

Allgemeine Geschäftsbedingung

der INFORM Institut für Operations Research und Management GmbH („INFORM“)

für

das Produkt SYNCROTESS in der Cloud

Stand: März 2023

§ 1 Geltungsbereich

- (1) Diese Allgemeinen Geschäftsbedingungen (im Folgenden „AGB“) in ihrer zum Zeitpunkt des Vertragsschlusses geltenden Fassung regeln die zeitlich begrenzte Zurverfügungstellung des bei der Bestellung ausgewählten Softwareproduktes (im Folgenden „Software“) über das Internet ausschließlich an Unternehmen (im Folgenden „Kunden“; INFORM und der Kunde zusammen die „Vertragspartner“). Diese AGB einschließlich ihrer Anhänge bilden zusammen mit den individuellen Angaben und Bestelldaten des Kunden den Vertrag.
- (2) Der Kunde kann sich bei Vertragsschluss zwischen unterschiedlichen Editionen der Software und optionalen Zusatzpaketen entscheiden. Die hierfür geltenden Parameter wie Leistungsumfang des Supports, Höhe der Nutzungsgebühr, Zeitraum der Speicherung der mit der Software verarbeiteten Transaktionsdaten werden dem Kunden bei Vertragsschluss angezeigt.
- (3) Es gilt ausschließlich der Vertrag. Mündliche Nebenabreden zwischen den Parteien bestehen nicht. Abweichende oder diesen AGB entgegenstehende Geschäftsbedingungen des Kunden finden keine Anwendung; dies gilt auch dann, wenn INFORM den Geschäftsbedingungen des Kunden nicht ausdrücklich widerspricht. Werden zwischen dem Kunden und INFORM ausdrücklich individualvertragliche Vereinbarungen geschlossen, so gelten diese ergänzend zu diesen AGB und gehen ihnen im Zweifel vor.
- (4) Einseitige Änderungen dieser AGB mit Wirkung auf bestehende Verträge dürfen nur insoweit erfolgen, als hierdurch das Äquivalenzverhältnis zwischen Leistung und Gegenleistung nicht unangemessen zu Lasten des Kunden verändert wird. INFORM ist in diesem Rahmen berechtigt, diese AGB zu ändern. Neufassungen der AGB werden dem Kunden schriftlich oder per E-Mail unter Hervorhebung der Änderungen mitgeteilt. Sie werden wirksam, wenn der Kunde der Neufassung nicht innerhalb von sechs Wochen ab Zugang der Änderungsmitteilung schriftlich widerspricht. Auf die Folgen seines Untätigbleibens wird der Kunde bei Mitteilung der Änderungen ausdrücklich hingewiesen. Widerspricht der Kunde der Neufassung der AGB, setzt sich das Vertragsverhältnis zu den ursprünglichen Bedingungen fort, kann von INFORM aber mit einer Frist von drei Monaten außerordentlich gekündigt werden.

§ 2 Vertragsschluss

- (1) Die Darstellung der Software auf der Webseite stellt noch kein rechtlich bindendes Angebot von INFORM dar, sondern lediglich eine unverbindliche Aufforderung an den Kunden, seinerseits ein Angebot abzugeben. Mit Abschluss der Bestellung des Kunden durch Anklicken des Bestell-Buttons gibt der Kunde ein verbindliches Angebot auf Abschluss eines Vertrages ab. Vor Abschluss der Bestellung kann der Kunde auf einer gesonderten Seite seine Bestell- und Vertragsdaten noch einmal kontrollieren und ggf. Korrekturen vornehmen (z.B. eine andere Software-Edition auswählen).

- (2) INFORM wird den Eingang der elektronischen Bestellung des Kunden durch Versand einer automatischen Eingangsbestätigung per E-Mail bestätigen. Diese Eingangsbestätigung stellt noch keine verbindliche Annahme des Angebots des Kunden dar. Sie dient lediglich dazu, den Kunden über den Zugang seiner Bestellung zu informieren. Der Vertrag kommt erst mit Freischaltung des Kunden-Accounts zustande. INFORM ist frei darin, Bestellungen des Kunden nicht anzunehmen; die Entscheidung darüber liegt im Ermessen von INFORM.
- (3) Nach einer elektronischen Bestellung des Kunden über die Webseite von INFORM werden die individuellen Bestell- und Vertragsdaten des Kunden von INFORM gespeichert. INFORM ist berechtigt den Kunden zu kontaktieren, um seine Identität zu prüfen und ggfs. Rückfragen zur Bestellung zu klären. Der Kunde kann seine Bestell- und Vertragsdaten nach Freischaltung seines Kunden-Accounts mit der Rolle „Firmenadmin“ über die Benutzeroberfläche der Software einsehen und ergänzen. Im Übrigen bekommt jeder Kunde nach Prüfung seiner Bestellung eine Zusammenfassung der Bestell- und Vertragsdaten (mitsamt der in den Vertrag einbezogenen AGB) nochmals per E-Mail zugesandt. Die jeweils aktuelle Fassung der AGB ist ferner über die Webseite von INFORM jederzeit abrufbar und ausdrückbar. Verträge über die Webseite werden in deutscher und/ oder englischer Sprache geschlossen.

§ 3 Sonderregelung während der Testphase

- (1) Die Vertragslaufzeit beginnt mit einer Testphase, in der die Software kostenfrei genutzt werden kann. Die Laufzeit dieser Testphase ist bei Vertragsabschluss festgelegt, im Bestellvorgang angegeben und kann durch INFORM auf Anfrage in besonderen Fällen verlängert werden.
- (2) Während dieser Testphase hat der Kunde die Möglichkeit, die Funktionalität der gewählten Edition ohne Einschränkungen zu nutzen, die operativen Stammdaten aufzubauen und den Arbeitsablauf zu testen. Die für eine spätere Rechnungsstellung benötigten Vertragsdaten sind bis zum ersten Monatswechsel einzupflegen, um auch hier einen reibungslosen Ablauf sicherzustellen.
- (3) Der Kunde wird per E-Mail rechtzeitig auf den Ablauf der kostenfreien Testphase hingewiesen. Bis zum Ende der Testphase steht beiden Parteien ein außerordentliches fristloses Kündigungsrecht zu. Für eine solche Kündigung innerhalb der Testphase gilt abweichend von den übrigen Regelungen dieser AGB nicht die Schriftform, sondern die Textform. Eine Kündigung per E-Mail an cloud-support@inform-software.com ist also ausreichend.

§ 4 Hauptleistungen; Funktionsumfang der Software

- (1) INFORM stellt dem Kunden für die Laufzeit des Vertrages die Software in der jeweils aktuell freigegebenen Version im Rahmen der vereinbarten Verfügbarkeit (vgl. SLA im Anhang B) zur Nutzung über das Internet zur Verfügung. Eine Überlassung der Software auf Dauer (Kauf) erfolgt nicht. Dem Kunden steht zusammen mit der Software eine elektronische Benutzerdokumentation als Online-Hilfe in deutscher Sprache zur Verfügung.
- (2) Entwickelt INFORM während der Vertragslaufzeit zusätzliche Module, Sprachversionen und/ oder neue Funktionalitäten der Software, kann sie diese nach eigenem Ermessen in den Standard der Software aufnehmen und dem Kunden (z.B. im Rahmen eines regulären Updates) ohne zusätzliche Vergütung zur Verfügung stellen oder dem Kunden gegen entsprechende Erhöhung der Nutzungsgebühr im Rahmen neuer Editionen oder hinzubuchbarer Zusatzpakete gesondert anbieten. Der Kunde hat keinen Anspruch auf kostenlose Zurverfügungstellung solcher neu entwickelten Module, Sprachversionen bzw. Funktionalitäten.
- (3) INFORM stellt dem Kunden während der Vertragslaufzeit Speicherplatz in einem externen Rechenzentrum zur Speicherung seiner mit der Software verarbeiteten Transaktionsdaten zur Verfügung (Hosting). Die Speicherung der Daten erfolgt über den für die vom Kunden gewählte Software-Edition geltenden Zeitraum und zwar auf externen Servern, die von einem Dritten im Auftrag von INFORM betrieben werden. Die Kosten für die Speicherung der Transaktionsdaten sind mit der einheitlichen Nutzungsgebühr abgegolten. Der Kunde ist nicht berechtigt, den Speicherplatz einem Dritten ganz oder teilweise, entgeltlich oder unentgeltlich zur Nutzung zu überlassen.

- (4) INFORM ist berechtigt, die vertraglich vereinbarten Leistungen durch Dritte als Subunternehmer zu erbringen, insbesondere bedient sich INFORM des externen Rechenzentrums, in dem die Software zur Nutzung vorgehalten und die Transaktionsdaten des Kunden gespeichert werden.
- (5) Im Rahmen der kontinuierlichen Verbesserung und Weiterentwicklung der Software können während der Vertragslaufzeit neue Funktionen und Leistungen hinzukommen, verändert werden oder wegfallen, sofern dies zu keiner wesentlichen Einschränkung der vertraglich vereinbarten Leistungen führt, die Erreichung des Vertragszwecks hierdurch nicht gefährdet wird und die Anpassung für den Kunden zumutbar ist.

§ 5 Einräumung von Nutzungsrechten

- (1) Die Urheber- und sonstigen Schutzrechte an der Software inklusive der Benutzerdokumentation stehen im Verhältnis zum Kunden ausschließlich INFORM zu. Der Kunde erhält lediglich die im Folgenden näher beschriebenen einfachen Nutzungsrechte an der Software.
- (2) Der Kunde erhält an der Software das nicht ausschließliche, nicht übertragbare und nicht unterlizenzierbare, zeitlich auf die Laufzeit des Vertrages begrenzte Recht, diese für seine eigenen geschäftlichen Zwecke zu nutzen. Alle darüber hinausgehenden Rechte, insbesondere das Recht zur Vervielfältigung, Verbreitung einschließlich der (Weiter-)Vermietung, zur Bearbeitung sowie zur öffentlichen Zugänglichmachung verbleiben bei INFORM. Die Software darf vom Kunden ausschließlich zum vertragsgemäßen Zweck eingesetzt werden; die bestimmungsgemäße Nutzung der Software ergibt sich im Einzelnen aus der entsprechenden Beschreibung der Einsatzzwecke auf der INFORM-Webseite. Jede über die bestimmungsgemäße Nutzung hinausgehende Verwendung der Software ist unzulässig.
- (3) Der Kunde ist nicht berechtigt, die Software für geschäftliche Zwecke Dritter zu nutzen oder von Dritten für sich nutzen zu lassen oder Dritten zugänglich zu machen. Ausgenommen hiervon sind Dritte, die im schriftlichen Auftrag des Kunden mit Tätigkeiten im Rahmen der Durchführung der Transaktionen des Kunden betraut sind.
- (4) Die Transaktionsdaten gehören dem Kunden. Dieser räumt INFORM alle zur Vertragserfüllung erforderlichen Rechte an den von ihm übermittelten Daten ein, insbesondere zur Speicherung und Verarbeitung seiner Transaktionsdaten. Ferner erhält INFORM vom Kunden das Recht, die mit der Software verarbeiteten Transaktionsdaten für Analyse- und Benchmarkingzwecke anonymisiert auszuwerten und sie hierfür mit anderen Daten zusammenzuführen, zu vervielfältigen und zu bearbeiten. INFORM stellt dabei sicher, dass der Kunde bei einer etwaigen Publizierung der Ergebnisse für Dritte nicht (auch nicht indirekt) identifizierbar ist. Eine anderweitige Verwendung der Daten durch INFORM oder Weitergabe von nicht anonymisierten Daten an Dritte ist nicht zulässig.

§ 6 Serviceleistungen

INFORM erbringt während der Laufzeit dieses Vertrages die in diesem § 6 näher beschriebenen und – sofern im Folgenden nicht anders angegeben – von der einheitlichen transaktionsabhängigen Nutzungsgebühr abgedeckten Serviceleistungen:

- (1) INFORM wird dem Kunden die Software während der Vertragslaufzeit im Rahmen der vereinbarten Verfügbarkeit (vgl. SLA im Anhang B) betriebsbereit zur Nutzung zur Verfügung stellen und instand halten. Dem Kunden werden während der Vertragslaufzeit von INFORM allgemein freigegebene Updates der Software zentral zur Verfügung gestellt.
- (2) Für Fragen zur Anwendung und Nutzung der Software steht dem Kunden während der Laufzeit seines Vertrages eine Online-Hilfe im Kundenportal zur Verfügung. Bei auftretenden Störungen und Fehlern, die eine Nutzung der Software ganz oder teilweise verhindern, kann sich der Kunde an die Service E-Mail-Adresse cloud-support@inform-software.com richten. Nutzt der Kunde die Enterprise Edition der Software, steht ihm darüber hinaus bei Auftreten nutzungsverhindernder Störungen und Fehler auch eine Hotline zur Verfügung. Details sind der jeweils gültigen Fassung des Anhang B – Service Level Agreement (SLA) zu entnehmen.

- (3) Der Kunde wird aufgetretene Störungen und Fehler der Software so detailliert beschreiben, dass diese durch INFORM reproduziert und nachvollzogen werden können. Ordnungsgemäß gemeldete Fehler wird INFORM im Rahmen ihrer Instandsetzungspflicht nach näherer Maßgabe des § 8 sowie der Regelungen des SLA im Anhang B beseitigen.
- (4) Auf Wunsch des Kunden erbringt INFORM optional Beratungs- und Unterstützungsleistungen zur Einführung und Anwendung der Software, wie Unterstützung bei der Konfiguration, Schulungen von Mitarbeitern des Kunden oder Inbetriebnahmeunterstützung. Hierzu zählt ebenfalls die individuelle Bereitstellung aller gespeicherten Transaktionsdaten in einem durch den Kunden spezifizierten Form. Diese Leistungen werden auf Anforderung des Kunden erbracht und diesem gemäß der jeweils gültigen Jahrespreisliste bzw. der INFORM-Schulungsbedingungen von INFORM gesondert nach Aufwand in Rechnung gestellt.

§ 7 Verantwortung und Mitwirkung des Kunden

- (1) Der Kunde erbringt alle für eine Nutzung der Software erforderlichen Mitwirkungsleistungen, insbesondere die in diesem § 7 und in den Anhängen im Einzelnen aufgeführten und beschriebenen Leistungen.
- (2) Der Kunde ist dafür verantwortlich, dass die für die vertragsgemäße Inanspruchnahme und Nutzung der Software erforderlichen und von INFORM in Anhang A beschriebenen technischen Mindestanforderungen an die von ihm eingesetzte Hard- und Software sowie seine Internetanbindung erfüllt sind. Der Kunde ist selbst für die Beschaffung eines geeigneten Internet-Browsers verantwortlich, mit dem auf die Software zugegriffen werden kann. Der Kunde darf keine Software oder andere technische Einrichtungen verwenden, die das Funktionieren der Software gefährden können. Insbesondere ist es dem Kunden nicht gestattet, mit anderen technischen Mitteln als den in Anhang A aufgeführten auf die Software und seine Transaktionsdaten zuzugreifen.
- (3) Der Kunde verpflichtet sich, keine Inhalte auf dem Speicherplatz zu speichern, deren Übermittlung, Speicherung oder Nutzung gegen geltendes Recht oder Vereinbarungen mit Dritten (z.B. zur Geheimhaltung) verstößt. Der Kunde wird die Software nicht manipulieren und keinerlei Daten auf den Servern von INFORM speichern, die die Software, die Server, die sonstige IT-Infrastruktur oder Daten anderer Kunden beschädigen oder gefährden. Er wird die Daten anderer Kunden ferner nicht entwenden und den zur Verfügung gestellten Speicherplatz nicht mit außergewöhnlich großen Datenmengen belasten, die zur Bearbeitung seiner Transaktionen nicht erforderlich sind.
- (4) Der Kunde trägt die alleinige Verantwortung für die Einhaltung aller rechtlichen Anforderungen an seine Transaktionsabwicklung und die Speicherung, Aufbewahrung und Archivierung seiner Transaktionsdaten. Hierzu zählt auch die Beachtung der allgemeinen handels- und steuerrechtlichen Aufbewahrungsfristen sowie der ggf. anwendbaren spezifischen (z.B. branchenabhängigen) Aufbewahrungspflichten und -fristen (z.B. für bestimmte Umweltdaten). Der Kunde trifft im Rahmen seiner Schadensminderungspflicht angemessene Vorkehrungen für den Fall eines Datenverlusts, insbesondere durch regelmäßige Überprüfung seiner eigenen IT-Systeme und die regelmäßige Anfertigung von Sicherungskopien seiner mit der Software verarbeiteten Transaktionsdaten über die von INFORM hierfür bereitgestellte Exportfunktion.
- (5) Aufwendungen, die INFORM durch die unterbliebene, verzögerte oder nicht ordnungsgemäße Mitwirkung des Kunden, insbesondere durch Einsatz veralteter oder fehlerhafter Schnittstellen, falsche Handhabung der Software, fehlerhafte, unvollständige, widersprüchliche, veraltete oder nicht den Anforderungen von INFORM entsprechende Daten oder terminliche Verzögerungen seitens des Kunden entstehen, werden dem Kunden gesondert nach Aufwand gemäß der jeweils gültigen Jahrespreisliste von INFORM in Rechnung gestellt. Weitergehende Rechte von INFORM bleiben hiervon unberührt.

§ 8 Gewährleistung

- (1) INFORM übernimmt keine Gewähr für die mit der Software erzielten Ergebnisse und Ausgaben, insbesondere deren Aktualität, Korrektheit, Qualität und Vollständigkeit, soweit diese auf den

Eingaben des Kunden beruhen. Die vom Kunden eingegebenen Transaktionsdaten werden weder von INFORM noch von der Software auf ihre inhaltliche Richtigkeit geprüft oder korrigiert.

- (2) INFORM übernimmt die Gewähr dafür, dass die Software der Produktbeschreibung auf der Webseite www.inform-software.com und der Benutzerdokumentation entspricht und frei von Schutzrechten Dritter ist, die den vertragsgemäßen Gebrauch der Software verhindern oder beschränken. Ansprüche können vom Kunden nur geltend gemacht werden wegen Mängeln, die reproduzierbar sind oder vom Kunden nachvollziehbar beschrieben werden können. Keinen Mangel stellen insbesondere Funktionsbeeinträchtigungen der Software dar, die aus der Hardware- oder Softwareumgebung des Kunden, fehlerhaften Daten, unsachgemäßer Benutzung oder aus sonstigen aus dem Verantwortungsbereich des Kunden stammenden Umständen resultieren. INFORM übernimmt keine Gewährleistung für nicht von INFORM erstellte Anbindungen der Software an die Systeme des Kunden.
- (3) Ordnungsgemäß gerügte Mängel der Software werden von INFORM während der Laufzeit dieses Vertrages im Rahmen der durch die Nutzungsgebühr abgedeckten Instandhaltungs- und Instandsetzungspflichten innerhalb angemessener Frist und nach näherer Maßgabe des SLA in Anhang B behoben.
- (4) Das Kündigungsrecht gemäß § 543 Abs. 2 Nr. 1 BGB kann der Kunde nur unter der Voraussetzung geltend machen, dass er INFORM zuvor schriftlich unter angemessener Fristsetzung von mindestens zwei Wochen zur Nacherfüllung aufgefordert hat und die Frist erfolglos verstrichen ist.
- (5) Schadensersatz und Ersatz vergeblicher Aufwendungen leistet INFORM nur in den Grenzen des § 9.

§ 9 Haftung

- (1) Erbringt INFORM gegenüber dem Kunden Leistungen, ohne dass hierfür eine Vergütung anfällt, z.B. die Überlassung der Software während einer unentgeltlichen Testphase, haftet INFORM insoweit nur für vorsätzliche und grob fahrlässige Pflichtverletzungen.
- (2) Für Mängel der Software, die bereits bei Vertragsschluss vorhanden waren, haftet INFORM entgegen der gesetzlichen Regelung des § 536a BGB nur, wenn INFORM solche Mängel zu vertreten hat.
- (3) Im Übrigen leistet INFORM Schadensersatz und Ersatz vergeblicher Aufwendungen, gleich aus welchem Rechtsgrund (z. B. vertragliche Pflichtverletzung, unerlaubte Handlung), nur in folgendem Umfang:
 - bei Arglist, Vorsatz und grober Fahrlässigkeit in voller Höhe;
 - in Fällen einfacher Fahrlässigkeit nur bei Verletzung einer vertragswesentlichen Pflicht (wenn keiner der in diesem § 9 genannten Fälle der unbegrenzten Haftung vorliegt), deren Erfüllung die ordnungsgemäße Durchführung des Vertrages erst ermöglicht und auf deren Einhaltung der Kunde regelmäßig vertrauen darf (sog. Kardinalpflicht) und nur in Höhe des bei Vertragsschluss typischerweise vorhersehbaren Schadens, maximal jedoch bis zur zehnfachen Höhe der in den letzten zwölf Monaten vor Schadenseintritt für die Nutzungsgebühr gezahlten Netto-Summe.
- (4) Außer im Falle von Vorsatz oder grober Fahrlässigkeit und sofern es sich nicht um eine Kardinalpflicht seitens INFORM handelt, haftet INFORM bei Datenverlusten nur für den Schaden, der auch bei ordnungsgemäßer und risikoadäquater Datensicherung durch den Kunden entstanden wäre, begrenzt auf die in den letzten zwölf Monaten vor Schadenseintritt für die Nutzungsgebühr gezahlte Netto-Summe.
- (5) Bei Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, ist die Haftung, auch bei einer einfach fahrlässigen Pflichtverletzung von INFORM oder eines gesetzlichen Vertreters oder Erfüllungsgehilfen von INFORM, der Höhe nach unbegrenzt. Ebenfalls unbegrenzt der Höhe nach ist die Haftung auch für Schäden, die auf schwerwiegendes Organisationsverschulden von INFORM zurückzuführen sind, sowie für Schäden, die durch Fehlen einer garantierten Beschaffenheit, eines garantierten Leistungserfolges oder der Übernahme eines Beschaffungsrisikos hervorgerufen wurden.

§ 10 Geheimhaltung; Zugangsdaten; Datenschutz; Datensicherheit

- (1) Die Vertragspartner verpflichten sich gegenseitig, vertrauliche Informationen und Unterlagen des anderen Vertragspartners, die entweder offensichtlich als vertraulich anzusehen sind oder vom anderen Vertragspartner als vertraulich bezeichnet werden, wie Geschäfts- und Betriebsgeheimnisse zu behandeln. Der Kunde wird insbesondere sämtliche von INFORM zur Verfügung gestellten Programme, Dokumentationen und sonstige Unterlagen als Betriebs- und Geschäftsgeheimnisse von INFORM behandeln und nicht an unbefugte Dritte weitergeben.
- (2) Die Software darf nur von Mitarbeitern des Kunden sowie vom Kunden schriftlich beauftragte Dritte genutzt werden, die den Kunden bei der Durchführung seines Arbeitsauftrags unterstützen, z.B. der Logistikdienstleister oder die Speditionen des Kunden. Solche Dritten sind vor dem Zugriff auf die Software durch den Kunden schriftlich zur Geheimhaltung zu verpflichten. Sonstigen Dritten darf der Kunde die Benutzung der Software und den Zugang zur Cloud-Oberfläche weder direkt noch indirekt ermöglichen.
- (3) Es ist dem Kunden untersagt, seine persönlichen Zugangsdaten zum Kunden-Account bzw. zur Cloud-Oberfläche der Software an unbefugte Dritte weiterzugeben. Alle Zugangsdaten sind geschützt aufzubewahren, so dass Dritte darauf nicht zugreifen können. Der Kunde wird INFORM unverzüglich benachrichtigen, sofern der Verdacht besteht, dass unbefugte Dritte von ihnen Kenntnis erlangt haben könnten. Besteht der Verdacht einer unbefugten Kenntnisnahme der Zugangsdaten durch Dritte ist INFORM berechtigt, den Zugang des Kunden zu seinem Kunden-Account bzw. zur Cloud-Oberfläche der Software vorübergehend zu sperren.
- (4) INFORM bedient sich zur Erfüllung ihrer Vertragspflichten eines externen Rechenzentrums bzw. Rechenzentrumsbetreibers. Der Kunde hat keinen Anspruch auf die Einschaltung und Nutzung eines bestimmten Rechenzentrumsbetreibers. INFORM wird jedoch stets sicherstellen, dass sich die genutzten Rechenzentren innerhalb der EU befinden und dass – nach den Angaben des jeweiligen Rechenzentrumsbetreibers – eine Übermittlung von Daten des Kunden in Länder außerhalb der EU nicht erfolgt. Die Browser-Anbindung an das Rechenzentrum erfolgt SSL-verschlüsselt. Die betroffenen Sicherheitsmaßnahmen im externen Rechenzentrum umfassen insbesondere die physische Sicherheit, die logische Sicherheit, die Betriebssicherheit und den Datenschutz.
- (5) Der Kunde bearbeitet und speichert mit der zur Verfügung gestellten Hard- und Software lediglich seine eigenen operativen Transaktionsdaten. Soweit die INFORM überlassenen Daten des Kunden einen Personenbezug aufweisen, ist der Kunde als verantwortliche Stelle für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Der Kunde stellt sicher, dass die für die Übermittlung an und Verarbeitung durch INFORM einschlägigen gesetzlichen Anforderungen erfüllt sind. Hierbei ist zur Sicherstellung der Möglichkeiten einer vollumfänglichen datenschutzrechtlichen Selbstauskunft nach der europäischen Datenschutzgrundverordnung DSGVO durch den Endanwender dringend darauf zu achten, dass Eingabefelder zweckbezogen befüllt werden und in Freitextfeldern (z.B. Bemerkungsfeldern) keine personenbezogenen Daten, z.B. UserID, Name, Telefonnummer, Email-Adressen usw. eingegeben werden. Der Kunde akzeptiert die im Anhang beigefügte Vereinbarung zur Auftragsverarbeitung. INFORM ist berechtigt, die überlassenen Daten zu Zwecken der Vertragserfüllung an den Betreiber des jeweils beauftragten externen Rechenzentrums weiterzugeben.
- (6) Im Rahmen des Kundenprojektes werden i.A. sensible Kundendaten und personenbezogene Daten verarbeitet. Nicht nur für Aspekte der Software sondern auch für die Verarbeitung der Daten wird durch die INFORM die Einhaltung eines Sicherheitsniveaus auf Grundlage der ISO27001 angestrebt. Die Informationen innerhalb von Kundenprojekten klassifiziert die INFORM als vertraulich, was auch geeignete Maßnahmen zur sicheren Kommunikation und Datenaustausch zwischen Kunde und INFORM einschließt, u.a. auch die Verwendung einer, nach dem Stand der Technik, sicheren Transportverschlüsselung auf beiden Seiten.

§ 11 Laufzeit und Kündigung

- (1) Der Vertrag hat eine anfängliche Laufzeit bis zum 31.12. des auf den Vertragsschluss folgenden Kalenderjahres. Er verlängert sich danach jeweils um ein weiteres Kalenderjahr, wenn er nicht von

einem der Vertragspartner mit einer Frist von drei (3) Monaten vor Ablauf der jeweiligen Laufzeit gekündigt wird.

- (2) Ein Upgrade auf eine höhere Edition und/oder eine Hinzubuchung von Zusatzpaketen ist jederzeit möglich mit einer Umstellungszeit von in der Regel ein bis drei Werktagen. Die ursprüngliche Vertragslaufzeit bleibt hiervon unberührt. Ein Downgrade auf eine niedrigere Edition ist zum Ende der jeweiligen Vertragslaufzeit möglich und muss vom Kunden jeweils spätestens eine Arbeitswoche vor dem Ende der jeweiligen Vertragslaufzeit angezeigt werden. Mit Wirksamwerden der Umstellung wird die Vergütungshöhe für die nachfolgenden Transaktionen entsprechend angepasst.
- (3) Das Recht beider Vertragspartner zu einer außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund besteht für INFORM insbesondere dann, wenn der Kunde sich mit einem erheblichen Teil der Vergütung in Zahlungsverzug befindet oder in sonstiger Weise gegen wesentliche Pflichten aus dem Vertrag verstößt. Nach ihrer Wahl kann INFORM bei Vorliegen eines wichtigen Grundes den Zugang des Kunden zur Cloud-Oberfläche der Software sowie den Zugriff des Kunden auf seine Transaktionsdaten zunächst vorübergehend sperren und den Kunden unter angemessener Fristsetzung zur Beseitigung des Pflichtverstoßes bzw. zur Vertragserfüllung auffordern. Weitergehende Rechte von INFORM bleiben hiervon unberührt.
- (4) INFORM kann den Vertrag auch dann jederzeit mit sofortiger Wirkung außerordentlich kündigen, wenn der Kunde mit der Software in einem Zeitraum von mindestens 12 Monaten keine zahlungspflichtige Transaktion mehr durchgeführt hat.
- (5) Die Parteien sind zur Einhaltung aller anwendbaren Export- und Importkontrollvorschriften sowie zur Beachtung aller nationalen und ausländischen Handelsbeschränkungen verpflichtet. Ist eine Partei aufgrund solcher Beschränkungen nicht in der Lage, ihre Verpflichtungen aus dem Vertrag zu erbringen, so steht ihr ein außerordentliches fristloses Kündigungsrecht zu. Schadensersatzansprüche sind in diesem Fall für beide Parteien ausgeschlossen.
- (6) Jede Kündigung bedarf zu ihrer Wirksamkeit der Schriftform.
- (7) INFORM ist nicht verpflichtet, die Daten des Kunden über den Zeitpunkt der Beendigung dieses Vertrages hinaus zu speichern, zu archivieren und/ oder für den Zugriff durch den Kunden vorzuhalten

§ 12 Vergütung und Zahlungsbedingungen

- (1) Die Vergütung der vertraglichen Leistungen erfolgt über eine feste Grundgebühr zuzüglich einer transaktionsabhängigen Nutzungsgebühr (zusammen im Folgenden „Nutzungsgebühr“). Die transaktionsabhängige Nutzungsgebühr kann ausgelegt sein auf Nutzungsgebühr pro Einzeltransaktionen oder gestaffelt nach Transaktionsblöcken. Die Höhe der Nutzungsgebühr richtet sich zum einen nach der vom Kunden bei Vertragsschluss ausgewählten Software-Edition, den ausgewählten Zusatzpaketen sowie zum anderen nach der Anzahl von Transaktionen/Transaktionsblöcke (im Sinne von durch den Kunden angelegten (Transport-) Aufträgen, die der Kunde mit der Software verarbeitet (pay-per-use Modell). Die Anzahl der Transaktionen wird vom System automatisch und transparent erfasst und gespeichert; der Kunde kann die aktuelle Anzahl seiner Transaktionen jederzeit über seinen Kunden-Account einsehen.
- (2) Die Nutzungsgebühr wird von INFORM monatlich jeweils zu Beginn eines Kalendermonats für den vorangegangenen Monat abgerechnet. Sollte der Rechnungsbetrag den Mindestbetrag von 300 € unterschreiten, behält sich INFORM vor, die Abrechnung dieses Betrages in den nachfolgenden Abrechnungszyklus zu verschieben. Die Rechnung erhält der Kunde als pdf-Dokument per E-Mail an die von ihm in seinem Kunden-Account hinterlegte E-Mail Adresse.
- (3) INFORM hat das Recht, sowohl die Grundgebühr als auch die transaktionsabhängige Nutzungsgebühr durch schriftliche oder per E-Mail erfolgende Ankündigung unter Einhaltung einer Frist von sechs Wochen zum Kalenderjahresende entsprechend der allgemeinen Preisentwicklung (unter Berücksichtigung der Entwicklung des Verbraucherpreisindex, vgl. www.destatis.de) anzupassen. Eine solche Anpassung darf die vorstehenden Gebührenanteile des vorausgehenden Kalenderjahres um nicht mehr als 10% überschreiten. Soweit eine Erhöhung der Nutzungsgebühr um

mehr als 5% erfolgt, kann der Kunde den Vertrag schriftlich mit einer Frist von vier Wochen zum Kalenderjahresende kündigen.

- (4) Leistungen, die der Kunde gesondert nach Aufwand zu vergüten hat, werden monatlich zu Beginn des Folgemonats abgerechnet. Es gelten mangels abweichender Vereinbarung im Einzelfall die Stundensätze der jeweils aktuellen Jahrespreisliste von INFORM. Fahrzeiten bei Vor-Ort-Einsätzen von Mitarbeitern von INFORM werden als Arbeitszeiten separat erfasst und dem Kunden nach Aufwand in Rechnung gestellt. Reisekosten und Reisespesen werden zusätzlich in tatsächlich angefallener Höhe in Rechnung gestellt.
- (5) Alle Vergütungsbestandteile verstehen sich zuzüglich der jeweils geltenden gesetzlichen Umsatzsteuer. Zahlungen sind vom Kunden innerhalb von 30 Kalendertagen ab Rechnungsdatum ohne Abzug zu leisten. Einwendungen gegen die Rechnung können vom Kunden nur innerhalb von 14 Kalendertagen ab Rechnungsdatum schriftlich mit Begründung geltend gemacht werden.
- (6) Kommt der Kunden mit der Zahlung der Vergütung in Verzug, so ist INFORM nach vorheriger Mahnung und angemessener Nachfristsetzung (unter Androhung der ansonsten erfolgenden Sperrung) berechtigt, den Zugang des Kunden zur Cloud-Oberfläche der Software und den Zugriff des Kunden auf seine Transaktionsdaten bis zum vollständigen Ausgleich sämtlicher offenen und fälligen Rechnungen zu sperren. Weitergehende Rechte von INFORM aufgrund des Zahlungsverzugs (insbesondere zu einer außerordentlichen Kündigung des Vertrages) bleiben unberührt.

§ 13 Schlussbestimmungen

- (1) Stimmt der Kunde einer Nennung als Referenzkunde zu, ist INFORM zur Veröffentlichung von Logos, Marken und Namen des Kunden in Referenzlisten und Fachartikeln (in Print- und Online-Format) berechtigt, ggf. in Verbindung mit inhaltlich abgestimmten Stellungnahmen (z.B. Pressemitteilungen). Diese Zustimmung kann jederzeit schriftlich oder per E-Mail an cloud-support@inform-software.com widerrufen werden.
- (2) Änderungen und Ergänzungen des Vertrages bedürfen zu ihrer Wirksamkeit der Schriftform. Die Aufhebung dieses Schriftformerfordernisses bedarf ebenfalls der Schriftform. Zur Wahrung der Schriftform nach diesem Vertrag genügt die Übermittlung per Fax (nicht jedoch per E-Mail, soweit in diesem Vertrag nicht anders angegeben).
- (3) Sollte eine Bestimmung dieses Vertrages unwirksam oder nicht durchsetzbar sein oder werden, so wird hiervon die Wirksamkeit der übrigen Bestimmungen nicht berührt. Die unwirksame bzw. nicht durchsetzbare Bestimmung wird von den Vertragspartnern einvernehmlich durch eine wirtschaftlich möglichst gleichwertige Vorschrift ersetzt. Entsprechendes gilt für Vertragslücken.
- (4) Der Kunde kann die Rechte und Pflichten aus diesem Vertrag nur nach vorheriger schriftlicher Zustimmung von INFORM auf einen Dritten übertragen.
- (5) INFORM hält sich selbstverständlich an die Anforderungen des deutschen Mindestlohngesetzes (MiLoG) und verpflichtet sich gegenüber ihren Kunden, diese Verpflichtungen an ihre Unteraufnehmer weiterzugeben und deren Einhaltung gegebenenfalls nachweisen zu lassen.
- (6) Diese Vereinbarung unterliegt ausschließlich dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Ausschließlicher Gerichtsstand für alle sich aus diesem Vertragsverhältnis ergebenden Streitigkeiten ist Aachen.

Anhang A - Technische Voraussetzungen

Die folgenden technischen Voraussetzungen sind für die Nutzung der Software vom Kunden einzuhalten bzw. zu schaffen und während der Vertragslaufzeit aufrechtzuerhalten:

1. Unterstützte Browser

Für den Zugriff auf die Benutzeroberfläche der Software empfehlen wir die Verwendung der folgenden Browser:

- Mozilla Firefox,
- Google Chrome,
- Microsoft Internet Explorer,
- Microsoft Edge oder
- Apple Safari

in der jeweils neuesten Version. Grundsätzlich nicht unterstützt werden Browser-Versionen, die vom Browser-Hersteller nicht mehr supportet werden.

In der Konfiguration muss die Ausführung von JavaScript sowie das Einblenden von Pop-Up-Fenstern erlaubt sein und bei der Verwendung des Internet Explorers muss zusätzlich der Kompatibilitätsmodus deaktiviert sein.

2. Monitor-Auflösung

Die Benutzeroberfläche der Software erfordert eine Mindestauflösung des Monitors von 1920 x 1080 Pixeln (HD-Format).

Bei geringerer Auflösung kann die vollständige Bedienbarkeit, z.B. durch Nicht-Darstellung von Bedienelementen, nicht gewährleistet werden.

3. Internet-Anbindung

Eine ausreichende Arbeitsgeschwindigkeit wird von vielen Faktoren beeinflusst. Neben der genutzten Infrastruktur (Festnetz/Mobil) für den Zugriff auf das Internet sind auch die jeweils übertragene Datenmenge und die Komplexität der Software, z.B. der zeitgleiche Systemzugriff verschiedener Nutzer, einfließende Parameter. Eine allgemeine Mindestanforderung an die Bandbreite einer Internetanbindung ist von daher kaum zu definieren.

Es wird daher zur störungsfreien Nutzung der Software eine verfügbare Download-Geschwindigkeit über Internet von 4 Mbit/s vorausgesetzt. Die Anforderung an die Upload-Geschwindigkeit beträgt 10% der Download-Geschwindigkeit.

4. Passwort Richtlinie

Aus Sicherheitsgründen muss jeder Nutzer der Software ein Passwort wählen, welches den üblichen Sicherheitskriterien entspricht. Entsprechende Regelwerke werden beim Setzen des Passwortes durch die Software vorgegeben. Der bewusste Umgang mit persönlichen und sicherheitsrelevanten Informationen liegt in der Verantwortung jedes einzelnen Benutzers.

Mehrfache vergebliche Rateversuche des Passwortes führen zur Sperrung des Nutzer-Kontos.

Anhang B – Service Level Agreement (SLA)

Dieses SLA regelt die Verfügbarkeit und Störungsbearbeitung der Software.

A. Servicezeiten

Die Servicezeiten sind Montag bis Freitag zwischen 8:30 und 16:30 Uhr, ausgenommen gesetzliche oder unternehmensweite Feiertage, sowie dem 24. und 31. Dezember eines Jahres.

In der Enterprise Edition können die Servicezeiten durch Hinzubuchen eines entsprechenden Zusatzpaketes bis zu einem 24/7-Service (24 Stunden an 7 Tagen die Woche) ausgebaut werden. Angaben zur gebuchten Edition und zu den gebuchten Zusatzpaketen finden sich in der Bestellbestätigung und auf der Benutzeroberfläche der Software, wobei Vertragsinformationen nur für die Benutzerrolle „Firmenadmin“ einsehbar sind.

B. Verfügbarkeit

INFORM gewährleistet eine Verfügbarkeit der Software (inklusive des Zugriffs auf die vom Kunden gespeicherten Transaktionsdaten) am Ausgang des von INFORM beauftragten Rechenzentrums von 99% im Kalenderjahresmittel. Nichtverfügbarkeit ist anzunehmen, wenn die Software aufgrund von Umständen, die im Verantwortungsbereich von INFORM liegen, dem Kunden nicht zur Verfügung steht. Nichtverfügbarkeit ist insbesondere nicht anzunehmen, wenn die Software aufgrund von

- Fehlbedienung oder vertragswidriger Nutzung des Kunden,
- geplanten und angekündigten Wartungsarbeiten,
- technischen Problemen außerhalb des Einflussbereichs von INFORM oder
- höherer Gewalt

nicht erreichbar ist.

INFORM wird geplante Wartungsarbeiten möglichst außerhalb der Servicezeiten durchführen und so rechtzeitig terminieren und dem Kunden per E-Mail ankündigen, dass diese den Kunden so wenig wie möglich beeinträchtigen. Insgesamt darf die Dauer geplanter Wartungsarbeiten 10 Stunden im Monat nicht überschreiten.

INFORM kann den Zugang des Kunden zeitweise beschränken, sofern die Sicherheit des Netzbetriebes, die Aufrechterhaltung der Netzintegrität, die Vermeidung schwerwiegender Störungen des Netzes, der Software und/oder der gespeicherten Kundendaten dies erfordern. INFORM wird bei einer solchen Entscheidung auf die berechtigten Interessen des Kunden angemessen Rücksicht nehmen, den Kunden über die getroffenen Maßnahmen unverzüglich unterrichten und alles Zumutbare unternehmen, um die Zugangsbeschränkung so schnell wie möglich wieder aufzuheben.

C. Störungsbeseitigung

Kommunikation

Die gesamte Kommunikation bei der Störungsbearbeitung erfolgt zwischen dem Kunden-Administrator (Benutzerrolle „Admin“) oder seinem Stellvertreter (als *Single Point Of Contact* auf Seiten des Kunden) und dem Support-Team der INFORM, erreichbar über die Service-E-Mail cloud-support@inform-software.com.

In der Enterprise Edition steht dem Kunden-Administrator zusätzlich auch die telefonische Service Hotline zur Verfügung. Zur Service Hotline gelten die gleichen Bedingungen bzgl. Servicezeiten und Service Level, wie für die Service-Email.

Service Level

Jeder gemeldeten Störung wird durch INFORM ein Service Level zugeordnet. Dieser ist definiert über die Schwere und Dringlichkeit der jeweiligen Auswirkungen. Eine individuelle und nicht automatisierte Reaktion auf eine Störungsmeldung erfolgt innerhalb der Servicezeit.

Störungs- klasse	angestrebte Lösungszeit nach Reaktion	Beschreibung
1	8 Stunden (innerhalb der Servicezeit)	Totalausfall, Nichterreichbarkeit
2	2 INFORM-Geschäftstage	Ausfall von Teilfunktionen z.B. Anfragen für Zeitfensterbuchungen werden durch die Software nicht beantwortet
3	1 Geschäftswoche	eingeschränkte Bedienbarkeit z.B. Stammdaten können nicht gepflegt werden
4	nach Ankündigung	leicht eingeschränkte Bedienbarkeit z.B. falsche Farbgebung oder Beschriftung

Erfolgt die Störungsmeldung des Kunden außerhalb der Servicezeiten, beginnen die Messung der Reaktions- und Behebungszeiten mit Beginn der Servicezeit des nächsten Arbeitstages. Erfolgt die Störungsmeldung des Kunden innerhalb der Servicezeiten, so läuft eine am Ende der Servicezeit dieses Tages noch nicht abgelaufene Rest-Reaktions- bzw. Rest-Lösungszeit ab dem Beginn der Servicezeit des nächsten Arbeitstages weiter.

Störungen dürfen nur durch den hierzu autorisierten Ansprechpartner des Kunden (Admin oder dessen Stellvertreter) an INFORM gemeldet werden; dieser fungiert gegenüber INFORM als *Single Point Of Contact*. Der Ansprechpartner des Kunden muss qualifiziert und im Umgang mit der Software vertraut sein.

Die Parteien werden ordnungsgemäß gemeldete Störungen einvernehmlich einer der beschriebenen Störungsklassen zuordnen. Für den Fall, dass die Parteien sich nicht auf eine Störungsklasse einigen können, erfolgt die verbindliche Klassifizierung durch INFORM unter angemessener Berücksichtigung der Interessen des Kunden.

Die angestrebten Lösungszeiten beginnen nicht vor ordnungsgemäßer und vollständiger Meldung der Störung (s.u.) durch den Kunden und Überlassung aller notwendigen und nützlichen Dokumente, Informationen und Daten an INFORM, die mit der Störung in Zusammenhang stehen und die INFORM eine Analyse und Reproduktion der gemeldeten Störung ermöglichen. Zeiträume, in denen INFORM aus Gründen, die nicht aus ihrem eigenen Verantwortungsbereich stammen, an der Erbringung von Supportleistungen gehindert ist und/ oder in denen INFORM auf die Erbringung von notwendigen Mitwirkungsleistungen (s.u.) oder das Treffen notwendiger Entscheidungen durch den Kunden wartet, bleiben bei der Berechnung der angestrebten Lösungszeiten außer Betracht.

Vollständige Störungsmeldung

Eine Störungsmeldung muss vollständig sein. Im Folgenden werden die benötigten Informationen gelistet, die bei Verfügbarkeit und Relevanz übermittelt werden müssen.

Im Betreff der E-Mail:

- vorgeschlagene Störungsklasse
- Kundenname und Standort
- Schlagworte bzgl. der Störung.

Im Text der E-Mail wird eine kurze, prägnante Beschreibung der Störung erwartet mit folgenden Details:

- Einen Screenshot mit dem kompletten Bildschirminhalt. Wichtige Punkte sollten markiert sein.
- Exakter Zeitpunkt des Auftretens der Störung bzw. bei mehrfachen oder Andauerndem Auftreten
 - Erstes Auftreten der Störung bzw.
 - Häufigkeit der Störung
- Störungsablauf
 - Schritt für Schritt Beschreibung
 - Erwartetes (normales) Verhalten
- Beispiele mit zugehörigen Identifikationen. z.B. UserID, Auftragsnummer, usw.

Mitwirkungspflicht

Um Auswirkungen von Störungen zu minimieren hat der Kunde folgende Pflichten:

- Der Kunde erstellt und pflegt für unterschiedliche Störungs-Szenarien Notfallpläne.
- Der Kunde pflegt Stammdaten und Konfigurationen. Er stellt sicher, dass sie stets vollständig und korrekt sind, sowie keine logischen Inkonsistenzen enthalten.
- Der Kunde stellt sicher, dass alle Eingaben in die Anwendungen vollständig und korrekt sind, sowie keine logischen Inkonsistenzen enthalten.
- Der Kunde meldet auftretende Störungen unverzüglich an die Service-E-Mail.
- Der Kunde unterstützt INFORM bei der Störungsbehebung und -analyse im Rahmen des Zumutbaren.

Anhang C – Auftragsverarbeitung

Präambel

Die nachfolgenden Standardvertragsklauseln zur Auftragsverarbeitung (im Folgenden „AVV“) wurden die EU-Kommission aufgrund Art. 28 Abs. 7 DSGVO erlassen und gelten für die INFORM (im Folgenden „Auftragsverarbeiter(in)“) und den Kunden (im Folgenden „Verantwortliche(r)“), jedoch nicht unmittelbar für dessen Mitarbeiter oder sonstige Dritte, die der Kunde in die Nutzung der Software einbindet.

Im Falle von Widersprüchen zwischen dieser AVV und sonstigen Regelungen der AGB haben die AVV Vorrang.

Standardvertragsklauseln

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

- a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.
- b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 zu gewährleisten.
- c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.
- d) Die Anhänge I bis IV sind Bestandteil der Klauseln.
- e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.
- f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

- a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.
- b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3

Auslegung

- a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
- b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.
- c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4 **Vorrang**

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 – fakultativ **Kopplungsklausel**

- a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.
- b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.
- c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II **PFLICHTEN DER PARTEIEN**

Klausel 6 **Beschreibung der Verarbeitung**

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7 **Pflichten der Parteien**

7.1. Weisungen

- a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren. Klarstellend sind die Parteien darüber einig, dass Weisungen des Verantwortlichen zu einer Leistungsänderung im Rahmen des Hauptvertrages führen können.
- b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung

- a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes

personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

- b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogener Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

- a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
- b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
- c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.
- d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
- e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG: Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste als Anhang IV aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens vier Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

- a) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.
- b) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.
- c) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen

Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

- d) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. Internationale Datenübermittlungen

- a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.
- b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

- a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.
- b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.
- c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:
- 1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
 - 2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
 - 3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
 - 4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.
- d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

- a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);
- b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679] in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:
 - 1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - 2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - 3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

- c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679] , die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

- a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
- b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
- c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679] oder zu unterstützen.

ABSCHNITT III SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

- a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.
- b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
 - 1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
 - 2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;
 - 3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.
- c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.
- d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I
Liste der Parteien

Verantwortliche(r):

Kunde

Auftragsverarbeiterin:

*INFORM Institut für Operations Research und Management GmbH
Pascalstraße 35, 52076 Aachen, Deutschland*

*Datenschutzbeauftragter: Dr. Oliver Meyer-van Raay
V-Formation GmbH, Stephaniensstrasse 18, 76133 Karlsruhe, Deutschland
Tel.: +49 721 17029034, E-Mail: om@v-formation.gmbh*

ANHANG II

Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:
Arbeitnehmer, Zeitarbeitskräfte, Auszubildende, Hilfskräfte, Kunden, Dienstleister

Kategorien personenbezogener Daten, die verarbeitet werden:

<i>Nutzer:</i>	<i>Allgemeine Personendaten (Name, Vorname, Sprache) Kennnummer (UserCode, Password) Organisationsdaten (Organisation, Rolle, Qualifikation) Kontaktdaten (Email-Adresse, Telefon)</i>
<i>Fahrer:</i>	<i>Allgemeine Personendaten (Name, Vorname, Sprache) Organisationsdaten (Organisation, Rolle, Qualifikation) Kontaktdaten (Email-Adresse, Telefon)</i>

Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen:

Es werden keine sensiblen Daten, gem. DSGVO, verarbeitet

Art der Verarbeitung:

Dauerhafte Verarbeitung der Daten und Betrieb der Software in einem Rechenzentrum. Geplante und ungeplante Wartung im Fehlerfall und Softwarepflege oder die Unterstützung des Verantwortlichen legen pro Einzelfall die Art der Datenverarbeitung im Detail fest.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

Bereitstellung der Softwarefunktionalität über das Internet, geplante und ungeplante Wartung im Fehlerfall, Softwarepflege, Unterstützung des Verantwortlichen.

Dauer der Verarbeitung:

Die Verarbeitung der Daten und der Betrieb der Software im Rechenzentrum endet mit dem Vertragsende. Bei Fehlermeldungen oder durchzuführender Softwarepflege wird über Fernwartung auf das beim Hosting-Dienstleister (Unterauftragsverarbeiter) installierte Softwaresystem zugegriffen. Hierbei sind die Datenbestände, inkl. der personenbezogenen Daten der Nutzer und der Fahrer, für den besonders sensibilisierten und geschulten INFORM-Mitarbeiter zu sehen. Die Dauer der Verarbeitung richtet sich nach der Dauer der Fehlerbehebung.

Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben. *Vgl insoweit Anhang IV.*

ANHANG III

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

ERLÄUTERUNG:

Die technischen und organisatorischen Maßnahmen müssen konkret beschrieben werden; eine allgemeine Beschreibung ist nicht ausreichend.

Beschreibung der von dem/den Auftragsverarbeiter ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen Beispiele für mögliche Maßnahmen:

Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten

Maßnahmen zur fortwährenden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Maßnahmen zur Identifizierung und Autorisierung der Nutzer Maßnahmen zum Schutz der Daten während der Übermittlung Maßnahmen zum Schutz der Daten während der Speicherung

Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen

Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit

Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten Maßnahmen zur Gewährleistung der Datenminimierung

Maßnahmen zur Gewährleistung der Datenqualität

Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung Maßnahmen zur Gewährleistung der Rechenschaftspflicht

Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-) Auftragsverarbeiter zur Unterstützung des Verantwortlichen ergreifen muss.

Ergänzend gelten die Sicherheits-Zertifizierungen und technischen und organisatorischen Sicherheitsmaßnahmen der eingesetzten Unterauftragsverarbeiter aus Anhang IV.

Sicherheits-Zertifikate der INFORM, GB60 Industrielogistik



ISO 27001 zertifiziert durch
den TÜV Rheinland
Ergebnis unter
https://www.certipedia.com/quality_marks/9000021449



Das Ergebnis ist ausschließlich über das ENX-Portal abrufbar:
<https://portal.enx.com/en-US/TISAX/tisaxassessmentresults/>

Technische und organisatorische Maßnahmen der INFORM (v5, Stand Feb 2022)

1 Maßnahmen zu Gewährleistung der Vertraulichkeit

1.1 Zutrittskontrolle

Zutrittskontrolle Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.	vor- handen ja
Elektronische Zutrittscodekarten/Zutrittstransponder	x
Zweifaktorauthentifizierung Rechenzentren	x
Zentraler Empfang	x
Zutrittsberechtigungskonzept	x
Videüberwachung	x
Alarmanlage	x
Schlüsselregelung	x
Sicherheitsbereiche mit unterschiedlichen Zutrittsberechtigungen	x
Begleitung von Besucherzutritten durch eigene Mitarbeiter	x
Sicherung auch außerhalb der Arbeitszeit durch Werkschutz	x
Abgestufte Sicherheitsbereiche und kontrollierter Zutritt	x
Gesicherter Eingang für An- und Ablieferung	x
Spezialverglasung (Erdgeschoß)	x
Server in zutrittsgeschützten Rechenzentren	x
Aufbewahrung der Datenträger unter Verschluss bzw. in abgeschlossenen Räumen	x
Datensicherungen in zutrittsgeschützten Rechenzentren	x
Anweisung zur Ausgabe von Zutrittscodekarten/Zutrittstransponder	x

1.2 Zugangskontrolle

Zugangskontrolle Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.	vor- handen ja
Verschluss von Datenverarbeitungsanlagen	x
Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen	x
Verwendung von individuellen Passwörtern	x
Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern	x
Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)	x
▪ Mindestens zehn Zeichen	x
▪ Groß- und Kleinschreibung, Sonderzeichen, Zahl (davon mind. vier Kriterien)	x
▪ Wechsel des Passworts nach max. 180 Tagen	x
▪ Verhinderung von Trivialpasswörtern	x
▪ Passworthistorie (keine erneute Verwendung der letzten 10 Passwörter)	x
▪ Überprüfung von AD Passwörtern auf Kompromittierung	x
Hashing von gespeicherten Passwörtern	x
Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern	x
Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern	x
Prozess zum Rechteentzug bei Austritt von Mitarbeitern	x
Verpflichtung auf Vertraulichkeit	x
Zertifizierte Vernichtung von Datenträgern	x
Absicherung extern erreichbarer Services mittels Zweifaktorauthentifizierung	x
Aufbewahrung verkörperter personenbezogener Daten in verschließbaren Sicherheitsschränken	x

1.3 Zugriffskontrolle

Zugriffskontrolle Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.	vorhanden ja
Festlegung der Zugriffsberechtigung, Berechtigungskonzept	x
Festlegung der Befugnis zur Dateneingabe, -änderung, -löschung	x
Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch)	x
Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)	x
Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken	x
Zeitliche Begrenzung von Zugriffsmöglichkeiten	x
Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)	x
Werden entsprechende Sicherheitssysteme (Software/Hardware) eingesetzt?	
▪ Virens Scanner	x
▪ Firewalls	x
▪ SPAM-Filter	x
▪ Intrusionprevention (IPS)	x
▪ Intrusiondetection (IDS)	x
Verschlüsselte Speicherung der Daten	
▪ Verwendete Verschlüsselungsalgorithmen:	
▫ AES (128/256 bit)	x
▫ 3DES	x
▫ RSA (1024/2048 bit)	x
▪ Verwendete Hash-Funktion:	
▫ SHA2 (256, 384, 512 bit)	x
▫ SHA3	x
▫ bcrypt	x

1.4 Auftragskontrolle

Auftragskontrolle Es ist sicherzustellen, dass Daten die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftraggebers verarbeitet werden.	vorhanden ja
Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)	x
Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)	x
Vorabkontrollen beim Auftragnehmer vor Vertragsbeginn	x
Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (Während Vertragsdauer)	x
Überprüfung des Datensicherheitskonzepts beim Auftragnehmer (sofern vorgelegt)	x
Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer (sofern vorgelegt)	x
Erteilung von Weisungen zur Verbesserung des Datenschutzes ggü. Auftragnehmer	x
Etablierter Meldeprozess bei schwerwiegenden Betriebsstörungen und Verdacht auf Datenschutzverletzungen	x

1.5 Trennungskontrolle

Trennungskontrolle Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.	vorhanden ja
Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)	x
Datenseparierung bei Datenbanken	x
Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)	x
Verarbeitung der Daten des Auftraggebers und anderer Kunden von unterschiedlichen Mitarbeitern des Auftragnehmers	x
Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt	x
Funktionstrennung	x
Trennung von Entwicklungs-, Test- und Produktivsystem	x

2 Maßnahmen zur Gewährleistung der Integrität

2.1 Weitergabekontrolle

Weitergabekontrolle Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, sowie deren Kontrolle.	vor- handen ja
Welche Versendungsart der Daten besteht zwischen Auftraggeber und Dritten?	
▪ Terminalserver-Verbindungen (mind. 128 Bit verschlüsselt)	x
▪ VPN-Verbindung (IP-Sec)	x
▪ E-Mail Versand mit verschlüsselten ZIP-Dateien	x
▪ Datenaustausch über https-Verbindung	x
▫ verwendetes Verschlüsselungsprotokoll:	
- TLS 1.2	x
Gesicherter Eingang für An- und Ablieferung	x
Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle	x
Verschlüsselung vertraulicher Datenträger	x
Verschlüsselung von Laptopfestplatten	x
Verschlüsselung mobiler Datenträger	x
Datenträgerentsorgung - Sichere Löschung von Datenträgern:	
▪ Physikalische Zerstörung (z.B. Shredder bei Partikelgrößen bis max. 1000 Quadrat-Millimeter)	x
Papierentsorgung: Sicheres Vernichten von Papierdokumenten:	
▪ Verschlussene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleister	x
▪ Shredder gem. DIN 66399	x

2.2 Eingabekontrolle

Eingabekontrolle Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten	vor- handen ja
Festlegung von Benutzerberechtigungen (Profile)	x
Lesen, Ändern, Löschen	x
Teilzugriff auf Daten bzw. Funktionen	x
Feldzugriff bei Datenbanken	x
Organisatorische Festlegung von Eingabezuständigkeiten	x
Protokollierung von Eingaben/Löschungen	x
Verpflichtung zur Vertraulichkeit	x
Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke	x

3 Maßnahmen zur Gewährleistung der Verfügbarkeit

3.1 Verfügbarkeitskontrolle

Verfügbarkeitskontrolle Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.	vorhanden ja
Datensicherungs- und Backupkonzepte	x
Durchführung der Datensicherungs- und Backupkonzepte	x
Zutrittsbegrenzung in Serverräumen auf notwendiges Personal	x
Brandmeldeanlagen in Serverräumen	x
Rauchmelder in Serverräumen	x
Wasserlose Brandbekämpfungssysteme in Serverräumen	x
Klimatisierte Serverräume	x
Blitz-/ Überspannungsschutz	x
Wassersensoren in Serverräumen	x
Serverräume in separaten Brandabschnitt	x
Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitt	x
Gewährleistung der technischen Lesbarkeit von Backup Speichermedien für die Zukunft	x
Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)	x
CO2 Feuerlöscher in unmittelbarer Nähe der Serverräume	x
USV-Anlage (Unterbrechungsfreie Stromversorgung)	x

4 Maßnahmen zur Gewährleistung der Belastbarkeit

4.1 Widerstandsfähigkeit- und Ausfallsicherheitskontrolle

Widerstandsfähigkeit- und Ausfallsicherheitskontrolle Systeme müssen die Fähigkeit besitzen mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.	vorhanden ja
Redundante Stromversorgung	x
Redundante Datenanbindung	x
Redundante Klimatisierung	x
Redundante Brandbekämpfung	x
Festplattenspiegelung	x
Einsatz einer hochverfügbaren SAN-Lösung	x
Loadbalancer	x
Datenspeicherung auf RAID-Systemen (RAID 1 und höher)	x
Abgrenzung kritischer Komponenten	x
Trennung des internen Netzes von öffentlichen Netzen mittels demilitarisierter Zonen (DMZ)	x
Durchführung von Penetrationstests (für Anwendungs- und Entwicklungssysteme)	x
Überwachung kritischer Systeme durch einen Security Operating Center (SOC)	x
Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)	x
Unverzögliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates	
<ul style="list-style-type: none"> ▪ Identifikation der verschiedenen Geräte, aus denen sich das Netzwerk zusammensetzt, und Bestimmung ihrer Hardware-Version sowie ihrer aktuellen Software- und Firmware-Versionen. 	x
<ul style="list-style-type: none"> ▪ Kommunikationskanal mit den Herstellern, um sich über neue Updates und Patches zu informieren, die für die im Besitz befindlichen Geräte freigegeben wurden. 	x
<ul style="list-style-type: none"> ▪ Definition von Zeiträumen, in denen die Updates implementiert werden sollen (z. B. Perioden niedrigerer Operationen, Wartungszeiten usw.). 	x
<ul style="list-style-type: none"> ▪ Verwendung redundanter Systeme, um den Betrieb aufrecht zu erhalten, während die Hauptgeräte aktualisiert werden. 	x
<ul style="list-style-type: none"> ▪ Bereitstellung von Updates / Patches 	x

<ul style="list-style-type: none"> ▪ Festlegung einer Testperiode, um die korrekte Implementierung des Updates zu überprüfen und sicherzustellen, dass die Operationen mit den neuen Updates weiterhin reibungslos ablaufen. 	x
Sicherheit wird während der Konzeptionsphase der Systeme als Hauptbetrachtung mit umfasst.	
<ul style="list-style-type: none"> ▪ Definition von Sicherheitsmaßnahmen zum Schutz und zur Validierung der Kommunikation zwischen Systemkomponenten 	x
<ul style="list-style-type: none"> ▪ Begrenzung von Berechtigungen auf Bedarfsnotwendigkeit. 	x
<ul style="list-style-type: none"> ▪ Widerruf vorübergehender Privilegien, sobald sie nicht mehr erforderlich sind. 	x
<ul style="list-style-type: none"> ▪ Externe Auftragnehmer und Wartungspersonal erhalten einen spezifischen Zugang, der nur während des Eingriffs aktiv und den Rest der Zeit deaktiviert ist. 	x
<ul style="list-style-type: none"> ▪ Bei der Definition von Netzwerkkommunikationstechnologien und Architektur wird auch die Interoperabilität mit einbezogen. 	x
<ul style="list-style-type: none"> ▪ Identifizierung von Systemen, Infrastrukturen und Umgebungen, die eine Kommunikation mit anderen Systemen (intern oder extern) erfordern, oder die diese Kommunikation in naher Zukunft erfordern (unter Berücksichtigung des Lebenszyklus der beteiligten Geräte). 	x
<ul style="list-style-type: none"> ▪ Auswahl von Kommunikations-Protokollen, die mit den identifizierten Systemen und den Systemen der anderen Organisationen oder Umgebungen kompatibel sind. 	x
<ul style="list-style-type: none"> ▪ Kollaborative Umgebungen, die den Austausch von Informationen zwischen verschiedenen Parteien ermöglichen. 	x
<ul style="list-style-type: none"> ▪ Identifizierung von potentiellen Hauptangriffsvektoren. 	x
Periodische Sicherheitstrainings und Sensibilisierungskampagnen innerhalb der Organisation.	
<ul style="list-style-type: none"> ▪ Sensibilisierungskampagnen, um die Benutzer über die Sicherheitskonzepte zu informieren, die sowohl für konkrete Systeme als auch für traditionelle IT-Systeme spezifisch sind. 	x
<ul style="list-style-type: none"> ▪ Spezielles Sicherheitstraining, um zu lehren, wie man Sicherheitsmaßnahmen und Verhaltensweisen auf die täglichen Prozesse mit möglichst geringem Aufwand anwendet. 	x
<ul style="list-style-type: none"> ▪ Anlassbezogene Warnung vor Bedrohungen und Risiken. 	x

5 Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Kontrollverfahren

Kontrollverfahren	vor-
Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren	handen ja
Verarbeitungsverzeichnisse werden regelmäßig/anlassbezogen aktualisiert	x
Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten	x
Meldung neuer/veränderter Datenverarbeitungsverfahren an den IT-Sicherheitsbeauftragten (CISO)	x
Es werden datenschutzfreundliche Voreinstellungen gewählt	x
Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen	x
Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt	x

ANHANG IV
Liste der Unterauftragsverarbeiter

Der Parteien erkennen bei Abschluss dieses Vertrags die Inanspruchnahme folgender Unterauftragsverarbeiter an:

1. Name: *Microsoft Ireland Operations Ltd*
Anschrift: *Microsoft Plc,
Leopardstown South County Business Park Dublin 18
D18 P521 Ireland*

Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden):

*INFORM-interne Kommunikationsplattform MS Office 365 E5,
u.a. mit Teams inkl. Telefonie, Outlook, Sharepoint und OneDrive.*

2. Name: *Amazon Web Services EMEA SARL*
Anschrift: *38 avenue John F. Kennedy
L-1855 Luxemburg*

Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden):

*Bereitstellung und Betrieb des Rechenzentrums für
die Software SYNCROTESS*