers, (ii) Kosten, (iii) Qualitätsprüfungs- und Managementberichten sowie (iv) andere vertrauliche Daten des Auftragnehmers, die nicht unmittelbar relevant für die Auftragsverarbeitung sind.
- 11.3. Beauftragt der Auftraggeber einen Dritten mit der Durchführung, verpflichtet er diesen schriftlich (i) wie auch er gegenüber dem Auftragnehmer verpflichtet ist sowie (ii) auf Verschwiegenheit und Geheimhaltung, wenn der Dritte keiner beruflichen Verschwiegenheitspflicht unterliegt. Auf Verlangen legt er die Verpflichtungserklärung vor. Es darf kein Wettbewerber des Auftragnehmers beauftragt werden.
- 11.4. Nach Wahl des Auftragnehmers kann der Nachweis durch Vorlage eines geeigneten, aktuellen Testats oder Berichts unabhängiger Instanzen (Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder geeigneter Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (etwa BSI-Grundschutz) (insgesamt Prüfungsbericht) erbracht werden, wenn der Prüfungsbericht dem Auftraggeber ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

12. DAUER UND KÜNDIGUNG

Die Dauer der Verarbeitung sowie die Laufzeit und Kündigung dieses AVV richten sich nach der Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses AVV. Jede isolierte Kündigung dieses AVV ist ausgeschlossen.

13. HAFTUNG

Die Haftung für die Auftragsverarbeitung richtet sich nach Art. 82 DSGVO. Im Übrigen richtet sich die Haftung nach der Nutzungsvereinbarung.

14. ALLGEMEINE BESTIMMUNGEN

- 14.1. Die Vergütung des Auftragnehmers ergibt sich aus dem zugrundeliegenden Hauptvertrag. Im Fall von Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen die Regelungen dieses Vertrags vor. Sind einzelne Bestimmungen ganz oder teilweise unwirksam, auslegungs- oder ergänzungsbedürftig, erfolgt die Auslegung bzw. Ergänzung danach, welche Regelung dem sonstigen Inhalt und Zweck der Zusammenarbeit vernünftigerweise am ehesten entspricht und den Anforderungen des Art. 28 DSGVO genügt.
- 14.2. Änderungen und Ergänzungen dieser Vereinbarung müssen in Textform erfolgen und bedürfen der ausdrücklichen Angabe, dass damit die vorliegenden Bestimmungen geändert und/oder ergänzt werden. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- 14.3. Diese Vereinbarung unterliegt deutschem Recht.
- 14.4. Sofern der Zugriff auf die Daten, die der Auftraggeber dem Auftragnehmer zur Datenverarbeitung übermittelt hat, durch Maßnahmen Dritter (z.B. Maßnahmen eines Insolvenzverwalters, Beschlagnahme durch Finanzbehörden, etc.) gefährdet wird, hat der Auftragnehmer den Auftraggeber unverzüglich hierüber zu benachrichtigen.
- 14.5. Die Einrede des Zurückbehaltungsrechts gemäß § 273 BGB wird hinsichtlich der verarbeiteten Daten und der dazugehörigen Datenträger ausgeschlossen.
- 14.6. Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit des Vertrages im Übrigen unberührt. Die Parteien verpflichten sich, an Stelle der unwirksamen oder undurchführbaren Bestimmung eine solche wirksame und durchführbare Regelung zu vereinbaren, deren Wirkungen der wirtschaftlichen Zielsetzung am nächsten kommt, die die Parteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich der Vertrag als lückenhaft erweist.