Vertrag zur Auftragsbearbeitung gemäss Art. 9 DSG und Art. 28 Datenschutz Grundverordnung (DSGVO, soweit anwendbar)

Rahmenvereinbarung, gültig für alle Beauftragungen

zwischen

[Vollständiger Firmenname Kunde]
[Adresse]
[Ort]
Schweiz
(Verantwortlicher, nachfolgend „**Auftraggeber**“)

und

Allegion International AG
Interflex
Mellingerstrasse 207 / Täfernhof
5405 Baden-Dättwil
Schweiz

(Auftragsbearbeiter, nachfolgend „**Auftragnehmer**“)

§ 1 Gegenstand und Dauer der Vereinbarung

(1) Gegenstand

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

Dieser Vertrag zur Auftragsbearbeitung („**ABV**“) gilt für sämtliche zwischen den Parteien bestehende und ggf. zukünftig abgeschlossene Vereinbarungen über die Erbringung bestimmter IT-Dienstleistungen in Bezug auf diese Systeme durch den Auftragnehmer für den Auftraggeber (im Folgenden „**Leistungsvereinbarung**“, auch wenn es sich um mehrere Vereinbarungen handelt).

Die Systeme des Auftragnehmers werden in der Regel durch den Auftraggeber als on-premise Lösung beim Auftraggeber betrieben, jedoch kann zumindest nicht ausgeschlossen werden, dass der Auftragnehmer im Rahmen der oben genannten IT-Dienstleistungen Zugriff nach Massgabe dieser Vereinbarung auf die personenbezogenen Daten des Auftraggebers haben kann.

(2) Dauer, Kündigung

Die Vereinbarung gilt solange der Auftragnehmer personenbezogene Daten im Rahmen der Durchführung der Leistungsvereinbarung bearbeitet, 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. 9 Schweizer Bundesgesetz über den Datenschutz („**DSG**“) bzw. Art. 28 DSGVO (soweit anwendbar) abgeleiteten Pflichten stellt einen schweren Verstoss dar.

§ 2 Konkretisierung des Vereinbarungsinhalts

Zweck der vorgesehenen Bearbeitung von personenbezogenen Daten

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

Die Erbringung der vertraglich vereinbarten Datenbearbeitung findet derzeit ausschliesslich im Gebiet der Schweiz, 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 Art. 16 DSG bzw. Artt. 44 ff. DSGVO (soweit anwendbar) zu erfüllen.

§ 3 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer bearbeitet 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 Bearbeitung 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 weisungsberechtigten Personen – oder einen etwaigen Wechsel der weisungsberechtigten Personen - für die Durchführung der Auftragsbearbeitung 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 Bearbeitung, 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 Bearbeitung gem. Art. 9 DSG und 8 DSG bzw. Artt. 28 Abs. 3 lit. c, 32 DSGVO (soweit anwendbar) insbesondere in Verbindung mit Art. 6 DSG bzw. Art. 5 Abs. 1, Abs. 2 DSGVO (soweit anwendbar) 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 Bearbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 8 DSG bzw. Art. 32 Abs. 1 DSGVO (soweit anwendbar) zu berücksichtigen (Einzelheiten in **Anlage 2**, die 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 Auftragsbearbeitung gesetzliche Pflichten gemäss Art. 9 DSG bzw. Artt. 28 bis 33 DSGVO (soweit anwendbar); insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung einer/s Datenschutzbeauftragten gemäss Art. 10 DSG bzw. Artt. 38 und 39 DSGVO (soweit anwendbar).

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

b) Die Wahrung der Vertraulichkeit gemäss Art. 8 DSG bzw. Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO (soweit anwendbar). 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 Auftragsbearbeitung erforderlichen technischen und organisatorischen Massnahmen gemäss Art. 8 DSG bzw. Artt. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (soweit anwendbar) (Einzelheiten in **Anlage 2**, die 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 Auftragsbearbeitung beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Bearbeitung personenbezogener Daten bei der Auftragsbearbeitung 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 Auftragsbearbeitung 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 Bearbeitung 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 Datenbearbeitung 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 Bearbeitung 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 Auftragsbearbeiter 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 **Anlage 3 – Unterauftragnehmer** aufgeführt.

(3) Der Auftragnehmer wird mindestens die Pflichten nach dieser Vereinbarung im Rahmen von abzuschliessenden Vereinbarungen zur (Unter-)Auftragsbearbeitung 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 Datenbearbeitung und sodann regelmässig von den technischen und organisatorischen Massnahmen des Auftragnehmers gemäss **Anlage 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 dreissig (30) Tagen nach Abschluss der Kontrolle mit.

§ 8 Rechte der Betroffenen

(1) Die Rechte der durch die Bearbeitung 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 Mitteilungen bei Verstössen

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 8 DSG und Art. 24 DSG und Artt. 32 bis 36 der DSGVO (soweit anwendbar) 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 Bearbeitung 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. 24 DSG und Art. 33 DSGVO (soweit anwendbar) bestehen kann, die eine Meldung an die Aufsichtsbehörde so rasch als möglich, spätestens aber 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 Auftragsbearbeitung 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.

(5) Vor dem Hintergrund, dass es sich vorliegend um eine vom Auftraggeber betriebene on-premise Lösung handelt, besteht die Unterstützungspflicht des Auftragnehmers gemäss dieses § 10 nur soweit der Auftraggeber nicht selbst in der Lage ist, die aufgeführten Informationen zu erlangen bzw. die aufgeführten Tätigkeiten nicht selbst auszuführen.

§ 10 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag bearbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Bearbeitung 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) bearbeitet, werden gelöscht, sobald sie nicht mehr zur Erbringung der jeweiligen Leistung erforderlich sind (vgl. **Anlage 2 unter Zutrittskontrolle**).

§ 11 Haftung

Es gelten die üblichen Haftungsbestimmungen des Schweizer Obligationenrechts. Es gilt zudem Art. 82 DSGVO (soweit anwendbar). Soweit in der Leistungsvereinbarung Regelungen über die Haftung enthalten sind, gelten diese auch für das Innenverhältnis der Parteien im Rahmen dieser Vereinbarung.

§ 12 Vergütungspflicht

(1) Soweit der Auftragnehmer durch diesen Vertrag zur Auftragsbearbeitung 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, § 9 und § 10 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 wird hinsichtlich der für den Auftraggeber bearbeiteten 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 des DSG und der DSGVO (soweit anwendbar) liegen.

(5) Diese ABV unterliegt dem Schweizer unter Ausschluss der Anwendung des internationalen Privatrechts und dem Wiener Kaufrecht (CISG). Als Gerichtsstand für alle Streitigkeiten, die sich aus oder im Zusammenhang mit dieser ABV ergeben, wird Baden, Schweiz vereinbart.

Allegion International AG	Name Kunde
_____	_____
Unterschrift	Unterschrift
_____	_____
Name, Funktion	Name, Funktion
_____	_____
Datum	Datum

Anlage 1 – Datenschutzrechtliche Spezifikation

Diese Anlage 1 (Datenschutzrechtliche Spezifikation) ist zusammen mit der jeweils abgeschlossenen Leistungsvereinbarung zu lesen. Selbstverständlich werden nur die personenbezogenen Daten bearbeitet, die Bestandteil des vereinbarten Leistungsumfangs sind.

Kategorien betroffener Personen:

1. Beschäftigte, die das IF- System nutzen
2. Besucher/ Fremdarbeiter, ggf. mit Besucher-/Gastausweis für das IF- System, soweit entsprechendes Modul in der Leistungsvereinbarung vereinbart.

Datenarten per Leistungselemente:

Folgende Datenarten (unten näher definiert) können vom Auftragnehmer, soweit Bestandteil der in Auftrag gegebenen Leistung, bearbeitet werden:

	Leistungen des Auftragnehmers, die mit einer Auftragsbearbeitung (Art. 8 DSG und Art. 28 DSGVO (soweit anwendbar)**) einhergehen**				
	Inbetriebnahme und Reparatur der Buchungsterminals	**Inbetriebnahme der Software**	**Softwareergänzung und Softwareupdates für Interflex IF-System(e)**	**Softwarepflege im Sinne von Störungsbeseitigungen**	**Datenbearbeitung per gesichertem Remote-zugriff (z.B. via VPN Verbindung)**
Produkte/ Systeme					
IF 6020 *Das Interflex System IF-6020 ist eine modular aufgebaute Software Applikation. Bei den meisten Anwendungen werden Terminals zur Zeiterfassung und oder Zutrittskontrolle angeschlossen.*	- Buchungsdaten Zutritt - Buchungsdaten Zeiterfassung	- Personenstammdaten - Buchungsdaten Zutritt - Buchungsdaten Zeiterfassung einschliesslich Webclient - Workflowdaten Zutrittskontrolle - Workflowdaten Zeit-erfassung - Vorrechnerdaten - Lohnabrechnungskonten - Ausweiserstellungsdaten - Besucher-/Fremdfirmendaten	- Personenstammdaten - Buchungsdaten Zutritt - Buchungsdaten Zeiterfassung einschliesslich Webclient - Workflowdaten Zutrittskontrolle - Workflowdaten Zeit-erfassung - Vorrechnerdaten - Lohnabrechnungskonten - Ausweiserstellungsdaten - Besucher-/Fremdfirmendaten	- Personenstammdaten - Buchungsdaten Zutritt - Buchungsdaten Zeiterfassung einschliesslich Webclient - Workflowdaten Zutrittskontrolle - Workflowdaten Zeit-erfassung - Vorrechnerdaten - Lohnabrechnungskonten - Ausweiserstellungsdaten - Besucher-/Fremdfirmendaten - Personaleinsatzplanungs- und Steuerungsdaten	- Personenstammdaten - Buchungsdaten Zutritt - Buchungsdaten Zeiterfassung einschliesslich Webclient - Workflowdaten Zutrittskontrolle - Workflowdaten Zeit-erfassung - Vorrechnerdaten - Lohnabrechnungskonten - Ausweiserstellungsdaten - Besucher-/Fremdfirmendaten - Personaleinsatzplanungs- und Steuerungsdaten

Produkte/Systeme					
IF 6040 *Das Interflex System IF-6040 ist eine modular aufgebaute Software Applikation. Bei den meisten Anwendungen werden Terminals zur Zeiterfassung und oder Zutrittskontrolle angeschlossen.*	- Buchungsdaten Zutritt - Buchungsdaten Zeiterfassung	- Personenstammdaten - Buchungsdaten Zutritt - Buchungsdaten Zeiterfassung einschliesslich Webclient - Workflowdaten Zutrittskontrolle - Workflowdaten Zeiterfassung - Vorrechnerdaten - Lohnabrechnungskonten - Ausweiserstellungsdaten - Besucher-/Fremdfirmendaten	- Personenstammdaten - Buchungsdaten Zutritt - Buchungsdaten Zeiterfassung einschliesslich Webclient - Workflowdaten Zutrittskontrolle - Workflowdaten Zeiterfassung - Vorrechnerdaten - Lohnabrechnungskonten - Ausweiserstellungsdaten - Besucher-/Fremdfirmendaten	- Personenstammdaten - Buchungsdaten Zutritt - Buchungsdaten Zeiterfassung einschliesslich Webclient - Workflowdaten Zutrittskontrolle - Workflowdaten Zeiterfassung - Vorrechnerdaten - Lohnabrechnungskonten - Ausweiserstellungsdaten - Besucher-/Fremdfirmendaten - Personaleinsatzplanungs- und Steuerungsdaten	- Personenstammdaten - Buchungsdaten Zutritt - Buchungsdaten Zeiterfassung einschliesslich Webclient - Workflowdaten Zutrittskontrolle - Workflowdaten Zeiterfassung - Vorrechnerdaten - Lohnabrechnungskonten - Ausweiserstellungsdaten - Besucher-/Fremdfirmendaten - Personaleinsatzplanungs- und Steuerungsdaten
SP-EXPERT *Das Interflex System SP-EXPERT ist eine modular aufgebaute Software Applikation. Bei den meisten Anwendungen werden Personaleinsatz-planungs- und Steuerungsdaten erstellt oder verwendet.*	- Buchungsdaten Zutritt - Buchungsdaten Zeiterfassung	- Personenstammdaten - Bewegungsdaten - Zeitwirtschaftsdaten - Buchungsdaten Zeiterfassung - Vorrechnerdaten - Lohnabrechnungskonten	Kein IF-System	- Personenstammdaten - Bewegungsdaten - Zeitwirtschaftsdaten - Buchungsdaten Zeiterfassung - Vorrechnerdaten - Lohnabrechnungskonten - Personaleinsatzplanungs- und Steuerungsdaten - Log Dateien - Transferverzeichnisse mit aus anderen Systemen importierten Daten oder in	- Personenstammdaten - Bewegungsdaten - Zeitwirtschaftsdaten - Buchungsdaten Zeiterfassung - Vorrechnerdaten - Lohnabrechnungskonten - Personaleinsatzplanungs- und Steuerungsdaten - Log Dateien - Transferverzeichnisse mit aus anderen Systemen importierten Daten oder in

				andere Systeme exportierte Daten	andere Systeme exportierte Daten
Ausweis-personalisierung	Ausweiserstellungsdaten	Ausweiserstellungsdaten	Ausweiserstellungsdaten	Ausweiserstellungsdaten	Ausweiserstellungsdaten
Besucher-/Fremdfirmen-personalisierung	Besucher-/ Fremdfirmendaten	Besucher-/ Fremdfirmendaten	Besucher-/ Fremdfirmendaten	Besucher-/ Fremdfirmendaten	Besucher-/ Fremdfirmendaten

Definition der Datenarten:

Buchungsdaten Zutritt	Buchungsart Zutritt mit Buchungsterminal, Zeitstempel und Ergebnis der Berechtigungs-prüfung.
Personenstammdaten	Stammsatznummer, Ausweisnummer, Name, Vorname, Personalnummer, Abteilung und den optionalen Feldern, sofern diese vom Auftraggeber im System genutzt werden
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.
Workflowdaten Zutrittskontrolle	Anträge für Zutrittsberechtigungen; Genehmigender und Rückmeldung genehmigt ja/nein; E-Mailadresse dienstlich für die Workflowkommunikation.

Lohnabrechnungskonten	Stundensummen für das Gehalts-/ Abrechnungssystem
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.
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,

Workflowdaten Zeiterfassung	Anträge für Korrekturen, Fehlgründe, Fehlzeiten; Genehmigender und Rückmeldung genehmigt ja/nein; E-Mailadresse dienstlich für die Workflow-kommunikation.

	Besuchter, Besuchsgrund, Einzelbesucher, Dauerbesucher.
Personaleinsatzplanungs- und Steuerungsdaten	Funktionen, Qualifikationen, zeitliche Verfügbarkeit, Schichtpläne/ Arbeitsplatz-planung, statistische Daten aus der ACD (Telefonanlage) zur Aufbereitung des Personalbedarfs, Zeitkontenauswertungen.

Anlage 2 – Technisch-organisatorische Massnahmen

1. Vertraulichkeit

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenbearbeitungsanlagen, 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 Auftragsbearbeitung 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 Administrationsrechten ausgestattet. Bei Bedarf können lokale Adminrechte unter Angabe von Gründen beantragt werden und durchlaufen einen Freigabeworkflow. Sofern eine Bestätigung erfolgt, werden Administratorentätigkeiten geloggt.

- Trennungskontrolle

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

  Massnahmen zur getrennten Bearbeitung (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
  Die Bearbeitung 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

- 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 auf CD/DVD

  ⇨ 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 mittels Zip-Programm, 256 Bit AES- Verschlüsselung und mit Passwort auf CD/DVD gebrannt und per Post versendet, 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

- 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

  ⇨ USV für Server

  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;

  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 Bearbeitungszweckes, 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 Systeme 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 Widerherstellungspläne im Einsatz, um bei Systemausfällen schnell reagieren zu können.

4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management;
- Incident-Response-Management: ist im ISMS (Informationssicherheits-Managementsystem) beinhaltet.
- Datenschutzfreundliche Voreinstellungen;
- Kontinuierliches Monitoring
- Rücksicherungen von Backups zu Testzwecken
- Regelmässige Tests der USV

- Auftragskontrolle
  Keine Auftragsdatenbearbeitung ohne entsprechende Weisung des Auftraggebers

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

  ⇨ Eindeutige Vertragsgestaltung

  ⇨ 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.

Anlage 3 Unterauftragsverhältnisse

a) ☐ Eine Unterbeauftragung findet derzeit nicht statt.

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

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Interflex Datensysteme GmbH	Epplestr. 225, 70567 Stuttgart	Hersteller, zusätzlicher Support (z.B. 2nd und 3rd Level)