# Vertrag zur Auftragsverarbeitung (AVV) gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

## für Interflex Cloud Services

zwischen

**dem Kunden**
- wie näher im Interflex Cloud Services Vertrag identifiziert -
(Verantwortlicher, nachfolgend „**Auftraggeber**“)

und

**Interflex Datensysteme GmbH**
Epplestraße 225
70567 Stuttgart
(Auftragsverarbeiter, nachfolgend „**Auftragnehmer**“)

## § 1 Gegenstand und Dauer der Vereinbarung

(1) Gegenstand

Der Auftragnehmer bietet Systeme für die automatisierte Zutrittskontrolle, Besuchermanagement, Zeiterfassung/-wirtschaft und Personaleinsatzplanung an.

Diese Vereinbarung gilt für alle Verarbeitungen von personenbezogenen Daten gemäß dem Interflex Cloud Services Vertrag (im Folgenden „**Leistungsvereinbarung**“). Dieser Vertrag zur Auftragsverarbeitung (AVV) wird dem Interflex Cloud Services Vertrag als Anhang 4 beigefügt.

(2) Dauer, Kündigung

Die Vereinbarung gilt solange der Auftragnehmer personenbezogene Daten im Rahmen der Durchführung der Leistungsvereinbarung verarbeitet, wenn nichts anderes vereinbart ist.

Beide Parteien können die Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß einer Partei gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt. Insbesondere die Nichteinhaltung der in dieser Vereinbarung vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

## § 2 Konkretisierung des Vereinbarungsinhalts

Zweck der vorgesehenen Verarbeitung von personenbezogenen Daten

Der Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber, die verarbeiteten Datenarten sowie die Kategorien betroffener Personen sind in der Leistungsvereinbarung und in **Anhang 1 - Datenschutzrechtliche Spezifikation** - näher beschrieben.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet derzeit ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Eine mögliche

spätere Verlagerung in ein Drittland bedarf der Zustimmung des Auftraggebers und hat die besonderen Voraussetzungen der Artt. 44 ff. DSGVO zu erfüllen.

## § 3 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich zur Erbringung seiner Leistungen gemäß Leistungsvereinbarung in Übereinstimmung mit den dokumentierten Weisungen des Auftraggebers, auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder eines Mitgliedstaates dem er unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtliche Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Die Weisungen ergeben sich im Übrigen aus der Leistungsvereinbarung und der durch den Auftraggeber vorgenommenen Einstellung und Konfiguration des Dienstes. Einzelweisungen nach Abschluss des Vertrages bedürfen der Textform und der Auftraggeber hat sie, falls der Auftragnehmer dies anfordert, schriftlich zu bestätigen.

(2) Erteilt der Auftraggeber Einzelweisungen, die über den in der Leistungsvereinbarung vereinbarten Leistungsumfang hinausgehen, bedarf dies der Zustimmung durch den Auftragnehmer.

(3) Der Auftragnehmer wird den Auftraggeber darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung auszusetzen.

(4) Der Auftraggeber kann dem Auftragnehmer in Textform durch eine vertretungsberechtigte Person die weisungsberechtigte Personen – oder einen etwaigen Wechsel der weisungsberechtigten Personen - für die Durchführung der Auftragsverarbeitung benennen. Grundsätzlich sind beim Auftragnehmer der entsprechend zuständige Key Account Manager oder Projektmanager oder Servicetechniker Weisungsempfänger, soweit eine vertretungsberechtigte Person des Auftragnehmers dem Auftraggeber nicht in Textform etwas anderes mitgeteilt hat.

## § 4 Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage der Vereinbarung. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit der Verarbeitung gem. Artt. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen (Einzelheiten in Anhang 2, der Bestandteil dieser Vereinbarung ist).

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen aber nicht unterschritten werden. Wesentliche Änderungen sind in Schriftform oder elektronisch zu dokumentieren.

(4) Sofern der Auftragnehmer Leistungen beim Auftraggeber vor Ort vornimmt, ist der Auftragnehmer nicht für die Einhaltung der technischen und organisatorischen Maßnahmen verantwortlich, die im Einfluss- und Verantwortungsbereich des Auftraggebers liegen.

## § 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieser Auftragsverarbeitung gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung einer/s Datenschutzbeauftragten gemäß Artt. 38 und 39 DSGVO.

   Die aktuellen Kontaktdaten des/der Datenschutzbeauftragten sind stets auf der Homepage des Auftragnehmers abrufbar.

b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

c) Die Umsetzung und Einhaltung aller für diese Auftragsverarbeitung erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Einzelheiten in Anhang 2, der Bestandteil dieser Vereinbarung ist).

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diese Auftragsverarbeitung beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Auf Anfrage des Auftraggebers weist der Auftragnehmer die getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 7 dieses Vertrages nach.

i) Bei Beendigung der unter der Leistungsvereinbarung zu erbringenden Leistungen oder auf Ersuchen des Auftraggebers gibt der Auftragnehmer dem Auftraggeber nach Maßgabe der Leistungsvereinbarung alle in seinem Besitz befindlichen Dokumente und alle Arbeitsergebnisse und Daten, die im Zusammenhang mit der Vereinbarung erstellt wurden, zurück oder löscht sie im Einklang mit dem Datenschutzrecht mit der vorherigen Zustimmung des Auftraggebers.

j) Der Auftragnehmer bewahrt Dokumentation, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dient, entsprechend den anwendbaren Aufbewahrungsfristen über das Ende der Vereinbarung hinaus auf. Der Auftragnehmer darf die Dokumentation bei Beendigung der Vereinbarung dem Auftraggeber übergeben.

## § 6 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Vereinbarung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, bei denen die Unterbeauftragung nicht im Schwerpunkt die Verarbeitung personenbezogener Daten betrifft, z. B. die Inanspruchnahme von Post-, Telekommunikations-, Logistik-, Reinigungs- und Handwerkerleistungen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der personenbezogenen Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf einen anderen Auftragsverarbeiter engagieren (nachstehend Unterauftragnehmer). Durch Unterzeichnung dieser Vereinbarung gibt der Auftraggeber dem Auftragnehmer die allgemeine Erlaubnis zur Beschäftigung von Unterauftragnehmer. Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern informieren. Der Auftraggeber kann etwaige Einwände gegen den Unterauftragnehmer mitteilen und, sollten diese nicht einvernehmlich gelöst werden, diese Vereinbarung zum Zeitpunkt des Wirksamwerdens der Änderung kündigen. Aktuell werden keine Unterauftragnehmer eingesetzt, es sei denn, solche sind in **Anhang 3 – Unterauftragnehmer** aufgeführt.

(3) Der Auftragnehmer wird mindestens die Pflichten nach dieser Vereinbarung im Rahmen von abzuschließenden Vereinbarungen zur (Unter-)Auftragsverarbeitung an seine Unterauftragnehmer weitergeben, einschließlich der Gewährleistung angemessener technisch-organisatorischer Maßnahmen. Diese müssen den Anforderungen des anwendbaren Datenschutzrechts entsprechen.

(4) Der Auftragnehmer wird mit allen Unterauftragnehmern Geheimhaltungsvereinbarungen treffen, soweit diese nicht bereits einer entsprechenden gesetzlichen Geheimhaltungspflicht unterliegen.

## § 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber kann sich auf eigene Kosten vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers gemäß Anhang 2 überzeugen und das Ergebnis dokumentieren. Dies kann u.a. durch Einholung einer Selbstauskunft des Auftragnehmers erfolgen, die dieser auch durch Vorlage eines geeigneten Zertifikats eines Sachverständigen erfüllen kann oder durch Durchführung einer Vor-Ort-Kontrolle.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer entsprechenden Kontrolle erforderlich sind.

(3) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle (einschließlich einer Vor-Ort-Kontrolle), hat der Auftraggeber den Dritten schriftlich auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen.

(4) Eine Durchführung einer Vor-Ort-Kontrolle ist in der Regel mit dreißig (30) Tagen schriftlich anzukündigen und hat zu üblichen Geschäftszeiten stattzufinden und hat die Störung des Geschäftsbetriebes des Auftragnehmers, soweit möglich, zu vermeiden. Routinemäßige Vor-Ort-Kontrollen sind auf maximal ein Mal pro Kalenderjahr begrenzt. Der Auftraggeber teilt dem Auftragnehmer schriftlich das Ergebnis seiner Kontrolle in der Regel innerhalb von 30 Tagen nach Abschluss der Kontrolle mit.

## § 8 Rechte der Betroffenen

(1) Die Rechte der durch die Verarbeitung von personenbezogenen Daten betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen.

(2) Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Auskunft, Berichtigung, Löschung oder Sperrung der ihn betreffenden Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(3) Für den Fall, dass eine betroffene Person ihre datenschutzrechtlichen Rechte geltend macht, wird der Auftragnehmer den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung dieser Ansprüche in angemessenem und für den Auftraggeber erforderlichen Umfang unterstützen, sofern der Auftraggeber die Ansprüche nicht ohne Mitwirkung des Auftragnehmers erfüllen kann.

(4) Der Auftragnehmer wird es dem Auftraggeber ermöglichen, personenbezogene Daten zu berichtigen, zu löschen oder zu sperren oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Löschung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

## § 9 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Daten, die der Auftragnehmer nur zur Durchführung seiner Leistungen (z. B. Wartung) verarbeitet, werden gelöscht, sobald sie nicht mehr zur Erbringung der jeweiligen Leistung erforderlich sind (vgl. Anhang 2 (Zugriffskontrolle).

## § 10 Mitteilung bei Verstößen

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Hierzu gehören u.a.

a) 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
b) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
c) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung, soweit erforderlich
d) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei entsprechenden Meldepflichten unterstützen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn ihm eine Verletzung des Schutzes personenbezogener Daten im Rahmen der Auftragsverarbeitung bekannt wird.

(4) Soweit den Auftraggeber aufgrund eines Vorkommnisses gesetzliche Informationspflichten wegen einer unrechtmäßigen Kenntniserlangung von personenbezogenen Daten treffen, hat der Auftragnehmer den Auftraggeber bei der Erfüllung der Informationspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen zu unterstützen. Die Mitwirkung ist vergütungspflichtig, es sei denn, sie ist in der Leistungsbeschreibung enthalten oder die Verletzung beruht auf einem Verschulden des Auftragnehmers.

## § 11 Haftung

Es gilt Art. 82 DSGVO. Soweit in der Leistungsvereinbarung Regelungen über die Haftung enthalten sind, gelten diese auch für das Innenverhältnis der Parteien im Rahmen dieser Vereinbarung.

## § 12 Vergütungspflicht

Soweit der Auftragnehmer durch diesen Vertrag zur Auftragsverarbeitung zu Leistungen verpflichtet ist, die nicht vom Leistungsumfang gemäß Leistungsvereinbarung umfasst sind („**Zusatzleistungen**“), sind diese gesondert nach Zeit- und Materialaufwand zu vergüten. Dies ist insbesondere der Fall für die in § 3(2), § 5 lit. d) und f), § 7 (soweit Leistungen nicht wegen eines vom Auftragnehmer verschuldeten Datenschutzverstoß erforderlich werden), § 8 und § 9 genannten Tätigkeiten. Die Parteien stellen klar, dass soweit der Auftragnehmer Zusatzleistungen rechtswidrig verursacht haben sollte, der Auftraggeber keine Vergütung gemäß diesem § 12 schuldet. Für Zusatzleistungen gelten die in der Leistungsvereinbarung oder anderweitig vereinbarten Stundensätze.

## § 13 Sonstiges

(1) Ergänzungen und Änderungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für einen etwaigen Verzicht auf das Schriftformerfordernis.

(2) Sollte eine Bestimmung dieser Vereinbarung rechtsunwirksam sein, so wird dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen Bestimmungen tritt rückwirkend eine inhaltlich möglichst gleiche Regelung, die dem wirtschaftlichen Zweck der gewollten Regelung am nächsten kommt.

(3) Die Einrede des Zurückbehaltungsrechts iSv. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(4) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DSGVO liegen.

(5) Diese Vereinbarung unterliegt deutschem Recht unter Ausschluss der Anwendung des internationalen Privatrechts. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist Stuttgart, Deutschland.

# Anhang 1 – Datenschutzrechtliche Spezifikation: Interflex Cloud Services:

Diese Anhang 1 (Datenschutzrechtliche Spezifikation) ist zusammen mit der abgeschlossenen Leistungsvereinbarung (Interflex Cloud Services Vertrag) zu lesen. Selbstverständlich werden nur die personenbezogenen Daten verarbeitet, die Bestandteil des vereinbarten Leistungsumfangs sind.

**Kategorien betroffener Personen:**

1. Beschäftigte im Sinne des § 26 Abs. 8 BDSG-neu, die das IF- System nutzen
2. Besucher/ Fremdarbeiter, ggf. mit Besucher-/Gastausweis für das IF- System, soweit entsprechendes Modul in der Leistungsvereinbarung vereinbart.

**Datenarten:**
Folgende Datenarten können vom Auftragnehmer, soweit Bestandteil der in Auftrag gegebenen Leistung, verarbeitet werden:

| | |
|---|---|
| **Ausweiserstellungsdaten** | Personalisierungsdaten für den sichtbaren Aufdruck auf dem Ausweismedium (Name, Vorname, ggf. Unterschrift und ggf. digitales Foto). Diese Daten sowie ggf. Unterschriftsdatum können in dem Modul für die Ausweiserstellung gespeichert werden. |
| **Besucher-Fremdfirmendaten** | Anmeldedaten, ggf. für den sichtbaren Aufdruck auf dem Ausweismedium/ Passier-schein (Name, Vorname, ggf. Unterschrift und ggf. digitales Foto des Betroffenen). Aufenthaltsdauer, Voranmeldedaten, Besuchter, Besuchsgrund, Einzelbesucher, Dauerbesucher. |
| **Buchungsdaten Zeiterfassung einschließlich Webclient** | Buchungsart Zeiterfassung mit Buchungs-terminal, Zeitstempel und Salden der Zeitkonten; Fehlgründe (Dienstgang, Dienstreise, Krank, Seminar, Urlaub etc.); Fehlzeiten (von bis); Fehlzeitsummen (Stunden pro Tag) – Die Möglichkeiten/ Zulässigkeit der Fehlgrund-eingaben und Fehlgrundanzeigen bestimmt der Auftraggeber selbst. |
| **Buchungsdaten Zutritt** | Buchungsart Zutritt mit Buchungsterminal, Zeitstempel und Ergebnis der Berechtigungs-prüfung. |
| **Logindaten** | Logindaten |
| **Lohnabrechnungskonten** | Stundensummen für das Gehalts-/ Abrechnungssystem |
| **Personaleinsatzplanungs- und Steuerungsdaten** | Funktionen, Qualifikationen, zeitliche Verfügbarkeit, Schichtpläne/ Arbeitsplatz-planung, statistische Daten aus der ACD (Telefonanlage) zur Aufbereitung des Personalbedarfs, Zeitkontenauswertungen. |
| **Personenstammdaten** | Stammsatznummer, Ausweisnummer, Name, Vorname, Personalnummer, Abteilung und den optionalen Feldern, sofern diese vom Auftraggeber im System genutzt werden |

| | |
|---|---|
| **Vorrechnerdaten** | Datenübergabe/ Datenaustausch mit Lohn- und Gehaltssystem. Datensätze bestehend aus: Stammsatznummer, Ausweisnummer, Name, Vorname, Personalnummer, Abteilung, Buchungsdaten Zeiterfassung und den optionalen Feldern, sofern diese vom Auftraggeber im System genutzt werden. Die Datenkommunikation hängt von der jeweiligen Konfiguration (Customizing) der Schnittstelle ab. |
| **Workflowdaten Zutrittskontrolle** | Anträge für Zutrittsberechtigungen; Genehmigender und Rückmeldung genehmigt ja/nein; E-Mailadresse dienstlich für die Workflowkommunikation. |
| **Workflowdaten Zeiterfassung** | Anträge für Korrekturen, Fehlgründe, Fehlzeiten; Genehmigender und Rückmeldung genehmigt ja/nein; E-Mailadresse dienstlich für die Workflow-kommunikation. |

# Anhang 2 – Technisch-organisatorische Maßnahmen

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

- Zutrittskontrolle
  *Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, wobei der Begriff räumlich zu verstehen ist*.

  Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

  ⇨ Zutrittskontrollsystem mit Ausweislesern für Chipkarten

  ⇨ Schlüssel / Schlüsselvergabe

  ⇨ Türsicherung (elektrische Türöffner usw.)

  ⇨ Empfang für Besucher

  Der Zutritt zu den Gebäuden / Gebäudeteilen bei Interflex erfolgt mittels elektronischer IF-Zutrittskontrolle. Besucher / Fremde können die Gebäudeteile von Interflex nur nach Registrierung und Freigabe betreten. Sie werden vom Besuchten begleitet.

- Zugangskontrolle
  *Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.*

  Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

  ⇨ Kontrolliertes Kennwortverfahren (Syntax mindestens 1 Sonderzeichen oder 1 Großbuchstabe, 1 Ziffer, Kleinschreibung, Mindestlänge = 10, regelmäßiger Kennwortwechsel alle 90 Tage, Wiederholzyklus = 24)

  ⇨ Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)

  ⇨ Einrichtung eines Benutzerstammsatzes pro User und Funktion

  ⇨ Verschlüsselung von Datenträgern mit AES 256 Bit Zip-Programm oder VeraCrypt oder ähnlichen Programmen.

  ⇨ Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)

Für die Anmeldung an den Rechnersystemen verwendet jeder Mitarbeitende einen individuellen Benutzernamen und Kennwort (bzw. Adminstratoren-Login für Administratoren). Bei Bedarf werden sie manuell mittels Active Directory mit dem Intranet verbunden. Ein externer Zugang zum Intranet ist ausschließlich via VPN möglich. Zugang wird nur gewährt, wenn die Identifikationsdaten des Rechners, Benutzernamen und Passwort dort bekannt sind und übereinstimmen. Die Syntax der, in regelmäßigen Abständen zu wechselnden Passwörter, lautet mindestens 10 Stellen, Sonderzeichen oder Großbuchstabe, Kleinschreibung sowie mindestens eine Ziffer. Der Wiederholzyklus beträgt 24. Diese Bedingungen werden beim Passwortwechsel automatisch kontrolliert, und bei Nichteinhaltung erfolgt die Ablehnung des neuen Passworts. Wird ein Passwort nicht rechtzeitig geändert, erlischt es und der Zugang wird verwehrt.

- Zugriffskontrolle

  *Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.*

  Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

  ⇨ Differenzierte Berechtigungen und temporäre Passwortvergabe (gemäß Berechtigungskonzept Interflex System) durch den Auftraggeber

  ⇨ Speicherung überlassener Daten auf lokalem Rechner in verschlüsselten Containern (z.B. mittels VeraCrypt oder ähnlichen Programmen). Der lokale Rechner ist zusätzlich mit einer Unternehmenslösung komplett verschlüsselt.

  ⇨ Zugriff erhält nur derjenige, der die jeweiligen Auftragsverarbeitung ausführt

  Dem Auftragnehmer überlassene Daten werden für die Dauer der Bearbeitung in lokalen, verschlüsselten Containern (z.B. VeraCrypt oder ähnlichen Programmen) vorgehalten und nach Abschluss der Arbeiten mit einem speziellen Löschtool (Eraser) wieder entfernt. Die lokalen Datenträger der Rechner, sind zusätzlich mit einer Unternehmenslösung komplett verschlüsselt. Die temporäre Vorhaltung der Daten erfolgt nur auf den lokalen Systemen derjenigen, die mit der Erfüllung des Auftrages beauftragt sind. Zugang zum PC haben nur berechtigte Interflex Nutzer.

  Die Zugriffskontrolle zu den Daten des Interflex- Kundensystems regelt der Auftraggeber durch Vergabe/ Nennung/ Löschung eines temporären Passwortes selbst.

  Innerhalb der Systeme des Auftragnehmers werden Berechtigungen ausschließlich nach dem Need-to-Know-Prinzip vergeben. Außerordentliche Berechtigungen unterliegen einem dokumentierten Freigabe-Workflow.

  Es existiert ein Prozess zur Vergabe von Berechtigungen, der u.a. auch die Vergabe von Rechten und Berechtigungen bei Änderungen (bspw. Abteilungswechsel) oder Austritten regelt.

  Nutzer sind per se nicht mit Administratorrechten ausgestattet. Bei Bedarf können lokale Adminrechte unter Angabe von Gründen beantragt werden und durchlaufen einen Freigabeworkflow. Sofern eine Bestätigung erfolgt, werden Administratortätigkeiten geloggt.

- Trennungskontrolle

  *Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.*

  Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

  ⇨ "Interne Mandantenfähigkeit" / Zweckbindung

⇨ Funktionstrennung / Produktion / Test

Kundendaten werden strikt getrennt von anderen Kundendaten temporär in verschlüsselten, Passwortgeschützten Containern gespeichert und bearbeitet. Im Falle einer Bearbeitung mittels Online- Remote Control erfolgen die Änderungen direkt im System des Auftraggebers. Für Testdaten gibt es einen separaten Server.

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen

  Im Servicefall wird in der Regel mit Daten gearbeitet, die vom Kunden pseudonymisiert zur Verfügung gestellt werden. Bei Bedarf können die Daten anonymisiert werden. Genaue Vorgehensweise hängt vom jeweiligen Servicefall ab.

## 2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle
  *Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle. Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen.*

  Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

  ⇨ Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)

  ⇨ Datensicherungen mittels Zip-Programm (z.B. Winzip oder ähnlichen Programmen) und 256 Bit AES- Verschlüsselung mit Passwort

  ⇨ Protokollierung

  Eine Weitergabe der Daten erfolgt im Regelfall nicht, außer wenn die Problemlösung eine Mitwirkung des Entwicklungsbereiches beim Auftragnehmer erfordert. Sollte diese erforderlich sein, so wird die Datensicherung entweder per Dateitransfer über einen SFTP-Server oder bei geringen Datenmengen im Intranet mittels Zip-Programm und 256 Bit AES- Verschlüsselung direkt übertragen. Die Weitergabe von Datensicherungen wird in Dokumenten protokolliert.

- Eingabekontrolle
  *Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.*

  Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

  ⇨ Protokollierung mittels Logfile in Interflex-System(en).

  Die IF- Systeme verfügen über ein Logfile, in welches die Änderungen mit der jeweiligen Benutzerkennung sowie Datum und Uhrzeit eingetragen werden.

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

- Verfügbarkeitskontrolle

  *Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.*

  Maßnahmen zur Datensicherung (physikalisch / logisch):

⇨ Kein Backup-Verfahren für Kundendatensicherungen um die datenschutzgerechte Löschung nach Wegfall der Zweckbestimmung zu gewährleisten

⇨ Virenschutz / Firewall / Patch-Management

⇨ USV für Server

⇨ Regelmäßige Wartung der IT-Hardware oder Einsatz von Leasing-Geräten

Datensicherungen von Kundensystemen werden nicht auf Servern mit Backup- Funktion gesichert, damit die datenschutzgerechte Löschung dieser Daten nach Wegfall der Zweckbestimmung sichergestellt werden kann.
Alle Rechnersysteme sind mit einer Antiviren-Lösung ausgestattet. Die Aktualisierung der Antivirensignaturen erfolgt zeitnah nach deren Erscheinung über die zentral gesteuerte Endpoint Protection Lösung. Eine automatische Vollprüfung findet wöchentlich statt. Alle Server sind mittels USV gegen Stromschwankungen bzw. Stromausfall gesichert.

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

  a) Für die eigenen Systeme des Auftragnehmers gibt es mehrere Server. Datensicherung durch tägliche Backups. Virtualisierung der Systeme mit zentralisiertem Backup in Vorbereitung
  b) Kundensysteme:
  Wenn Daten an Interflex übermittelt werden, dann keine Echtdaten, sondern nur Kopien von Daten und / oder Datenbanken. Für diese wird kein Backup erstellt, um die Löschung nach Wegfall des Verarbeitungszweckes, also nach Auftragserfüllung zu gewährleisten. Die Echtdaten verbleiben im System des Auftraggebers. Für die Daten im System des Auftraggebers liegt die Verantwortung beim Auftraggeber.

- Belastbarkeit:

  a) Die Auslastung der eigenen Systemen des Auftragnehmers wie Server, Netzwerk-, Internetsysteme unterliegen einem Monitoring mit Echtzeit-Incident-Reporting.
  b) Eine Datenwiederherstellung ist durch das Backup-Konzept auch standortübergreifend möglich. Es ist ein Live-Test der Systeme in Betrieb, welches eine Schwachstellenauswertung und automatisiertes Reporting beinhaltet.
  c) Es sind regelmäßig überprüfte Notfall- sowie Wiederherstellungspläne im Einsatz, um bei Systemausfällen schnell reagieren zu können.

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Datenschutz-Management;
- Incident-Response-Management: ist im ISMS (Informationssicherheits-Managementsystem) beinhaltet.
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
- Kontinuierliches Monitoring
- Rücksicherungen von Backups zu Testzwecken
- Regelmäßige Tests der USV
- Patch-Management
- Change-Management
- Verpflichtende Awareness-Schulungen für alle Mitarbeiter

- Auftragskontrolle
  *Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers*

  Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

  ⇨ Eindeutige Vertragsgestaltung gemäß Art. 28 DSGVO

  ⇨ Formalisierte Auftragserteilung (Wartungsvertrag, bzw. schriftliche Einzelbeauftragungen)

Der Auftragnehmer führt den beauftragten Leistungsumfang grundsätzlich selbst nach den Weisungen des Auftraggebers durch oder, soweit einschlägig, unter Zuhilfenahme von Unterauftragnehmer nach entsprechender Genehmigung durch den Auftraggeber.
Grundsätzlich erfolgen beauftragte Änderungen nur in den Programmen und in der Auswertelogik.

# Anhang 3 Unterauftragsverhältnisse

a) ☐ Eine Unterbeauftragung findet derzeit nicht statt.

b) ☒ Es bestehen zum Zeitpunkt dieser Vereinbarung folgende Unterauftragsverhältnisse:

| **Firma Unterauftragnehmer** | **Anschrift/Land** | **Leistung** |
|---|---|---|
| IONOS SE | Elgendorfer Str. 57, 56410 Montabaur, Deutschland | Betreiber Rechenzentren und Computerplattformen (IaaS) |