Allgemeine Einkaufsbedingungen
für die Lieferung von Produkten und Waren sowie für die Erbringung von Dienst- und Werkleistungen – Version Dec2022

der Raiffeisen Informatik Consulting GmbH

1020 Wien, Lilienbrunngasse 7-9, nachfolgend „RI-C“ genannt

1. Geltungsbereich und Gegenstand dieser Allgemeinen Einkaufsbedingungen (nachfolgend AEB genannt)

1 Gegenstand dieser AEB ist die Regelung der Rahmenbedingungen sämtlicher zwischen der RI-C und dem LIEFERANTEN abgeschlossener Rechtsgeschäfte. Dies betrifft insbesondere alle Bestellungen für die Lieferung von Produkten und Waren, v.a. Software-Produkte und die dazu gehörige Software-Wartung, sowie auch die Erbringung von Dienst- und Werkleistungen.

1.1. Durch die Annahme einer auf diese AEB bezugnehmenden Bestellung durch den LIEFERANTEN werden die AEB in ihrer jeweils gültigen Version automatisch Bestandteil des entsprechenden Rechtsgeschäfts. Darüber hinaus gelten die AEB ab deren ersten Anwendung auch für jede weitere Art der Zusammenarbeit, Abstimmung, Informationsaustausch etc. zwischen den beiden Parteien (das gilt insbesondere aber nicht ausschließlich für Fragen der Haftung und Geheimhaltung), auch ohne direkten Zusammenhang mit einem konkreten Rechtsgeschäft bzw. Bestellung.
Die AEB in ihrer jeweils aktuell gültigen Fassung sind einzusehen auf der Homepage der RI-C oder können dem Lieferanten auf dessen Anfrage hin per E-Mail zur Ansicht übermittelt werden.

1.2. Bestellungen im Sinne von Punkt 1.1 und 2.1 können in oder ohne Verbindung mit dem Abschluss von dazugehörigen Einzelverträgen erfolgen. Diese AEB gelten dabei auch für sämtliche dieser Einzelverträge, auch wenn in diesen nicht explizit darauf verwiesen wird, es sei denn, dass die Anwendung dieser AEB darin ausdrücklich abbedungen wurde.

1.3. Vereinbarungen zwischen dem LIEFERANTEN und der RI-C gelten in nachstehender Reihenfolge, beginnend mit der höchsten Priorität:

i. Einzelverträge (Bestellungen) der RI-C

ii. Rahmenverträge

iii. Gegenständliche AEB

iv. Statements of Work oder ähnlich geartete Dokumente wie z.B. Leistungsbeschreibungen und Produktspezifikationen des Lieferanten

v. Auftragsverarbeitervereinbarung

1.4. Rechtliche und kommerzielle Bedingungen in Angeboten oder Standarddokumenten des Lieferanten (Statements of Work, Produktspezifikationen, etc.) kommen nur in jenem Ausmaß zur Anwendung als auf diese in der Bestellung und/oder im Einzelvertrag explizit verwiesen wird. Im Falle von Widersprüchen zwischen solchen Bedingungen und den Bedingungen der oben unter (i) bis (iv) angeführten Dokumente gehen jedenfalls die oben genannten Dokumente in der festgelegten Geltungsreihenfolge vor. Wie auch immer geartete Geschäftsbedingungen des LIEFERANTEN werden ausgeschlossen.

1.5. Mit der RI-C verbundene Unternehmen aus der Raiffeisen Gruppe („GRUPPENUNTERNEHMEN“) sind berechtigt, ebenfalls diese AEB zu verwenden, indem sie eine Bestellung unter Bezugnahme auf diese AEB durchführen. Darüber hinaus gelten vom LIEFERANTEN an die RI-C gerichtete Angebote stets auch als an alle GRUPPENUNTERNEHMEN gerichtet, sodass diese ein entsprechendes Angebot des LIEFERANTEN im eigenen Namen und auf eigene Rechnung annehmen können. Mit Annahme bzw. Durchführung einer Bestellung des GRUPPENUNTERNEHMENS durch den LIEFERANTEN stimmt der LIEFERANT der Geltung dieser AEB zu. Im Folgenden ist unter „RI-C“ daher sinngemäß „RI-C bzw. deren verbundene GRUPPENUNTERNEHMEN“ zu verstehen.

2. Bestellungen

2.1. Es sind ausnahmslos schriftliche Bestellungen, welche erkennbar von der RI-C ausgestellt wurden, verbindlich. Für Bestellungen von GRUPPENUNTERNEHMEN können allenfalls jedoch andere Regelungen zur Anwendung gelangen.

2.2. Mündliche Bestellungen sind nicht verbindlich, und dürfen vom LIEFERANTEN mit dem Verweis auf diese AEB nicht angenommen werden.

2.3. Lieferungen und/oder Leistungen, die vom LIEFERANTEN aufgrund der Annahme einer den Formvorschriften des Punktes 3.1 widersprechenden Bestellung erbracht werden, sind im Falle einer entsprechenden Aufforderung der RI-C auf Kosten und Gefahr des LIEFERANTEN rückabzuwickeln. Der LIEFERANT hat der RI-C insbesondere sämtliche aus einer solchen Bestellung erhaltene Zahlungen spesen- und abzugsfrei rück zu erstatten und in Abstimmung mit der RI-C den für die RI-C kostenfreien Rücktransport bereits gelieferter Waren und Produkte zu organisieren.

3. Preise und Angebote

3.1. Alle Angebote des LIEFERANTEN an die RI-C sind - soweit nichts anderes vereinbart wurde - per E-Mail an "" zu übermitteln. Im Zweifelsfall wird davon ausgegangen, dass die im Angebot angeführten Preise und sonstige Konditionen noch keine Sonderkonditionen für die RI-C darstellen und somit noch einer finalen Diskussion und Verhandlung unterliegen.

3.2. Die Gültigkeitsdauer von Angeboten und Preislisten muss mindestens drei Monate betragen. Die Erweiterung einer Preisliste um zusätzliche Produkte oder Leistungen bei gleicher oder längerer Gültigkeitsdauer ist möglich.

3.3. Bestellungen der RI-C können unter Bezugnahme auf Preislisten, individuelle Angebote oder dazugehörige Rahmen- oder Einzelverträge durchgeführt werden. Allfällige Steuern, Abgaben und Gebühren, sowie sonstige Kosten, die im Rahmen der Leistungserbringung anfallen können, wie Honorarsätze und Kosten für Aufwendungen, Kilometergeld, Verbrauchsmaterialien, Verschleißteile etc. sind in allen Angeboten und Preislisten gesondert anzuführen. Sofern im Einzelfall schriftlich zwischen den Parteien nichts Anderweitiges vereinbart wird (Pauschalen o.ä.), sind alle sonstige Kosten (wie oben beschrieben) nach tatsächlichem Aufwand unter Vorlage aller dazugehörigen Belege abzurechnen, und im Wege der jeweiligen Bestellung ist nach Möglichkeit eine Obergrenze für solche Kosten zu vereinbaren.

3.4. Als Währung wird einheitlich EURO festgelegt, sollte im Einzelfall nichts Anderweitiges vereinbart sein.

4. Zahlungskonditionen und Rechnungen

4.1. Sofern nicht anders vereinbart, lauten die Zahlungskonditionen nach Wahl der RI-C entweder 45 Tage netto oder 30 Tage mit 3% Skonto.

4.2. Alle Rechnungen sind entweder per Post oder per E-Mail (buchaltung@ri-c.at) an die Buchhaltung der RI-C zu übermitteln.

4.3. Die Zahlungsfrist beginnt entweder nach vertragsgemäßer Leistungserfüllung oder (im Fall eines Abnahmeprozesses gemäß Punkt 7.) nach positiv erfolgter Abnahme durch die RI-C oder nach Eingang einer ordnungsgemäßen Rechnung im Sinne des nachfolgenden Punktes.

Maßgeblich für den Beginn der Zahlungsfrist ist dabei immer jenes der oben angeführten Ereignisse, welches im konkreten Fall als letztes eintritt.

Mit Erteilung des Überweisungsauftrages an die Bank spätestens am Fälligkeitstag gilt die Zahlung seitens der RI-C als rechtzeitig erfolgt. Allfällige Bankspesen der Empfängerbank sind vom LIEFERANTEN zu tragen.

4.4. Unbeschadet Punkt 4.3 können Zahlungen durch RI-C nur erfolgen, wenn die Rechnungen alle nachfolgend aufgelisteten Informationen beinhalten. Fehlt auch nur eine dieser Informationen gilt die Rechnung bzw. der Lieferschein jedenfalls als nicht ordnungsgemäß im Sinne von Punkt 4.3. und das Zahlungsziel verlängert sich (unbeschadet weiterer Konsequenzen, die in diesen AEB vorgesehen sind) automatisch bis 30 Tage nach Ausstellung eines ordnungsgemäßen

Lieferscheins und / oder Rechnung.

Erforderliche Informationen in Rechnungen des LIEFERANTEN:

- RI-C Bestellnummer/RI-C Vertragsnummer (falls vorhanden) und Bestelldatum
- Empfänger, ggf. Projekttitel lt. Bestellung
- Positionsnummer, Menge und Spezifikation, Mengeneinheit gem. Bestellung
- Ausreichender Hinweis auf die auf ggf. in der Lieferung enthaltene Speichermedien oder Geräte entfallende Vergütung gemäß § 42b UrhG
- Preise und Rabatte
- Abgenommener Arbeits-/Leistungsbericht falls es sich um Dienst- oder Werkleistungen handelt
- Umsatzsteueridentifikationsnummer (UID-Nr.) des LIEFERANTEN
- Vermerk, ob es sich um eine Teilrechnung oder eine Schlussrechnung handelt

4.5. Sämtliche Steuern (mit Ausnahme der Umsatzsteuer), Gebühren und Abgaben (insbesondere auch allfällige Bankspesen und –gebühren), welche in Angeboten, Preislisten oder Einzelverträgen entgegen Punkt 3.3 nicht explizit angeführt wurden, gehen zu Lasten des LIEFERANTEN.

4.6. Jegliche Indexanpassungen werden einvernehmlich ausgeschlossen, sofern im Einzelfall schriftlich zwischen den Parteien nichts Anderweitiges vereinbart wurde.

4.7. Die RI-C ist berechtigt, Zahlungsverpflichtungen gegenüber dem LIEFERANTEN mit Forderungen, die der RI-C ihm gegenüber zustehen, aufzurechnen. Bis zur vollständigen Behebung von Mängeln kann die RI-C die Zahlung des gesamten Rechnungsbetrages zurückhalten. Während der Gewährleistungsfrist kann die RI-C einen unverzinslichen Garantierückhalt bis zu 10 % der AUFTRAGSUMME vom Rechnungsbetrag einbehalten. Wird ein solches Zurückbehaltungsrecht ausgeübt, hemmt dies die Fristen gemäß Punkt 4.1.

4.8. Eine Zahlung seitens der RI-C bedeutet weder eine konkludente Anerkennung der Ordnungsmäßigkeit der Lieferungen und Leistungen des LIEFERANTEN noch einen wie auch immer gearteten Verzicht auf der RI-C zustehende Rechte, insbesondere aus Gewährleistung, Garantie oder Schadenersatz.

4.9. Forderungen des LIEFERANTEN gegenüber der RI-C aus Rechtsgeschäften, die auf diesen AEB basieren, dürfen ohne vorherige schriftliche Zustimmung der RI-C weder abgetreten noch verpfändet noch in sonstiger Weise auf Dritte übertragen werden. Für den Fall einer Zustimmung durch die RI-C hat der Lieferant eine Bearbeitungs- und Aufwandspauschale in Höhe von 2% der Gesamtforderungssumme an die RI-C zu bezahlen.

5. Lieferbestimmungen

5.1. Sofern anwendbar und im Einzelfall schriftlich zwischen den Parteien nichts Anderweitiges vereinbart wurde, erfolgen alle Lieferungen transportsicher verpackt und grundsätzlich frei Haus an den vereinbarten Lieferort (DDP gem. INCOTERMS 2010). Somit trägt der LIEFERANT sämtliche Transport-, Versicherungs-, Verpackungs- und sonstige Nebenkosten und Gebühren, welche im Zusammenhang mit der Anlieferung anfallen.

5.2. Der Gefahrenübergang wird – auch bei Versendung – mit Übergabe an die RI-C am vereinbarten Lieferort bewirkt. Im Lieferumfang sind den genannten Anforderungen genügende Lieferscheine enthalten, welche so an der Lieferung anzubringen sind, dass diese ohne Öffnen der Transportverpackung zugänglich sind.

6. Leistungserbringung

6.1. Der LIEFERANT ist grundsätzlich verpflichtet, alle von der RI-C bestellten Lieferungen und Leistungen selbst zu erbringen. Sollte das – aus welchem Grund auch immer – nicht möglich sein, ist der LIEFERANT berechtigt, die Bestellung auf eigene Kosten von hierfür geeigneten Dritten durchführen oder fertig stellen zu lassen. Der LIEFERANT ist jedoch verpflichtet die RI-C

frühestmöglich vorab hierüber zu informieren und deren nachweisliche Zustimmung einzuholen.

6.2. Der LIEFERANT unterliegt hinsichtlich Arbeitszeit, Arbeitsort und konkreter Durchführung der Tätigkeit keinen Weisungen der RI-C, hat jedoch die vorgegebenen Termine einzuhalten und haftet für die pünktliche und ordnungsgemäße Durchführung.

6.3. Der LIEFERANT erbringt Lieferungen und Leistungen grundsätzlich mit seinen eigenen Betriebsmitteln. Sofern der Zugang zum Computernetzwerk der RI-C notwendig, aber mit den Betriebsmitteln des LIEFERANTEN nicht möglich ist oder gestattet wird, stellt die RI-C die dazu notwendigen Betriebsmittel zur Verfügung.

6.4. Der LIEFERANT sichert zu, ausschließlich zuverlässige, fachlich ausreichend qualifizierte und persönlich geeignete Personen für die Erbringung von Lieferungen und Leistungen gegenüber der RI-C zum Einsatz zu bringen, deren Beschäftigungsverhältnis den jeweils geltenden österreichischen Arbeits- und Sozialrechtsvorschriften genügt. Für das Einhalten der geltenden Arbeitsschutzvorschriften, das zur Verfügung stellen geeigneter Schutzausrüstungen und die Unterweisung in die notwendigen Schutzmaßnahmen, ist ausschließlich der LIEFERANT verantwortlich.

6.5. Der LIEFERANT sichert zu, über alle für die von ihm angebotenen bzw. durchgeführten Lieferungen und Leistungen notwendigen Gewerbeberechtigungen zu verfügen und deren Verlust der RI-C unverzüglich schriftlich anzuzeigen, sowie die Leistungserbringung bis zu deren Wiedererlangen, unbeschadet allfälliger Ersatzansprüche der RI-C, einzustellen.

6.6. Falls es sich beim LIEFERANTEN um eine natürliche Person handelt, gilt folgendes: Der LIEFERANT sichert zu, zum Zeitpunkt des Zustandekommens des Rechtsgeschäftsabschlusses (Bestellannahme) und für die gesamte Dauer der Leistungserbringung hinsichtlich der von ihm für die RI-C erbrachten Leistungen der Versicherung nach dem GSVG zu unterliegen, was er durch Vorlage des aktuellen Zahlungsbeleges der Versicherungsbeiträge nachzuweisen hat. Verliert der LIEFERANT die GSVG-Versicherung, hat er der RI-C unverzüglich schriftlich darüber zu informieren und die Leistungserbringung bis zu deren Wiedererlangen einzustellen. Die RI-C ist daher nicht verpflichtet für die Anmeldung des LIEFERANTEN oder dessen Erfüllungsgehilfen bei den zuständigen Krankenkassen zu sorgen.

6.7. Der LIEFERANT verpflichtet sich, die in Beilage A angeführten Sicherheits- und Verhaltensregeln vollständig einzuhalten, und seinen Mitarbeitern und Erfüllungsgehilfen rechtzeitig vor deren Einsatz für die RI-C, für deren Beteiligungen bzw. deren verbundenen Unternehmen im Raiffeisen-Sektor, für deren Kunden oder für deren Partner, zur Kenntnis zu bringen. Darüber hinaus ist der LIEFERANT verpflichtet, sonstigen individuellen schriftlichen Anweisungen der RI-C betreffend technischer oder personenbezogener Sicherheit Folge zu leisten.

6.8. Der LIEFERANT ist nicht berechtigt, gegenüber Dritten Erklärungen oder Verpflichtungen im Namen der RI-C abzugeben oder einzugehen.

7. Abnahme

Sofern anwendbar und in Einzelverträgen keine anders lautenden Abnahmeregelungen vereinbart werden, kommen die nachfolgenden Klauseln zum Einsatz:

7.1. Insbesondere bei Programm- und System-Entwicklungsleistungen erfolgt grundsätzlich eine Abnahme (Zwischen- oder Endabnahme) erst nach einem mindestens 4 wöchigen einwandfreien Probelauf. Der LIEFERANT hat zu diesem Zweck eine Datei mit entsprechenden Testdaten zur Verfügung zu stellen bzw. diese Datei aus Daten der RI-C selbst zu erstellen. Treten während des Probelaufes Fehler auf oder entspricht das Ergebnis nicht den vereinbarten Spezifikationen, hat der LIEFERANT diese Mängel unverzüglich zu beseitigen bzw. auszubessern. Der Probelauf beginnt sodann wieder neu zu laufen. Die RI-C wird sich bemühen, auftretende Mängel bzw. Fehlfunktionen zu dokumentieren und diese Informationen dem LIEFERANT zur Verfügung zu stellen. Soweit die Mitwirkung der RI-C bei der Fehlersuche zwingend erforderlich ist, wird die RI-C den LIEFERANTEN in adäquatem Umfang dabei unterstützen, sofern dadurch der Betriebsablauf der RI-C nicht beeinträchtigt wird und/oder kein Zusatzaufwand bei der RI-C entsteht.

7.2. Nach Fertigstellung aller vom LIEFERANT zu erbringenden Lieferungen und Leistungen hat der LIEFERANT der RI-C seine Lieferungen bzw. Leistungen zur Endabnahme anzubieten. Werden

dabei nicht bloß unerhebliche Mängel festgestellt oder hat der LIEFERANT seine Lieferungen und Leistungen nicht vollständig erbracht, so erfolgt keine Abnahme durch die RI-C. Sämtliche vom LIEFERANTEN geleisteten Arbeiten gelten rechtswirksam erst dann als abgenommen, nachdem die RI-C die Gesamtumfang der vereinbarten Lieferungen bzw. Leistungen ordnungsgemäß erhalten und übernommen hat. Erst mit dieser Übergabe geht Gefahr und Zufall auf die RI-C über; bis dahin trägt sie der LIEFERANT.

7.3. Über jede Abnahme sind gemeinsame Protokolle zu errichten, in denen die einzelnen Mängel sowie die Fristen/Termine von deren Beseitigung anzuführen. Diese Protokolle sind von beiden Parteien zu unterfertigen.

7.4. Die Abnahme einer Teillieferung oder -leistung durch die RI-C befreit den LIEFERANTEN nicht von seiner Verpflichtung für die ordnungsgemäße Erbringung der gesamten Lieferung und Leistung.

7.5. Hängen mehrere Lieferungen oder Leistungen voneinander ab oder baut eine solche auf einer anderen auf, so gelten diese Lieferungen oder Leistungen, auch wenn sie gesondert bestellt wurden, als einheitlich erbrachte Lieferung oder Leistung, sodass erst mit der abschließenden Endabnahme durch die RI-C die Tätigkeiten und Verpflichtungen des LIEFERANTEN als abgeschlossen zu betrachten sind.

7.6. Ein formeller Abnahmeprozess im Sinne der oben angeführten Regelungen kommt jedoch nicht zum Tragen, wenn es sich lediglich um die Lieferung von Standardprodukten und waren handelt oder wenn ein solcher auf Grund der Natur der Lieferungen und Leistungen nicht möglich bzw. nicht erforderlich ist.

8. Rücktritt, Kündigung und Sistierung von Rechtsgeschäften

8.1. Sofern nicht anders vereinbart, ist die RI-C berechtigt, unter Angabe von entsprechenden Gründen schriftlich von erfolgten Rechtsgeschäften wie Bestellungen und/oder abgeschlossenen Einzelverträgen zurückzutreten. In diesem Fall hat der LIEFERANT Anspruch auf Abgeltung seiner bis zum Zeitpunkt des Vertragsrücktritts erbrachten Leistungen. § 1168 Abs. 1 ABGB findet keine Anwendung.

8.2. Darüber hinaus bleibt der RI-C ihr Recht unbenommen, Rechtsgeschäfte aus erfolgten Bestellungen bzw. abgeschlossenen Einzelverträgen aus wichtigem Grund mit sofortiger Wirkung durch entsprechende schriftliche Mitteilung außerordentlich zu kündigen.

8.3. Dies trifft insbesondere, aber nicht nur, zu, sobald über das Vermögen des LIEFERANTEN ein Insolvenzverfahren eröffnet bzw. ein Eröffnungsantrag mangels kostendeckenden Vermögens abgewiesen wird, der LIEFERANT maßgebliche gesetzliche Bestimmungen verletzt, der

LIEFERANT sonstige wesentliche rechtsgeschäftliche/vertragliche Pflichten verletzt oder der LIEFERANT Kontakte mit terroristischen Gruppen hat oder sich in dieser Weise selbst betätigt.

8.4. Ferner ist die RI-C zur außerordentlichen Kündigung berechtigt, wenn sich die gesellschaftsrechtlichen Eigentümerverhältnisse auf Seiten des LIEFERANTEN derart geändert haben, dass (i) entweder mindestens 50% der Geschäftsanteile am LIEFERANTEN auf einen Dritten übergehen, oder (ii) Dritte die Stimmrechte oder Geschäftsführungsbefugnisse in der Organisation des LIEFERANTEN unabhängig von deren Beteiligung ausüben und somit das Geschäft des LIEFERANTEN kontrollieren können. Mit dem LIEFERANTEN konzernmäßig verbundene Gesellschaften (§ 15 AktG) gelten in diesem Zusammenhang nicht als Dritte.

8.5. Die Ausgestaltung von allfälligen ordentlichen Kündigungsrechten ist jeweils im Einzelfall im Wege einer Bestellung oder eines Einzelvertrages schriftlich festzulegen.

8.6. Die RI-C behält sich darüber hinaus das Recht vor, jederzeit die Unterbrechung der weiteren Vertragserfüllung zu verlangen (Sistierung). In diesem Fall ruhen die wechselseitigen Verpflichtungen aus dem Vertragsverhältnis. Dauert die Sistierung mehr als drei Monate hat der LIEFERANT Anspruch auf Ersatz der ihm allfällig aus der Sistierung entstehenden Kosten, jedoch nicht auf den entgangenen Gewinn. Für die Geltendmachung dieses Ersatzanspruches hat der LIEFERANT eine detaillierte Kostenaufstellung zur Verfügung zu stellen. Allfällige Kosten der ersten drei Monate der Sistierung sind nicht ersatzfähig.

9. Verzug

9.1. Gerät der LIEFERANT mit seiner Lieferung oder Leistung in Verzug, kann die RI-C die Erfüllung der Bestellung bzw. des Einzelvertrages fordern oder unter Setzung einer angemessenen Nachfrist von der erfolgten Bestellung bzw. dem abgeschlossenen Einzelvertrag zurückzutreten. Darüber hinaus ist die RI-C in jedem Fall (also sowohl beim Festhalten als auch beim Rücktritt von der Bestellung bzw. dem Einzelvertrag) berechtigt, eine Vertragsstrafe in Höhe von 0,5% der AUFTRAGSSUMME (gemäß Definition in Punkt 9.2) pro angefangenem Verspätungstag. jedoch maximal 20% der AUFTRAGSSUMME, zu fordern. Der LIEFERANT schuldet die Vertragsstrafe auch dann, wenn die bestellte Lieferung oder Leistung oder Teile davon von der RI-C vorbehaltlos angenommen wird. Die Geltendmachung darüber hinaus gehender Schadenersatzansprüche bleibt jedenfalls unberührt.

9.2. Unter AUFTRAGSSUMME ist in diesen AEB bei einmaliger Leistungserbringung (Zielschuldverhältnissen) der jeweilige Nettobestellwert bzw. Nettoauftragswert – inkl. eventuellen erfolgsabhängigen Entgeltkomponenten/Boni (bei einer angenommenen Zielerreichung von 100 %) – zu verstehen. Bei wiederkehrenden Leistungen (Dauerschuldverhältnissen, wie Miete, Wartung, laufende Servicierung, etc.) jener Nettobetrag, der in Summe für die durchgehende Leistungserbringung über die Vertragslaufzeit zu entrichten ist. Werden wiederkehrende Leistungen auf unbestimmte Dauer vereinbart, entspricht die AUFTRAGSSUMME dem Nettobetrag, der in Summe für die durchgehende Leistungserbringung über einen Zeitraum von 36 Monaten zu entrichten wäre.

9.3. Unbeschadet Punkt 9.1, hat der LIEFERANT die RI-C unverzüglich und unter Angabe einer Begründung über vorhersehbare Verzögerungen zu informieren. Verletzt der LIEFERANT diese Informationspflicht, so trägt er alle Kosten und Folgekosten, die ihm, der RI-C oder Dritten aus der verspäteten Lieferung oder Leistung entstehen, sowie die Kosten für einen allfälligen Sondertransport (dasselbe gilt für unvereinbarte Teillieferungen).

9.4. Sämtliche, auf Grund eines nicht von der RI-C zu vertretenden Verzugs bei Fixgeschäften im Sinne des § 919 ABGB entstehenden Mehrkosten, Schäden und entgangene Gewinne gehen zu Lasten des LIEFERANTEN. Dazu zählen insbesondere auch sämtliche Entgelte und Aufwände, die für eine Ersatzbeschaffung aufgebracht werden müssen oder mangels Möglichkeit eines Ersatzes die vollen Kosten für Ausfälle und Umdisponierungen.

10. Garantie und Gewährleistung

10.1. Der LIEFERANT leistet grundsätzlich Gewähr gemäß den gesetzlichen Vorschriften, wobei ergänzend hierzu vereinbart wird, dass ein Mangel jedenfalls dann als unbehebbar gilt, sobald zwei erfolglose Verbesserungsversuche stattgefunden haben. Es wird ausdrücklich festgehalten, dass diese Gewährleistungsrechte sinngemäß auch für alle Werk- und Dienstleistungen im Sinne des Kapitels 16. dieser AEB gelten.

10.2. Gewährt der Hersteller des Produktes oder der Ware bzw. der Sublieferant des LIEFERANTEN über die gesetzlichen Gewährleistungsrechte hinaus weitere Gewährleistungsrechte oder Garantieansprüche, gibt der LIEFERANT diese an die RI-C vollinhaltlich weiter. Jedenfalls aber gibt der LIEFERANT zusätzlich und unabhängig zu den oben angeführten Gewährleistungsrechten folgende Garantiezusage ab:

10.3. Der LIEFERANT garantiert der RI-C die Mängelfreiheit, den vertragsgemäßen und fehlerfreien Zustand sowie die fehlerfreie Funktion der von ihm erbrachten Lieferungen und Leistungen, unabhängig davon, ob der Mangel bereits bei Lieferung bzw. Abnahme vorhanden war oder erst während der vereinbarten Garantiefrist entstanden ist. Die Garantiefrist beträgt für unbewegliche Sachen einheitlich 5 Jahre, in allen anderen Fällen einheitlich 24 Monate.

10.4. Unbeschadet der Gewährleistungs- und sonstigen Ansprüche, ist die RI-C berechtigt, vom LIEFERANTEN für jede nicht bloß geringfügig mangelhafte Lieferung bzw. Leistungserbringung eine pauschale, aber Vertragsstrafe in Höhe von 5% der AUFTRAGSSUMME gemäß Punkt 9.4 zu fordern.

10.5. Die Anwendung der gesetzlichen Regelungen über die Mängelrüge gemäß §§ 377 ff UGB, wird ausgeschlossen. Es besteht somit keine Rügeobliegenheit der RI-C.

11. Haftung

11.1. Unbeschadet weitergehender Haftungsregelungen in diesen AEB haftet der LIEFERANT für Schäden grundsätzlich gemäß den österreichischen Rechtsvorschriften, und sofern der Erfüllungsort im Ausland liegt, subsidiär auch nach den für den Erfüllungsortgeltenden.

11.2. Der LIEFERANT verpflichtet sich für seine Geschäftsausübung ausreichend versichert zu sein und der RI-C nach Aufforderung einen geeigneten Nachweis darüber zu erbringen.

12. Qualitätssicherung und Review der erbrachten Leistungen

12.1. Die RI-C erwartet, dass der LIEFERANT mindestens vergleichbare Maßstäbe zur Lieferung und Leistungserbringung sowie hinsichtlich der Informationssicherheit anwendet.

12.2. Der LIEFERANT wird der RI-C über Neuerungen, Produkt-, Prozess- und Kostenoptimierungsmöglichkeiten, Leistungssteigerungen, sich ändernde Lizenzierungs- und Software-Wartungsmodelle oder Softwareupdates laufend, proaktiv und kostenlos informieren. Der LIEFERANT hat die Prozesse und die möglichen Tages- bzw. Nachtzeiten zur Meldung und Nachverfolgung von Mängeln und Fehlfunktionen gegenüber der RI-C zu definieren sowie die zugehörigen Kontakt- und Eskalationsstellen aktiv namentlich zu nennen und ist verpflichtet, etwaige Änderungen umgehend schriftlich an die RI-C zu kommunizieren.

12.3. Die RI-C und deren Endkunden erhalten vom LIEFERANTEN eine Prüfmöglichkeit betreffend die Bestellabwicklung sowie die Effizienz und Qualität der Lieferungs- und Auftragserfüllung, beschränkt auf die Geschäftsbeziehung mit der RI-C. Diese Prüfungsmöglichkeit der Nachweise soll es der RI-C ermöglichen, sich ein vollständiges Bild über Ethik, Qualität und Sicherheit der erbrachten oder noch zu erbringenden Lieferungen und Leistungen zu machen und Kundenanforderungen zu erfüllen. Eine solche Prüfmöglichkeit wird von der RI-C nur im Falle berechtigter Gründe, Anlässe oder Verdachtsmomente wahrgenommen.

12.4. Solche Prüfungen werden dem LIEFERANTEN mindestens zwei Wochen im Voraus unter Nennung der Ansprechperson auf Seiten der RI-C angekündigt. Der LIEFERANT nennt darauf möglichst rasch eine seinerseits zuständige Ansprechperson, mit welcher die weitereTerminvereinbarung durch die RI-C erfolgt. Die Prüfung erfolgt möglichst ökonomisch und störungsfrei für den LIEFERANTEN innerhalb seiner gewöhnlichen Betriebszeiten. Beim LIEFERANTEN im Zusammenhang mit der Prüfung entstehende Kosten oder Aufwände sind von der RI-C nicht zu ersetzen.

12.5. Der LIEFERANT erklärt sich im Zuge der Prüfung damit einverstanden, der RI-C bzw. deren zur Verschwiegenheit verpflichteten Prüfern ggf. auch schützwürdige und für den LIEFERANTEN wesentliche Informationen/Stichproben zur Verfügung zu stellen bzw. einsehen zu lassen, soweit diese im Kontext mit den gegenständlichen Rechtsgeschäften und deren Erfüllung stehen. Die während der Prüfung definierten / geforderten Nachweise sind spätestens binnen zwei Wochen nach Durchführung der Besichtigung an die RI-C zu übermitteln.

12.6. Ein allfälliger Abschlussbericht der Prüfung ist von der RI-C zu erstellen und wird in elektronischer Form den Geschäftsführungen des LIEFERANTEN und der RI-C übermittelt. Sollten im Abschlussbericht konkrete Maßnahmen definiert werden, so erfolgt deren Review in einer Folgeprüfung.
Wird die vorherige Abstimmung eines Rohberichts zwischen den Parteien vereinbart, so gilt der seitens der RI-C dem LIEFERANTEN vorgelegte Rohbericht als akkordiert, sofern der LIEFERANT diesem nicht binnen zwei Wochen schriftlich widerspricht.

13. Produktsicherheit und Umweltschutz

13.1. Der LIEFERANT verpflichtet sich nur Waren, Produkte und Leistungen zu liefern, welche den in Österreich geltenden Umweltschutz- und Sicherheitsbestimmungen und sonstigen allgemein anerkannten Standards sowie Grenzwerten entsprechen. Eine Entpflichtungspflicht seitens der RI-C hat der LIEFERANT der RI-C schriftlich mitzuteilen. Der LIEFERANT hat der RI-C alle mit einer Entpflichtung verbundenen Aufwendungen und Kosten zu ersetzen.

13.2. Der LIEFERANT verpflichtet sich sämtliche geltenden Sicherheitsvorschriften und die sonstigen einschlägigen europäischen und nationalen Rechtsvorschriften und Normen (ÖNORMEN, IEC-, EN-Normen, Industriestandards etc.) unter Beachtung des Standes der Technik einzuhalten.

Soweit gesetzlich (Österreichische Bestimmungen für Elektrotechnik, Elektrotechnikverordnung, etc) oder gemäß allgemein anerkannten Standards vorgesehen, haben die vom LIEFERANTEN zu liefernden Waren und Produkte ein ÖVE-Prüf-, CE-Konformitäts- oder ein diesen gleichwertiges und von der EU anerkanntes Sicherheitszeichen aufzuweisen. Gefährliche Produkte oder Stoffe sind vorschriftsmäßig zu kennzeichnen.

13.3. Technische Datenblätter, Beschreibungen, Dokumentationen oder Gefahrenhinweise, Sicherheitsblätter, gesetzlich geforderte Zertifikate, Nachweise über die Erlangung oder Vergabe von Prüf- oder Normzeichen sind spätestens gleichzeitig mit der Lieferung der entsprechenden Waren und Produkte an die RI-C zu übergeben.

13.4. Verpackungen müssen entsprechend der Verpackungsverordnung i.d.j.g.F. lizenziert sein. Der LIEFERANT sichert zu, dass er selbst oder ein jeweils vorgelagerter Hersteller oder Vertreiber an einem zugelassenen Sammel- oder Verwertungssystem im Sinne der Verpackungsverordnung teilnimmt (z.B. Vorliegen einer ARA-Lizenz).

13.5. Grundsätzlich sind bei der Lieferung und Leistungserbringung des LIEFERANTEN anfallende Abfälle von diesem auf eigene Kosten und Gefahr ordnungsgemäß zu entsorgen.

14. Urheberrechte, Marken und Musterschutz

14.1. Der LIEFERANT räumt RI-C in Bezug auf alle im Rahmen seiner Tätigkeit für bzw. im Auftrag der RI-C erstellten Arbeitsergebnisse (das gilt z.B. auch für erstellte Softwareprogramme, Dokumentationen, Methoden, Konzepte und sonstige erstellten Unterlagen etc.) das räumlich und zeitlich unbeschränkte, ausschließliche (somit auch den LIEFERANTEN selbst ausschließende) und übertragbare Werknutzungsrecht ein, diese Arbeitsergebnisse auf alle jetzt und in Zukunft bekannten Nutzungsarten zu verwenden und verwerten. Insbesondere steht der RI-C auch das Recht zu, die Arbeitsergebnisse zu ändern, zu bearbeiten, zu vervielfältigen und zu verbreiten. Die Nutzungsrechte gehen auf die RI-C in dem Zeitpunkt über, in dem im Laufe der Auftragserfüllung durch den LIEFERANTEN schutzfähige Arbeitsergebnisse entstehen.

14.2. Der LIEFERANT gewährleistet, dass die der RI-C überlassenen Arbeitsergebnisse frei von Rechten Dritter sind. Der LIEFERANT hält die RI-C in diesem Zusammenhang schad- und klaglos und unternimmt alles, um Ansprüche Dritter gegen die RI-C abzuwehren. Sollten Ansprüche aus gewerblichen Schutzrechten gegenüber der RI-C geltend gemacht werden, so wird die RI-C den LIEFERANTEN unverzüglich hierüber informieren. Die RI-C wird in diesen Fällen Entscheidungen über Vergleichs- oder Prozesshandlungen nur mit ausdrücklicher schriftlicher Zustimmung des LIEFERANTEN treffen.

14.3. Jede Referenzierung des LIEFERANTEN auf die RI-C, insbesondere die Nutzung oder Nennung von RI-C Marken und Logos auf der Website des LIEFERANTEN oder in anderen Publikationen, bedürfen der vorausgehenden schriftlichen Genehmigung der RI-C. Sofern nicht anders vereinbart, ist die genehmigte Nutzung jederzeit und ohne Angabe von Gründen durch die RI-C widerrufbar und auf die Darstellung der erbrachten Dienstleistung in einer allgemeinen Form sowie auf die Veröffentlichung der Tatsache des bestehenden oder vergangenen Kundenverhältnisses der RI-C zum LIEFERANTEN beschränkt, und unterliegt allen relevanten Richtlinien der RI-C zur Ausprägung des Handelsnamens und Logos.

14.4. Der LIEFERANT verpflichtet sich, für jeden Fall eines Verstoßes gegen die Bestimmungen des Punktes 14.3 eine Vertragsstrafe in Höhe von EUR 10.000,-- zu bezahlen. Darüber hinausgehende Schadenersatzforderungen der RI-C bleiben davon jedenfalls unberührt.

15. Besondere Bestimmungen für Software-Lizenzen und Software-Wartungen

15.1. Hat der LIEFERANT Standard-Softwareprodukte zu liefern, die nicht individuell für die RI-C oder deren Kunden entwickelt wurden, so räumt der LIEFERANT der RI-C ein übertragbares und örtlich unbegrenztes Nutzungsrecht an solchen Lizenzen ein. Dieses Nutzungsrecht ist zeitlich unbegrenzt, wenn hierfür die Zahlung eines einmaligen Entgeltes vereinbart ist. RI-C ist berechtigt, die erworbenen Softwarelizenzen auf Basis der vereinbarten Lizenzmetriken und –zahlen sowohl für den Eigenbedarf als auch für alle ihre Kunden einzusetzen, soferne keine anderweitigen einzelvertraglichen Regelungen dazu getroffen werden.

15.2. Der LIEFERANT verpflichtet sich des Weiteren, dafür Sorge zu tragen, dass die RI-C und/oder

ihre Kunden für die erworbenen Softwareprodukte eine Wartung (Software-Pflege) beziehen kann. Ein solche Software-Wartung beinhaltet auch das Recht der RI-C und deren Kunden, ohne Aufpreis alle zukünftigen Programmstände (sowohl alle neuen Versionen mit zusätzlichen Funktionen als auch Updates und Upgrades) der gegenständlichen Softwareprodukte zu beziehen und zu installieren.

15.3. Der LIEFERANT stellt sicher, dass für die gelieferten Softwareprodukte eine solche Wartung für mindestens 5 Jahre ab Lieferung der Lizenzen zu marktüblichen Konditionen angeboten wird.

15.4. Es gilt als vereinbart, dass das vereinbarte Wartungsentgelt innerhalb der ersten 36 Wartungsmonate nicht erhöht wird. Danach darf der LIEFERANT bzw. der Wartungserbringer die Software-Wartungsgebühr um maximal 3% pro Jahr erhöhen. Eine rückwirkende Erhöhung ist jedenfalls ausgeschlossen.

15.5. Die Regelungen der Punkte 15.2 bis 15.4 gelten sinngemäß auch für alle Softwareprogramme, die gemäß Punkt 14.1. individuell für die RI-C oder ihre Kunden entwickelt, erweitert oder geändert wurden.

15.6. Sollte der LIEFERANT bzw. der Hersteller der Softwareprodukte vertragliche Rechte besitzen, die Verwendung der Software-Lizenzen bei der RI-C zu auditieren oder zu vermessen (nachfolgend gesamthaft als „Audit“ bezeichnet), so gelten vorrangig dazu jedenfalls die folgenden Regelungen:

15.7. Der LIEFERANT bzw. der Hersteller muss ein solches Audit der RI-C zumindest 60 Tage im Voraus schriftlich ankündigen. Diese Ankündigung hat des Weiteren klar zu definieren, welche Methoden und Tools dabei angewendet werden sollen, was bzw. welche Produkte oder Installationen betrachtet werden, wer das Audit durchführt und wie der beabsichtigte Zeitplan und die Auditagenda aussieht.

15.8. Das Audit darf weder den normalen Geschäftsbetrieb noch die Sicherheit der RI-C oder ihren Kunden beeinträchtigen und ist kapazitätsschonend und zu den üblichen Geschäftszeiten durchzuführen.

15.9. Die Kosten für das Audit und der Auditoren können der RI-C oder ihre Kunden nicht weiterverrechnet werden, diese hat der LIEFERANT bzw. Hersteller aus eigenem zu tragen.

15.10. Sollte sich auf Basis des Audits ergeben, dass allenfalls Lizenzen nachgekauft werden müssen, so hat die RI-C in diesem Falle das ausdrückliche Recht, auch diese Lizenzen zu den bereits bestehenden Einkaufskonditionen zu erwerben.

16. Besondere Bestimmungen für Dienst- und Werkleistungen

16.1. Mit Annahme einer Bestellung für Dienst- oder Werkleistungen auf Basis einer Verrechnung nach Zeit verpflichtet sich der LIEFERANT, von sich aus rechtzeitig vor einer Überschreitung der bestellten Maximalsumme zu warnen und darüber hinausgehende Leistungen erst dann zu erbringen und zu verrechnen, wenn dazu eine weitere, schriftliche Bestellung der Einkaufsabteilung der RI-C vorliegt.

16.2. Die jeweiligen Leistungsabrufe bis zur jeweils bestellten Maximalsumme erfolgen durch den fachlichen Ansprechpartner auf Seiten der RI-C.

16.3. Vereinbarte Honorarsätze werden vom LIEFERANTEN jeweils für mindestens 24 Monate garantiert. Für eine vom LIEFERANTEN beabsichtigte Erhöhung ist es darüber hinaus erforderlich, dass dieses Begehren mindestens vier Monate vor der geplanten Wirksamkeit an die RI-C schriftlich herangetragen wird.

16.4. Der in einem Einzelvertrag angeführte Gesamtzeitaufwand versteht sich immer als ein Maximalwert, der seitens der RI-C jedoch nicht ausgeschöpft werden muss.

16.5. Die RI-C behält sich insbesondere vor, vom Gesamtleistungsaufwand Teile für das jeweilige Projekt selbst zu erbringen oder erbringen zu lassen oder dem LIEFERANTEN Vorleistungen beizustellen. Die von der RI-C beigestellten Unterlagen und/oder Leistungen sind vom LIEFERANTEN auf Eignung für dessen eigene Leistungserbringung zu überprüfen.

Grundsätzlich sind mit den vereinbarten Honorarsätzen auch sämtliche anfallenden Aufwendungen und sonstigen Kosten auf Seiten des LIEFERANTEN bei oder im Zusammenhang mit der Erbringung der vereinbarten Leistungen vollständig abgegolten. Die Sätze inkludieren daher insbesondere auch alle Spesen, Diäten sowie Reisekosten und–zeiten.

16.6. Sollte im Einzelfall die Verrechnung von solchen Kosten vorab vereinbart werden, so werden anfallende Reisekosten ohne Aufschlag vom LIEFERANTEN an die RI-C weiterverrechnet, sofern sie nicht direkt von dieser getragen werden. Der LIEFERANT wird alle möglichen Maßnahmen ergreifen, um die Reisekosten so gering wie möglich zu halten, bspw. durch Buchung bzw. Verwendung des jeweils günstigsten, adäquaten Transportmittels bzw. Hotels.

16.7. Sofern nicht anders vereinbart, erfolgt die Abrechnung der erbrachten Leistungen jeweils zum Ende des Kalendermonats unter Einhaltung der unter Punkt 4. geregelten Formalerfordernisse sowie unter Beilage von detaillierten und abgenommenen Arbeitsberichten und allfälliger Kostenbelege.

16.8. Soweit anwendbar gelten die obigen Regelungen sinngemäß auch für Dienst- oder Werkleistungen, die auf Basis eines Pauschalpreises verrechnet werden.

17. Geheimhaltung und Datenmissbrauch

17.1. Die Parteien verpflichten sich jeweils, gegenseitig mitgeteilte, vertrauliche Informationen und Unterlagen geheim zu halten, sie Dritten weder zugänglich zu machen, noch ihnen Einsicht zu gewähren, sie nicht zu veröffentlichen und sie nur im Rahmen des vertraglichen Zweckes zu verwenden, sowie alle erforderlichen Maßnahmen zu treffen, um deren Kenntnisnahme und Verwertung durch Dritte zu verhindern. Personen, mit denen laut vereinbartem Liefer- und Leistungsumfang ein Informationsaustausch stattzufinden hat, gelten in diesem Zusammenhang nicht als Dritte.

17.2. Unter vertraulicher Information sind Informationen und Daten aller Art zu verstehen, wie zum Beispiel Materialien, Produkte, Technologien, Computerprogramme, Beschreibungen, Business Pläne, Kunden- und Vertriebsdaten, Finanzinformationen, Marketingkonzepte und jede andere Information. Es ist unerheblich, ob solche vertrauliche Information schriftlich, mündlich, elektronisch oder durch ein sonstiges Medium an den Datenempfänger übermitteltwurde.

17.3. Die Verpflichtung zur Geheimhaltung gilt nicht für Informationen, die allgemein öffentlich bekannt sind oder ohne Verstoß gegen die in diesen AEB enthaltenen Verpflichtungen allgemein öffentlich bekannt werden, oder die der Datenempfänger aufgrund zwingenden Rechts gegenüber einem Gericht oder einer Behörde offen zulegen hat, sowie für jene Informationen, die die Parteien nachweislich von Dritten erhalten haben und für die die Parteien aufgrund ihres Wissenstandes über die jeweils andere Partei und die Marktgepflogenheiten davon ausgehen können, dass keine Geheimhaltungspflicht besteht.

17.4. Vertrauliche Informationen dürfen, außer zu Zwecken der Erfüllung der jeweiligen Bestellung, nicht vervielfältigt werden. Auf Verlangen der RI-C stellt der LIEFERANT, ohne Zurückbehaltung von Kopien, die vertrauliche Information zurück, vernichtet oder löscht sie nachweislich und nicht reproduzierbar. Alle Unterlagen und deren Kopien, die dem LIEFERANTEN im Zuge der Ausführung der jeweiligen Bestellung überlassen werden, sind spätestens bei Beendigung der Vertragsbeziehung an die RI-C zurückzustellen. Beide Parteien vereinbaren, ihnen versehentlich zugegangene Unterlagen unverzüglich zu retournieren und ebenfalls vertraulich zu behandeln.

17.5. Der LIEFERANT darf nur solche Personen Subunternehmer zur Vertragserfüllung heranziehen, die sich ihm gegenüber vertraglich zur Einhaltung der gegenständlichen Geheimhaltungsbestimmungen, des Datenschutzgesetzes sowie der Datenschutzgrundverordnung in der jeweils geltenden Fassung, der Einhaltung der Bestimmungen bezüglich Insider Informationen gemäß dem Börsengesetzes und, soweit anwendbar, der Geheimhaltungsverpflichtungen nach dem Bankwesengesetzes verpflichtet haben. Der LIEFERANT verpflichtet sich weiters, die vertraulichen Informationen nur solchen Mitarbeitern / Subunternehmern zugänglich zu machen, bei denen eine Notwendigkeit zur Kenntnis vorliegt.

17.6. Soweit der LIEFERANT Zugriff auf und/oder Einsicht in personenbezogene Daten erhält, wird er bei der vereinbarungsgemäßen Verarbeitung und Benützung solcher Daten für die RI-C als Auftragsverarbeiter bzw. Unterauftragsverarbeiter tätig. Der LIEFERANT verpflichtet sich in einem solchen Fall mit der RI-C eine Auftragsverarbeitervereinbarung bzw. Unterauftragsverarbeitervereinbarung abzuschließen. Sofern der LIEFERANT von der RI-C keine Auftragsverarbeitervereinbarung bzw. Unterauftragsverarbeitervereinbarung übermittelt

bekommen hat, dann wird dieser die RI-C sofort darauf hinweisen. In allen Belangen des Datenschutzes ist das österreichische Datenschutzgesetz, die Datenschutzgrundverordnung

sowie das BWG in seiner jeweils gültigen Fassung anzuwenden. Für beide Parteien sind die im Bankenbereich üblichen, strengen Sorgfaltspflichten maßgeblich.

17.7. Diese Vereinbarung begründet keine Verpflichtung der RI-C, dem LIEFERANTEN vertrauliche Informationen zur Verfügung zu stellen. Weiters werden allein durch diese Bestimmungen keine Lizenzen oder andere Rechte an irgendeiner vertraulichen Information vereinbart oder übertragen. Der LIEFERANT verpflichtet sich, keine vertraulichen Informationen in welcher Weise auch immer für die Entwicklung eigener ähnlicher oder konkurrierender Produkte zu verwenden oder in diese einfließen zu lassen.

17.8. Der LIEFERANT verpflichtet sich, die Bestimmungen dieser AEB und aller weiteren Verträge bzw. die Tatsache, dass die RI-C oder ihre Kunden ggf. Zutritt zu Räumlichkeiten bzw. Zugriff auf Systeme gewährt, geheim zu halten. Veröffentlichungen jeder Art, die mit der Vertragserfüllung im Zusammenhang stehen, bedürfen der vorherigen schriftlichen Zustimmung der RI-C.

17.9. Der LIEFERANT haftet für die Einhaltung sowohl der gesetzlichen als auch der aus diesen Geheimhaltungsbestimmungen erwachsenden Verpflichtungen. Der LIEFERANT ist sich darüber im Klaren, dass die RI-C im Falle einer schon erfolgten oder drohenden Verletzung dieser Bestimmungen in Ergänzung zu anderen Rechtsbehelfen auch einstweilige Verfügungen erwirken kann, um die Rechte des Dateninhabers zu schützen.

17.10. Der LIEFERANT verpflichtet sich, für jeden Fall eines Verstoßes gegen diese Geheimhaltungsbestimmungen eine verschuldensunabhängige Vertragsstrafe in Höhe von EUR 25.000,-- zu bezahlen. Darüber hinausgehende Schadenersatzforderungen der RI-C bleiben davon unberührt.

18. Verhaltenskodex für soziale Verantwortung und Integrität

18.1. Die Geschäftstätigkeit der RI-C ist ehrlich, fair und transparent. Die Einhaltung von rechtlichen Bestimmungen und ethischen Grundsätzen ist für die RI-C selbstverständlich. Dies erwartet die RI-C auch von allen ihren Lieferanten. Darüber hinaus sind der RI-C gesellschaftliches Engagement sowie Klima- und Umweltschutz wichtig.

18.2. Der LIEFERANT sichert die Einhaltung sämtlicher gesetzlichen Bestimmungen zu. Der LIEFERANT hat in diesem Zusammenhang insbesondere auch sicherzustellen, dass im Zusammenhang mit der vertragsgegenständlichen Leistungserbringung die Bestimmungen der International Labour Organisation (ILO) hinsichtlich der Rechte der Arbeitnehmer und deren Arbeitsbedingungen (wie insbesondere Einhaltung der Menschenrechte, Verbot der Kinder- und Zwangsarbeit, Mindeststandards im Bereich Arbeitssicherheit und Gesundheitsschutz, Gewährleistung angemessener Vergütung) eingehalten werden. Der LIEFERANT hat diese Verpflichtung seinen Sublieferanten nachweislich zu überbinden.

18.3. Der LIEFERANT bestätigt, dass es keine Vermittler gibt, die einen persönlichen und/oder wirtschaftlichen Vorteil aus dem Abschluss einer Vereinbarung mit der RI-C ziehen.

18.4. Der LIEFERANT ist verpflichtet, Interessenskonflikte gegenüber der RI-C und den mit ihr verbundenen Unternehmen des Raiffeisen-Sektors zu vermeiden und alles zu unterlassen, was der RI-C und/oder dem Raiffeisen-Sektor, insbesondere deren Ruf, schaden könnte.

18.5. Die RI-C lehnt Korruption und Bestechung in jeder Hinsicht ab. Im Besonderen verpflichtet sich daher der LIEFERANT es zu unterlassen, unrechtmäßige und/oder den guten Sitten widersprechende Zuwendungen oder sonstige Vorteile zu fordern, anzunehmen, solche anzubieten oder zu gewähren.

18.6. Ein Verstoß gegen die Bestimmungen dieses Verhaltenskodex ist ein wichtiger Grund, der die RI-C berechtigt, alle oder einzelne zwischen den Parteien bestehende Rechtsgeschäfte, Partnerschaften, Verträge etc. mit sofortiger Wirkung aufzulösen.

19. Allgemeine Bestimmungen

19.1. Die in diesen AEB verwendeten Überschriften dienen nur der Zweckmäßigkeit und sind bei der Auslegung nicht zu berücksichtigen. Alle Verweise auf gesetzliche Vorschriften schließen die Novellierung oder Wiederverlautbarung dieser Vorschriften ein, gleichgültig, ob diese vor oder nach dem Datum einer gegenständlichen Bestellung und/oder eines Einzelvertrages erfolgt sind oder erfolgen werden.

19.2. Diese AEB und deren Rechtswirksamkeit, Auslegung und Erfüllung unterliegen dem

österreichischen Recht unter Ausschluss der Kollisionsnormen. Das Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenkauf („UN Kaufrecht“) findet keine Anwendung.

19.3. Die Parteien werden nach Möglichkeit in allen Fragen der Auslegung dieser AEB und Zusammenarbeit zweckmäßige und einvernehmliche außergerichtliche Lösungen anstreben. Sollte eine solche Einigung nicht möglich sein, ist für alle Streitigkeiten, die sich im Zusammenhang mit diesen AEB und / oder darauf basierenden Rechtsgeschäften ergeben, das für Handelssachen zuständige Gericht für Wien, Innere Stadt, ausschließlich zuständig.

19.4. Sollte eine Bestimmung dieser AEB ganz oder teilweise unwirksam oder undurchführbar sein oder werden, wird dadurch die Wirksamkeit oder Durchführbarkeit der übrigen Bestimmungen nicht berührt. Anstelle der unwirksamen Bestimmung gilt diejenige wirksame Bestimmung als vereinbart, welche dem Sinn und Zweck der unwirksamen Bestimmung entspricht; dasselbe gilt entsprechend für allfällige Lücken in diesen AEB.

19.5. Änderungen oder Ergänzungen dieser AEB bedürfen zu ihrer Wirksamkeit einer schriftlichen Vereinbarung, welche den AEB als Anhang beizufügen ist. Dies gilt auch für Änderungen oder Ergänzungen dieser Schriftformklausel. Dieses Schriftformerfordernis ist auch mit einfacher elektronischer Signatur erfüllt. Die Parteien werden nach Möglichkeit die Dokumente elektronisch signieren.

19.6. Die Parteien verpflichten sich, die Rechte und Pflichten aufgrund und im Zusammenhang mit diesen AEB auf ihre jeweiligen Rechtsnachfolger zu überbinden.

Die RI-C ist weiters berechtigt, ihre Rechte und Pflichten aus Rechtsgeschäften, die auf diesen AEB basieren, sowie einen dazugehörigen Vertrag ohne vorherige Zustimmung seitens des LIEFERANTEN an ein GRUPPENUNTERNEHMEN oder einen Dritten zu übertragen. Die R-IC ist darüber hinaus auch berechtigt, die Inhalten (insbesondere die Preise) aus Angeboten des LIEFERANTEN sowie aus Verträgen mit dem LIEFERANTEN auch seinen Endkunden offen zu legen.

20. Beilagen

Beilage A: Lieferung von Produkten und Waren sowie für die Erbringung von Dienst- und Werkleistungen

Beilage B: Sicherheitsanforderungen für Lieferanten

Beilage C: Auftragsverarbeitung (Agreement on Order Processing in Acordance with Article 28 GDPR)

Beilage D: Oursourcing Regulations / Code of Conduct

Beilage A zu den Allgemeinen Einkaufsbedingungen für die Lieferung von Produkten und Waren sowie für die Erbringung von Dienst- und Werkleistungen

Sicherheitsbestimmungen für Lieferanten der Raiffeisen Informatik Consulting GmbH

- Für alle Dienst- oder Werkleistungen sind die Bestimmungen der aushangpflichtigen Gesetze sowie die Haus- oder Betriebsordnung zu beachten.
- Der etwaig gewährte Zugang zu den Räumlichkeiten/Systemen der RI-C oder deren Kunden darf nur zu dem Zweck verwendet werden, der sich aus dem zu Grunde liegenden Vertrag ergibt. Ein Versuch sich, ohne Genehmigung durch RI-C Zugang zu anderen als den genannten Systemen / Räumlichkeiten zu verschaffen, ist strengstens untersagt
- Die Brandschutzordnung der RI-C ist einzuhalten. Ein Merkblatt dazu ist in jedem Raum ausgehängt. Rauchen ist nur in den gekennzeichneten Freiluft-Raucherbereichen gestattet. In Gebäuden herrscht absolutes Rauchverbot. Systemräume sind mit Gaslöschanlagen ausgestattet. Bei Feueralarm oder Ausströmen des Löschgases ist der Raum sofort zu verlassen da Gesundheitsgefahr besteht!
- Die Zutrittsberechtigung ist personengebunden und nicht übertragbar. Ausgegebene Schlüssel (darunter werden auch Zutrittskarten, Token etc. verstanden) dürfen nicht weitergegeben oder durch unsichere Verwahrung Dritten zugänglich gemacht werden. Schlüssel dürfen nicht für Dritte erkennbar mit dem Unternehmen in Verbindung gebracht werden (z.B. durch Schlüsselband, Beschriftung etc.). Werden Schlüssel vom Portier ausgegeben, sind diese beim Verlassen des Gebäudes wieder abzugeben. Ausgegebene Schlüsseln sind sicher zu verwahren, der Verlust ist umgehend zu melden.
- Der Aufenthalt im Gebäude ist nur für die Zeit der Erbringung der vertraglich vereinbarten Dienstleistungen gestattet. Das Tragen von äußeren Erkennungszeichen wie beispielsweise Dienstkleidung, Ausweis etc. ist dabei verpflichtend.
- Es wird ausdrücklich untersagt, anderen Personen Zutritt zu Bereichen zu ermöglichen, die mit Hilfe der ausgegebenen Schlüssel durch Personal des LIEFERANTEN geöffnet wurden (z.B. durch das Aufhalten der Türe, das Mitfahren lassen mit gesicherten oder versperrten Aufzügen etc.). Gäste sind auf die Notwendigkeit der Anmeldung beim Portier hinzuweisen.
- Sind beim Verlassen von Büroräumen, die im Rahmen von Tätigkeiten betreten wurden, keine R-IT-Mitarbeiter anwesend, so sind die Türen zu schließen und zu versperren, unabhängig davon, wie sie vorgefunden wurden. Fenster in Büro- oder Besprechungsräumen sowie in den Gängen sind zu schließen sowie das Licht abzuschalten. Die Abmeldung beim Portier ist obligatorisch.
- Das Aufkeilen von Türen mit automatischen Schließvorrichtungen ist nicht gestattet. Werden aufgekeilte Türen vorgefunden, sind diese zu schließen.
- Das Fotografieren oder Filmen im Gebäude ist nicht gestattet.
- Dokumente sind entsprechend der Vertraulichkeit der Informationen zu entsorgen. Die bereitgestellten Aktenvernichtungscontainer sind für die Entsorgung von internen bzw. vertraulichen Dokumenten, technische Aufzeichnungen, Notizen etc. zu verwenden. In Büros sind entsprechend gekennzeichnete grüne und blaue Abfallbehälter bereitgestellt.
- Das Personal des LIEFERANTEN ist zu verpflichten, allfällige sicherheitsrelevante Beobachtungen unverzüglich einem Auftraggebervertreter (Mitarbeiter, Portier oder Wachdienst) zu melden. Dazu zählen unter anderem:
  - defekte Schlösser, Türen oder Fenster (lassen sich nicht schließen, zerbrochen etc.)
  - defekte Anlagen oder beobachtete Funktionsstörungen (z.B. an Armaturen, Geräten in Küche, bemerkter Wasseraustritt, Rauch, Geruch etc.) und wenn sonstige Gefahr besteht
  - gefundene Wertgegenstände, Schlüssel, Zutrittskarten, Token, etc.

Die hier beschriebenen Verhaltensregeln gelten für alle Standorte der RI-C sowie deren Kunden und Partner, zu denen der LIEFERANT im Auftrag der RI-C Zutritt erhält.

Security Requirements for Suppliers (SRS) / Sicherheitanforderungen für Lieferanten

of / der

Raiffeisen Informatik GmbH & Co KG
Lilienbrunngasse 7-9, 1020 Wien

(subsequently called “CUSTOMER” / nachfolgend „KUNDE“ genannt)

effective from December, 1st 2021 / gültig ab 01.Dezember 2021

Delivering trusted services is an integral part of our corporate strategy. Using innovative services and products as well as cooperating with professional partners and suppliers, meeting our security requirements is necessary to stay ahead in a fast-changing industry.

Die Erbringung vertrauenswürdiger Dienstleistungen ist ein integraler Bestandteil unserer Unternehmensstrategie. Der Einsatz innovativer Dienstleistungen und Produkte sowie die Zusammenarbeit mit professionellen und unsere Sicherheitsanforderungen erfüllenden Partnern und Lieferanten ist dabei notwendig, um in einer sich schnell verändernden Branche erfolgreich zu sein.

It is our due diligence to protect our as well as our client’s data, systems and applications with security measures according to leading industry standards as it is expected from an IT-provider, serving international financial institution.
Managing supplier relationships in regard to security is an important part of internal risk management framework, a common praxis (e.g. ISO 27000 series, NIST Cybersecurity Framework) and mandatory for financial institutions (e.g. the EBA Guidelines on ICT and security risk management dated 29 November 2019, § 25 and the Annex to § 25 of the Austrian Banking Act, etc.), together further referred to as the "Security Requirements".

Es gehört zu unserer Sorgfaltspflicht, sowohl unsere als auch die Daten, Systeme und Anwendungen unserer Kunden mit Sicherheitsmaßnahmen nach führenden Industriestandards zu schützen, wie es von einem IT-Provider internationaler Finanzinstitute erwarten wird.
Das Management von Lieferantenbeziehungen in Bezug auf die Sicherheit ist ein wichtiger Teil des internen Risikomanagements, eine gängige Praxis (zB. ISO 27000-Serie, NIST Cybersecurity Framework) und für Finanzinstitute verpflichtend (zB. die EBA-Leitlinien zum IKT- und Sicherheitsrisikomanagement vom 29. November 2019, § 25 und der Anhang zu § 25 des österreichischen Bankwesengesetzes usw.), die im Folgenden als "Sicherheitsanforderungen" bezeichnet werden.

The Security Requirements are derived from established industry standards and based on best practices, which can be expected from a service provider in the financial sector.

Die Sicherheitsanforderungen leiten sich von etablierten Branchenstandards ab und basieren auf Best Practices, die von einem Dienstleister im Finanzsektor erwartet werden können.

Having regard to the above, the Vendor, Processor or Partner (collectively referred to as “SUPPLIER”) represents and warrants that it has made all necessary due diligence and is familiar with and acknowledges the Security Requirements and agrees to comply with the Security Requirements in general, as well when (a) accessing CUSTOMER facilities, Networks and/or Information Systems, or (b) accessing, processing, or storing CUSTOMER information/data, or (c) providing infrastructure services and/or standard software, developing software.
Whenever these SRS or any other requirements talk

In Anbetracht des Vorstehenden sichert der Anbieter, Auftragsverarbeiter oder Partner (gemeinsam als „LIEFERANT" bezeichnet) zu und gewährleistet, dass er alle erforderlichen Sorgfaltspflichten erfüllt hat und mit den Sicherheitsanforderungen vertraut ist und diese anerkennt und sich verpflichtet, die Sicherheitsanforderungen im Allgemeinen einzuhalten, wenn er (a) auf Einrichtungen, Netze und/oder Informationssysteme des KUNDEN zugreift oder (b) auf Informationen/Daten des KUNDEN zugreift, diese verarbeitet oder speichert oder (c) Infrastrukturdienste und/oder Standardsoftware bereitstellt oder Software entwickelt.

Whenever the term "CUSTOMER" is used in this Security Policy, it shall mean not only the respective data (or systems, services, etc.) of R-IT, but also those of its customers.

Additional security requirements may be specified in individual agreements (e.g. SLA, statement of work).

The German version is for information purpose only. The English version shall prevail.

Wann immer in diesen Sicherheitsrichtlinie von "KUNDE" die Rede ist, sind sinngemäß nicht nur die jeweiligen Daten (bzw. Systeme, Services, etc.) der R-IT, sondern auch die ihrer Kunden zu verstehen.

Zusätzliche Sicherheitsanforderungen können in Einzelvereinbarungen (zB. SLA, statement of work) festgelegt werden.

Die deutsche Version dient nur zur Information. Die englische Fassung ist maßgebend.

ICT Governance	ICT Governance
Guidelines	**Richtlinien**
The SUPPLIER maintains an information security management system including a continuous improvement process based on recognized industry standards.	Der LIEFERANT unterhält ein Managementsystem für die Informationssicherheit, das einen kontinuierlichen Verbesserungsprozess auf der Grundlage anerkannter Branchenstandards umfasst.
Information security policies, procedures, roles, responsibilities and accountabilities are defined in accordance with SUPPLIER`s business requirements, relevant laws and regulations. Information security policies are approved by management, published and communicated to employees and relevant external parties.	Informationssicherheitsrichtlinien, -verfahren, -rollen, -verantwortlichkeiten und -zuständigkeiten werden in Übereinstimmung mit den Geschäftsanforderungen des LIEFERANTEN und den einschlägigen Gesetzen und Vorschriften festgelegt. Die Informationssicherheitsrichtlinien werden von der Geschäftsleitung genehmigt, veröffentlicht und an die Mitarbeiter und relevanten externen Parteien weitergegeben.
The SUPPLIER regularly reviews its compliance to established security policies, standards and any other security requirements.	Der LIEFERANT überprüft regelmäßig, ob er die festgelegten Sicherheitsrichtlinien und -standards sowie alle anderen Sicherheitsanforderungen einhält.
Risk Management	**Risikomanagement**
The SUPPLIER has a security risk management in place. The SUPPLIER ensures that risks, which directly or indirectly affect CUSTOMER services and/or data, are assessed and mitigation measures are in place and documented. Risks which directly or indirectly affect the CUSTOMER must be reported on demand.	Der LIEFERANT verfügt über ein Sicherheitsrisikomanagement. Der LIEFERANT stellt sicher, dass Risiken, die sich direkt oder indirekt auf die Dienste und/oder Daten des KUNDEN auswirken, bewertet und Maßnahmen zur Risikominderung ergriffen und dokumentiert werden. Risiken, die den KUNDEN direkt oder indirekt betreffen, müssen auf Verlangen gemeldet werden.
Contractual Agreement	**Vertragliche Vereinbarung**
The SUPPLIER must include responsibilities for information security in contractual agreements with their employees and contractors.	Der LIEFERANT muss die Verantwortung für die Informationssicherheit in die vertraglichen Vereinbarungen mit seinen Mitarbeitern und Auftragnehmern aufnehmen.
Background Checks	**Hintergrund-Checks**
Background verification checks on candidates for employment are carried out in accordance with relevant laws and regulations. The level of verification performed must be proportional to the risk associated with the candidate's role.	Die Überprüfung des Hintergrunds von Bewerbern für eine Beschäftigung erfolgt in Übereinstimmung mit den einschlägigen Gesetzen und Vorschriften. Der Umfang der Überprüfung muss im Verhältnis zu dem mit der Funktion des Bewerbers verbundenen Risiko stehen.
Awareness Program	**Sensibilisierungsprogramm**
All employees of the SUPPLIER and, where relevant, contractors receive awareness education and trainings appropriate for their job function. Additionally, updates of SUPPLIER`s policies and procedures are communicated to employees as well. All personnel must have adequate skills related to their roles and responsibilities.	Alle Mitarbeiter des LIEFERANTEN und gegebenenfalls auch die Auftragnehmer erhalten eine ihrer Funktion entsprechende Sensibilisierung und Schulung. Darüber hinaus werden die Mitarbeiter auch über Aktualisierungen der Richtlinien und Verfahren des LIEFERANTEN unterrichtet. Das gesamte Personal muss über die für seine Aufgaben und Zuständigkeiten erforderlichen Kenntnisse verfügen.
ICT Project and Change management	**ICT Projekt- und Changemanagement**
Asset Lifecycle	**Asset-Lebenszyklus**
The SUPPLIER ensures that information security is an integral part of information systems across their entire lifecycle (acquisition to decommission of assets).	Der LIEFERANT stellt sicher, dass die Informationssicherheit ein integraler Bestandteil der Informationssysteme über deren gesamten Lebenszyklus ist (Erwerb bis Stilllegung der Anlagen).

The SUPPLIER ensures that provided software is supported by operating systems and middleware (e.g. Java) versions, which receive security updates and are not end-of-life. The SUPPLIER provides regular, in time security updates over the entire contract lifecycle.	Der LIEFERANT stellt sicher, dass die bereitgestellte Software von Betriebssystemen und Middleware (zB. Java) unterstützt wird, die Sicherheitsupdates erhalten und nicht veraltet sind. Der LIEFERANT sorgt für regelmäßige, rechtzeitige Sicherheitsupdates während des gesamten Vertragslebenszyklus.
Software Change Management	**Software Change Management**
The SUPPLIER has formal change management and secure software development lifecycle policies that also define security related controls. Cybersecurity reviews for new system designs or changes to systems, and security testing prior to deployment must be part of the processes. Changes are appropriately requested, authorized, tested and approved prior release to production.	Der LIEFERANT verfügt über formale Richtlinien für das Change Management und den Lebenszyklus der sicheren Softwareentwicklung, die auch sicherheitsrelevante Kontrollen festlegen. Überprüfungen der Cybersicherheit bei neuen Systemdesigns oder Änderungen an Systemen sowie Sicherheitstests vor der Bereitstellung müssen Teil der Prozesse sein. Änderungen werden in angemessener Weise angefordert, autorisiert, getestet und genehmigt, bevor sie für die Produktion freigegeben werden.
Secure Software Development Lifecycle	**Lebenszyklus der sicheren Softwareentwicklung**
The SUPPLIER includes information security aspects in the product documentation. This documentation must contain instructions for the configuration of the service and/or the environment in order to ensure a secure operation. Developed software must be tested in a controlled environment in order to detect weaknesses before it is provided to the CUSTOMER.	Der LIEFERANT nimmt Aspekte der Informationssicherheit in die Produkt-dokumentation auf. Diese Dokumentation muss Anweisungen für die Konfiguration des Dienstes und/oder der Umgebung enthalten, um einen sicheren Betrieb zu gewährleisten. Entwickelte Software muss in einer kontrollierten Umgebung getestet werden, um Schwachstellen zu erkennen, bevor sie dem KUNDEN zur Verfügung gestellt wird.
The SUPPLIER ensures that the software development lifecycle contains appropriate security measures (Secure Software Development Lifecycle). This includes but is not limited to: -Usage of internationally recognized secure software development methods (including agile processes such as Scrum, Kanban, etc.) as integral part of the secure software development process -Secure coding guidelines based on international standards -Integrity of source code is ensured -Periodically carry out secure code reviews (Static Application Security Testing and Dynamic Application Security Testing) -Vulnerability scanning which also includes used third-party code and open source components (e.g. libraries) -Penetration tests which are performed by an independent third party -Appropriate trainings for internal and external software developers Findings and known vulnerabilities are mitigated before release to production.	Der LIEFERANT stellt sicher, dass der Lebenszyklus der Softwareentwicklung angemessene Sicherheitsmaßnahmen enthält (Secure Software Development Lifecycle). Dies beinhaltet, ist aber nicht beschränkt auf: -Einsatz international anerkannter, sicherer Softwareentwicklungsmethoden (einschließlich agiler Prozesse wie Scrum, Kanban, etc.) als integraler Bestandteil des sicheren Softwareentwicklungsprozesses -Sichere Coding-Richtlinien auf der Grundlage internationaler Normen -Die Integrität des Quellcodes ist gewährleistet. -Regelmäßige Überprüfung des sicheren Codes (statische und dynamische Anwendungs-sicherheitstests) -Schwachstellen-Scans, die auch den verwendet-en Code von Drittanbietern und Open-Source-Komponenten (zB. Bibliotheken) umfassen -Penetrationstests, die von einer unabhängigen dritten Partei durchgeführt werden -Angemessene Schulungen für interne und externe Softwareentwickler Gefundene und bekannte Schwachstellen werden vor der Freigabe für die Produktion beseitigt.

Outsourcing	Outsourcing
Sub-Outsourcing	**Sub-Outsourcing**
The SUPPLIER has clear contractual agreements with any SUB-SUPPLIERs of services, in order to state their responsibility for the security of CUSTOMER data they process / store / transmit on behalf of the CUSTOMER. The SUPPLIER ensures that security measures implemented by the SUB-SUPPLIERs have at least the same level as stated within this document and prime contract. The SUPPLIER verifies the effectiveness of the measures as part of their supplier management process.	Der LIEFERANT hat klare vertragliche Vereinbarungen mit allen Unterauftragnehmern von Dienstleistungen, um deren Verantwortung für die Sicherheit der KUNDENDATEN, die sie im Auftrag des KUNDEN verarbeiten / speichern / übermitteln, festzulegen. Der LIEFERANT stellt sicher, dass die von den UNTERAUFTRAGNEHMERN eingeführten Sicherheitsmaßnahmen mindestens das in diesem Dokument und im Hauptvertrag angegebene Niveau haben. Der LIEFERANT prüft die Wirksamkeit der Maßnahmen im Rahmen seines Lieferantenmanagementprozess.
Information Security	**Informationssicherheit**
Identity and Access Management	**Identitäts- und Zugriffsmanagement**
The SUPPLIER has access controls in place in order to verify identities and restrict access to authorized users only. Access rights are based on "need to know" and "least privilege" principles. Additionally, the principle of "separation of duties" is adhered to.	Der LIEFERANT hat Zugangskontrollen eingerichtet, um Identitäten zu überprüfen und den Zugang auf autorisierte Benutzer zu beschränken. Die Zugriffsrechte beruhen auf den Grundsätzen "Kenntnisnahme erforderlich" und "geringstmögliches Privileg". Darüber hinaus wird der Grundsatz der "Aufgabentrennung" beachtet.
The SUPPLIER has implemented authentication mechanisms to protect accesses to systems, according to best practices which include but are not limited to:- password policies (minimum lengths, complexity, avoiding re-use) -unique user identification (generic and shared users are avoided) -secure storage / management / transmission of credentials	Der LIEFERANT hat Authentifizierungs-mechanismen implementiert, um den Zugang zu den Systemen nach bewährten Verfahren zu schützen, die unter anderem Folgendes umfassen -Passwortrichtlinien (Mindestlänge, Komplexität, Vermeidung von Wiederverwendung) -eindeutige Benutzeridentifikation (generische und gemeinsame Benutzer werden vermieden) -Sichere Speicherung/Verwaltung/Übermittlung von Anmeldedaten
SUPPLIER ensures that accounts which are used for access over the internet are protected by strong authentication mechanisms (e.g. multi-factor authentication).	Der LIEFERANT stellt sicher, dass Konten, die für den Zugang über das Internet genutzt werden, durch starke Authentifizierungsmechanismen (zB. Multi-Faktor-Authentifizierung) geschützt sind.
The SUPPLIER has implemented strong controls for privileged accounts (e.g. system administrators) by means of strong authentication, limitation to a minimum and closely supervised usage (e.g. multi-factor authentication).	Der LIEFERANT hat strenge Kontrollen für privilegierte Konten (zB. Systemadministratoren) durch starke Authentifizierung, Beschränkung auf ein Minimum und streng überwachte Nutzung (zB. Multi-Faktor-Authentifizierung) eingeführt.
The SUPPLIER shall review the access rights of its staff on regular intervals and shall change (i.e. restrict or revoke) the access rights if necessary.	Der LIEFERANT überprüft die Zugriffsrechte seiner Mitarbeiter in regelmäßigen Abständen und ändert (d.h. beschränkt/widerruft) sie, falls erforderlich.
Patch Management	**Patch Management**
The SUPPLIER periodically analyzes systems (operating systems, applications, network components) for known vulnerabilities. Patches are applied in a consistent, standardized manner and prioritized based on criticality. If the root cause of vulnerabilities could not be mitigated within reasonable time, alternative risk mitigation measures must be implemented until the root cause is remedied. The SUPPLIER has implemented an emergency change process.	Der LIEFERANT analysiert regelmäßig die Systeme (Betriebssysteme, Anwendungen, Netzkomponenten) auf bekannte Schwachstellen. Patches werden in einer konsistenten, standardisierten Weise angewendet und nach ihrer Kritikalität priorisiert. Wenn die Ursache von Schwachstellen nicht innerhalb eines angemessenen Zeitraums beseitigt werden kann, müssen bis zur Behebung alternative Maßnahmen zur Risikominderung ergriffen werden. Der LIEFERANT hat einen Notfall-Changeprozess implementiert.

Network Security	Netzwerksicherheit
The SUPPLIER has implemented and maintained network security infrastructure components such as firewalls, intrusion detection/prevention systems (IDS/IPS) and other security controls, providing detection, continuous monitoring, and restrictive network traffic flow to assist in limiting the impact of attacks. Systems with a higher risk level (e.g. externally exposed) must have stricter measures in place.	Der LIEFERANT hat Komponenten der Netzsicherheitsinfrastruktur wie Firewalls, Intrusion Detection/Prevention Systeme (IDS/IPS) und andere Sicherheitskontrollen implementiert und aufrechterhalten, die eine Erkennung, kontinuierliche Überwachung und eine Einschränkung des Netzwerk Traffics ermöglichen, um die Auswirkungen von Angriffen zu begrenzen. Für Systeme mit einer höheren Risikostufe (zB. für einen Zugriff von externen Netzwerken erreichbar) müssen strengere Maßnahmen ergriffen werden.
The SUPPLIER ensures that a formal remote access policy is in place.	Der LIEFERANT stellt sicher, dass eine formelle Fernzugriffsrichtlinie vorhanden ist.
The SUPPLIER ensures segregation and segmentation of the environments according to industry standards, when: (1) environments are shared with other customers; and/or (2) SUPPLIER implements test, quality and production environments.	Der LIEFERANT stellt die Trennung und Segmentierung der Umgebungen gemäß den Industriestandards sicher, wenn: (1) Umgebungen gemeinsam mit anderen Kunden genutzt werden; und/oder (2) der LIEFERANT Test-, Qualitäts- und Produktionsumgebungen einrichtet.
Encryption	**Verschlüsselung**
The SUPPLIER ensures an appropriate level of protection of data confidentiality. The SUPPLIER must also consider specific measures for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture. The encryption is compliant to leading standards and guidelines or equivalent (e.g. National Institute of Standards and Technology - NIST).	Der LIEFERANT gewährleistet einen angemessenen Schutz der Vertraulichkeit der Daten. Der LIEFERANT muss auch spezifische Maßnahmen für Daten bei der Übertragung sowie in flüchtigen und persistenten Speicher berücksichtigen, wie z. B. die Verwendung von Verschlüsselungstechnologien in Kombination mit einer geeigneten Schlüsselverwaltungs-architektur. Die Verschlüsselung entspricht den führenden Standards und Richtlinien oder gleichwertigen Standards (zB. National Institute of Standards and Technology - NIST).
The SUPPLIER protects mobile devices and external electronic media (e.g. USB memory storage, tape) against unauthorized access, through adequate physical and logical security measures. Data-at-rest encryption on these devices must be enforced.	Der LIEFERANT schützt mobile Geräte und externe elektronische Medien (zB. USB-Speicher, Band) durch angemessene physische und logische Sicherheitsmaßnahmen vor unbefugtem Zugriff. Die Verschlüsselung von auf diesen Geräten gespeicherten Daten muss durchgesetzt werden.
Malware Protection	**Schutz vor Schadsoftware**
The SUPPLIER protects servers and endpoints with proper Malware protection which is kept up to date. The software must detect if anti-virus/malware software on devices has been disabled or not receiving regular updates.	Der LIEFERANT schützt die Server und Endgeräte mit einem angemessenen Schutz vor Malware, der stets auf dem neuesten Stand gehalten wird. Die Software muss erkennen, ob die Antiviren-/Malware-Software auf den Geräten deaktiviert wurde oder nicht regelmäßig aktualisiert wird.
Security Testing, Monitoring & Reporting	**Sicherheitsprüfung, Überwachung und Reporting**
The SUPPLIER has appropriate security measures (in particular related to cyber threats) for data, applications and systems. The SUPPLIER periodically evaluates the effectiveness of security measures related to known cyber threats and frauds as well as respective models (e.g. based on up-to-date threat catalogues like National Institute of Standards and Technology, Bundesamt für Sicherheit in der Informationstechnik).	Der LIEFERANT verfügt über angemessene Sicherheitsmaßnahmen (insbesondere im Hinblick auf Cyber-Bedrohungen) für Daten, Anwendungen und Systeme. Der LIEFERANT evaluiert regelmäßig die Wirksamkeit der Sicherheitsmaßnahmen in Bezug auf bekannte Cyber-Bedrohungen und Betrugsfälle sowie entsprechende Modelle (zB. auf der Grundlage aktueller Bedrohungskataloge wie National Institute of Standards and Technology, Bundesamt für Sicherheit in der Informationstechnik).

The SUPPLIER has periodic plans and executes Vulnerability Assessments and Penetration Tests on systems used to provide service to the CUSTOMER. Penetration Tests on these systems have to be conducted in the following manner: (1) at least once a year (2) in case of a major release/updates of applications/software/information services (3) Penetration tests are carried out by testers with sufficient knowledge, skills and expertise and who were not involved in the development of the security measures. The discovered vulnerabilities and the findings must be managed appropriately: Analysis, classification and remediation. Mitigation actions must be performed according to their criticality in a timely manner. The SUPPLIER must provide summary result reports of Vulnerability Assessments and/or Penetration Tests on demand.	Der LIEFERANT plant und führt in regelmäßigen Abständen Schwachstellenanalysen und Penetrationstests für die Systeme durch, die zur Erbringung der Dienstleistung für den KUNDEN eingesetzt werden. Penetrationstests für diese Systeme müssen in folgender Weise durchgeführt werden: (1) mindestens einmal pro Jahr (2) im Falle einer größeren Release/Aktualisierung von Anwendungen/Software/Informations-diensten (3) Penetrationstests werden von Testern mit ausreichenden Kenntnissen, Fähigkeiten und Erfahrungen durchgeführt, die nicht an der Entwicklung der Sicherheitsmaßnahmen beteiligt waren. Die aufgedeckten Schwachstellen und die Ergebnisse müssen in geeigneter Weise verwaltet werden: Analyse, Klassifizierung und Behebung. Die Abhilfemaßnahmen müssen entsprechend ihrer Kritikalität zeitnah durchgeführt werden. Der LIEFERANT muss auf Anfrage zusammenfassende Ergebnisberichte von Schwachstellenbewertungen und/oder Penetrationstests zur Verfügung stellen.
The SUPPLIER ensures that security issues identified and reported by the CUSTOMER are resolved within a reasonable timeframe.	Der LIEFERANT stellt sicher, dass vom KUNDEN gemeldete Sicherheitsprobleme innerhalb eines angemessenen Zeitrahmens behoben werden.
The CUSTOMER reserves the right to perform security assessments to verify compliance with here listed requirements. The CUSTOMER notifies the SUPPLIER in advance and ensures the audit is performed during normal business hours, and with minimal disruption to the SUPPLIER's business operations. Upon request, the SUPPLIER must confirm, in writing, the SUPPLIER's compliance with the requirements of here listed requirements and provide written responses to any questions that the CUSTOMER presents to the SUPPLIER regarding its security practices.	Der KUNDE behält sich das Recht vor, Sicherheitsbewertungen durchzuführen, um die Einhaltung der hier aufgeführten Anforderungen zu überprüfen. Der KUNDE benachrichtigt den LIEFERANTEN im Voraus und stellt sicher, dass das Audit während der normalen Geschäftszeiten und mit minimaler Unterbrechung des Geschäftsbetriebs des LIEFERANTEN durchgeführt wird. Auf Anfrage muss der LIEFERANT die Einhaltung der hier aufgeführten Anforderungen schriftlich bestätigen und alle Fragen des KUNDEN an den LIEFERANTEN zu seinen Sicherheitsverfahren schriftlich beantworten.
System Hardening	**System Hardening**
The SUPPLIER has configured and deployed their ICT assets (e.g. databases, applications, operating systems, network devices) using a secure baseline (hardening). The secure baseline is based on best practices (e.g. CIS standards) or equivalent. The hardening configurations on the ICT assets are periodically reviewed and updated.	Der LIEFERANT hat seine IT-Ressourcen (zB. Datenbanken, Anwendungen, Betriebssysteme, Netzwerkgeräte) unter Verwendung einer sicheren Grundlage (Hardening) konfiguriert und eingesetzt. Die Sicherheitsgrundlagen basieren auf Best Practices (zB. CIS-Standards) oder gleichwertigen Verfahren. Die Konfigurationen für die IT-Anlagen werden regelmäßig überprüft und aktualisiert.

ICT Operations	ICT Betrieb
Data Management	**Data Management**
The SUPPLIER ensures that measures against data loss and leakage are in place.	Der LIEFERANT stellt sicher, dass Maßnahmen gegen Datenverlust und -abfluss getroffen werden.
The SUPPLIER must not replicate CUSTOMER production data or use it in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from the CUSTOMER.	Der LIEFERANT darf keine Produktionsdaten des KUNDEN replizieren oder in Nicht-Produktionsumgebungen verwenden. Jede Verwendung von Kundendaten in Nicht-Produktionsumgebungen bedarf der ausdrücklichen, dokumentierten Zustimmung des KUNDEN.
Backup & Recovery	**Backup & Recovery**
The SUPPLIER ensures that backup and data retention concepts exist for each relevant platform/component under the responsibility of the SUPPLIER. Backups, retention periods and recovery tests are performed. Backup concepts and recovery procedures are suitable to ensure agreed availability levels.	Der LIEFERANT stellt sicher, dass für jede relevante Plattform/Komponente im Verantwortungsbereich des LIEFERANTEN Sicherungs- und Datenhaltungskonzepte existieren. Backups, Aufbewahrungsfristen und Wiederherstellungstests durchgeführt werden. Die Sicherungskonzepte und Wiederherstellungs-verfahren sind geeignet, die vereinbarten Verfügbarkeitsstufen zu gewährleisten.
Logging & monitoring	**Logging & Monitoring**
The SUPPLIER has adopted appropriate measures in order to ensure accountability and traceability of operations carried out. Logs must provide sufficient details to assist in the identification of the source of an (security) issue and enable a series of events to be recreated. Logs must be provided to the CUSTOMER if the CUSTOMER has justified reasons. Logs must record access attempts, system and network security event information, alerts, failures and errors. Integrity of log files must be ensured. Access to log files must be restricted.	Der LIEFERANT hat geeignete Maßnahmen ergriffen, um die Nachvollziehbarkeit und Rückverfolgbarkeit der durchgeführten Vorgänge zu gewährleisten. Die Protokolle müssen ausreichende Angaben enthalten, um die Ursache eines (Sicherheits-)Problems zu ermitteln und die Wiederherstellung einer Reihe von Ereignissen zu ermöglichen. Die Protokolle müssen dem KUNDEN zur Verfügung gestellt werden, wenn der KUNDE berechtigte Gründe hat. In den Protokollen müssen Zugriffsversuche, Informationen über System- und Netzsicherheits-ereignisse, Warnungen, Ausfälle und Fehler aufgezeichnet werden. Die Integrität der Protokolldateien muss gewährleistet sein. Der Zugang zu den Protokolldateien muss eingeschränkt werden.
Incident Management & Reporting	**Incident Management & Reporting**
The SUPPLIER must have documented information Security Incident procedures, enabling effective and orderly management of Security Incidents. The procedures must cover the reporting, analysis, monitoring, resolution and documentation of Security Incidents.	Der LIEFERANT muss über dokumentierte Verfahren für Informationssicherheitsvorfälle verfügen, die eine wirksame und ordnungsgemäße Handhabung von Sicherheitsvorfällen ermöglichen. Die Verfahren müssen die Meldung, Analyse, Überwachung, Lösung und Dokumentation von Sicherheitsvorfällen umfassen.
SUPPLIER notifies CUSTOMER without undue delay after becoming aware of an Incident which is directly or indirectly in connection with CUSTOMER related Services and Data and provide reasonable information in its possession to assist CUSTOMER to meet CUSTOMER'S obligations. SUPPLIER provides such information in phases as it becomes available. After verification of a security incident in connection with CUSTOMER related Services or Data, the SUPPLIER shall: i. provide written notification to the CUSTOMER´s Business Units and additionally to contacts defined in the contract and in time-critical cases or imminent danger also call R-IT's Help-Desk without undue delay.	Der LIEFERANT benachrichtigt den KUNDEN unverzüglich nach Bekanntwerden eines Vorfalls, der direkt oder indirekt mit den Diensten und Daten des KUNDEN zusammenhängt, und stellt alle ihm zur Verfügung stehenden Informationen zur Verfügung, um den KUNDEN bei der Erfüllung seiner Verpflichtungen zu unterstützen. Der LIEFERANT stellt diese Informationen schrittweise zur Verfügung, sobald sie verfügbar werden. Nach der Überprüfung eines Sicherheitsvorfalls in Verbindung mit den Diensten oder Daten des KUNDEN wird der LIEFERANT: i. die Geschäftsbereiche des KUNDEN und zusätzlich die im Vertrag definierten Kontakte schriftlich

ii. the notification shall include at least following details, if initially not all information is available, the SUPPLIER should provide details or imminent danger as soon as they are known in a staged reporting: • Contact information of SUPPLIER incident responsible • What occurred • How occurred • Why occurred • Components / assets affected • CUSTOMER services / data affected • Date and time the incident occurred • Date and time the incident was discovered • Business impact / effect for CUSTOMER services / data • Incident resolution • Action taken to resolve incident • Action planned to resolve incident iii. use all reasonable efforts to avoid and detect such incidents; iv. continuously inform the CUSTOMER of the measures the SUPPLIER is taking or intends to take; v. obtain the CUSTOMER´s prior written approval pursuant to Applicable Law in connection with any notification or public information with respect to such breach, and vi. coordinate any further activities with the CUSTOMER. vii. this reporting obligation also applies to sub-contractors	benachrichtigen und in zeitkritischen Fällen oder bei Gefahr im Verzug auch den Help-Desk von R-IT unverzüglich anrufen. ii. Die Meldung hat mindestens folgende Angaben zu enthalten, wenn zunächst nicht alle Informationen vorliegen, sollte der LIEFERANT die Angaben bei zeitkritischen Fällen oder Gefahr im Verzug sofort nach Bekanntwerden in einer gestaffelten Meldung nachliefern: - Kontaktinformationen der Person beim LIEFERANTEN, die für den Vorfall verantwortlich ist - Was ist passiert? - Wie ist es passiert - Warum ist es geschehen? - Betroffene Komponenten/Anlagen - Betroffene Dienste/Daten des KUNDEN - Datum und Uhrzeit des Auftretens des Vorfalls - Datum und Uhrzeit der Entdeckung des Vorfalls - Auswirkung auf das Geschäft / Auswirkungen auf KUNDEN-Services/ -Daten - Lösung des Vorfalls - Ergriffene Maßnahmen zur Behebung des Vorfalls - Geplante Maßnahmen zur Behebung des Vorfalls iii. alle angemessenen Anstrengungen zu unternehmen, um solche Vorfälle zu vermeiden und zu entdecken; iv. den KUNDEN laufend über die Maßnahmen zu informieren, die der LIEFERANT ergreift oder zu ergreifen beabsichtigt; v. die vorherige schriftliche Zustimmung des KUNDEN gemäß dem anwendbaren Recht in Verbindung mit jeglicher Benachrichtigung oder öffentlichen Information in Bezug auf eine solche Verletzung einzuholen, und vi. alle weiteren Aktivitäten mit dem KUNDEN zu koordinieren. vii. diese Meldepflicht gilt auch für Subauftragnehmer
Physical Security	**Physische Sicherheit**
Physical Access	**Physischer Zugang**
The SUPPLIER has categorized its premises into different protection zones, reflecting certain security measures and access rights according to the relevant security needs.	Der LIEFERANT hat seine Räumlichkeiten in verschiedene Schutzzonen eingeteilt, die bestimmte Sicherheitsmaßnahmen und Zugangsrechte entsprechend den jeweiligen Sicherheitsanforderungen widerspiegeln.
Access to IT systems such as servers is further restricted with special protection zones for authorized personnel only.	Der Zugang zu IT-Systemen wie zB. Servern ist durch spezielle Schutzzonen, die nur für befugtes Personal zugänglich sind, weiter eingeschränkt.
Only secure data center facilities must be used to store CUSTOMER data.	Für die Speicherung von Daten des KUNDEN dürfen nur sichere Rechenzentren verwendet werden

Business Continuity Management	Business Continuity Management
BCM	**BCM**
The SUPPLIER has up to date and maintained Disaster Recovery Plans and Business Continuity Plans in place. The Disaster Recovery Plans and Business Continuity Plans must be designed to prevent negativ impacts by unplanned disruptions to maximum possible extend and to ensure, that the SUPPLIER can continue to function through operational interruption and continue to provide Services as specified in its agreement with the CUSTOMER. The SUPPLIER will provide the CUSTOMER written summaries of its Disaster Recovery Plans and Business Continuity Plans upon request.	LIEFERANT verfügt über aktuelle und aufrechterhaltene Notfallpläne und Pläne zur Aufrechterhaltung des Geschäftsbetriebs. Die Disaster-Recovery-Pläne und Business-Continuity-Pläne müssen so konzipiert sein, dass negative Auswirkungen durch ungeplante Unterbrechungen so weit wie möglich verhindert werden und dass der LIEFERANT auch bei Betriebsunterbrechungen weiterarbeiten und die Dienstleistungen gemäß dem Vertrag mit dem KUNDEN erbringen kann. Der LIEFERANT stellt dem KUNDEN auf Anfrage schriftliche Zusammenfassungen seiner Disaster-Recovery-Pläne und Business-Continuity-Pläne zur Verfügung.
The SUPPLIER performs at least annual, adequate tests of their own Business Continuity Plans and Disaster Recovery Plans. Service relevant test results must be provided to the CUSTOMER on demand or at least if the tests have been carried out.	LIEFERANT führt mindestens einmal jährlich angemessene Tests seiner eigenen Business-Continuity- und Disaster-Recovery-Pläne durch. Servicerelevante Testergebnisse sind dem KUNDEN auf Verlangen, zumindest aber nach Durchführung der Tests zur Verfügung zu stellen.
The SUPPLIER has ensured the scope of the Business Continuity Plans and Disaster Recovery Plans encompasses all locations, personnel and information systems used to perform or provide services for the CUSTOMER.	LIEFERANT hat sichergestellt, dass der Geltungsbereich der Business Continuity- und Notfallwiederherstellungspläne alle Standorte, Mitarbeiter und Informationssysteme umfasst, die zur Erbringung von Dienstleistungen für den KUNDEN eingesetzt werden.

AGREEMENT ON ORDER PROCESSING IN ACCORDANCE WITH ARTICLE 28 GDPR

entered into by and between

Raiffeisen Informatik Consulting GmbH

Lilienbrunngasse 7-9

A-1020 Vienna

VENDOR

(hereinafter referred to as the "**Controller**" and/or the "**Processor**")

(hereinafter referred to as the "**Processor**" and/or the "**Sub Processor**")

(hereinafter referred to jointly as "**Parties**")

as follows:

1. The parties have concluded individual agreements (hereinafter referred to as "basic agreement"). The activities performed by the processor and/or sub processor under the basic agreement also include the processing of personal data for the benefit of the controller and/or processor. In addition to the basic agreement, the controller and/or processor and the processor and/or sub processor conclude this agreement for the comprehensive regulation of the data protection aspects of these activities. This agreement shall be concluded for the duration of the basic agreement and thus ends at the same time as the basic agreement.

2. The details of the respective data processing, ie (i) the nature and purpose of the data processing, (ii) the types of personal data and (iii) the categories of data subjects are listed and described in Appendix 2. In the case of changes in data processing under the contracts listed in Appendix 2 or in the event of termination, amendment or new conclusion of contracts, the parties will adapt, undertake and exchange Appendix 2, whereby the electronic transmission of copies of Appendix 2 shall suffice.

3. The processor and/or sub processor undertake to comply with the provisions of all applicable Austrian and European data protection law. These include in particular the following obligations:

    a. The processor and/or sub processor undertake to process personal data only in accordance with this Agreement or otherwise on the instructions of the controller and/or processor, unless subject to the law of the European Union or of the Member States, the processor and/or sub processor is obliged to do so; in such a case, the processor and/or sub processor shall inform the controller and/or processor of such legal requirements prior to processing, unless the law prohibits such communication on grounds of significant public interest.

    b. Data processing shall take place exclusively within the EU. Data processing in a third country outside the EU requires the prior written consent of the controller

and/or processor and compliance with the requirements of Article 44 et seq. GDPR.

c. The processor and/or sub processor guarantee that persons authorized to process the personal data have undertaken to maintain confidentiality or are subject to an appropriate statutory confidentiality obligation. In particular, the confidentiality obligation of the persons responsible for data processing remains in force even after the termination of their duties and their departure from the processor and/or sub processor. The obligation of confidentiality must also be observed for data of legal entities and commercial partnerships.

d. The processor and/or sub processor shall declare that it has taken sufficient technical and organizational measures within the meaning of Article 32 of the GDPR to ensure adequate personal data protection as regards the confidentiality, integrity and availability of the data and the resilience of the systems, and preventing data from being misused or made accessible to third parties without authorization. The technical and organizational measures to be followed by the processor and/or sub processor are described in more detail in Appendix 1. The processor and/or sub processor shall document the implementation of the technical and organizational measures. The technical and organizational measures are subject to technical progress and further development. In that regard, the processor and/or sub processor are allowed to implement adequate measures as an alternative. In doing so, the safety level of the specified measures must remain the same. Significant changes must be documented.

e. The controller and/or processor hereby grant general approval for the assignment of further sub processors by the processor and/or sub processor in relation to order processing. However, the processor and/or sub processor undertakes to inform the controller and/or processor of any intended use or replacement of additional sub processors. The controller and/or processor may object to such changes. If the other sub processor provides the agreed service outside of the EU, the processor and/or sub processor shall ensure that the data protection law is permissible through appropriate measures. If the processor and/or sub processor avail themselves of the services of another sub processor to carry out certain processing activities of the controller and/or processor, that other sub processor shall be bound, by contract, to the same data protection obligations as laid down in this contract. If the other sub processor fails to fulfil its data protection obligations, the processor and/or sub processor shall be liable to the controller and/or processor for compliance with the obligations of that additional sub processor.

f. The processor and/or sub processor shall undertake to assist the controller and/or processor with appropriate technical and organizational measures to fulfil the controller and/or processor's obligation to reply to requests for the rights of the data subject, in particular to provide information, rectify or delete them (Art 22 DSGVO), in order to comply.

g. Furthermore, the processor and/or sub processor undertakes to assist the controller and/or processor in complying with the obligations regarding the security of personal data referred to in Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to him.

h. In the event of a breach of data protection, the processor and/or sub processor shall immediately inform the controller and/or processor. The processor and/or sub processor shall assist the controller and/or processor in reporting the

breach of data protection obligations to the supervisory authority and to the parties concerned and shall provide all relevant information without delay.

i. The processor and/or sub processor shall assist the controller and/or processor in complying with his obligations in a data protection impact assessment (Art. 35 DSGVO). In particular, the processor and/or sub processor shall provide the controller and/or processor with relevant information on data processing, technical and organizational measures, and assist in the assessment of risks and any adjustments to technical and organizational measures.

j. The processor and/or sub processor undertakes, at the discretion of the controller and/or processor, upon completion of the data processing either to delete or destroy, in compliance with data protection statutes, all personal data, including any obtained documents, processing results and the data sets related to the data processing, or hand it over to the controller and/or processor.

k. The obligation to return or to delete data according to the previous paragraph does not apply, if there is an obligation to store the personal data according to the EU law or the law of a member state of the EU.

l. The processor and/or sub processor shall provide the controller and/or processor with all necessary information to demonstrate compliance with the obligations set out in this agreement and provide all necessary information when requested to do so. The processor and/or sub processor shall facilitate and contribute to inspections by the controller and/or processor or an inspector appointed by the controller and/or processor. In case of substantive justified objections against the inspector the processor and/or sub processor may object to the selection of such named inspector.

   In case of similar data processing operations for several controllers and/or processors, the processor and/or sub processor also authorizes inspections by auditors jointly appointed by the involved controllers and/or processors or alternatively commissions - on request or with consent and for the account of the controllers and/or processors - such audits by appropriate entities (e.g. internal auditors, certified public accountants, IT security auditors, data privacy auditors, quality auditors). The resulting audit reports shall be provided to the controllers and/or processors and their respective auditors and - upon request - to the supervisory authorities responsible for the controllers and/or processors.

m. The processor and/or sub processor shall assist the controller and/or processor in investigations or procedures of supervisory authorities and in the performance of obligations to supervisory authorities. The processor and/or sub processor shall immediately inform the controller and/or processor of any investigation or action taken by supervisory authorities in relation to order processing for the controller and/or processor. In addition, where the controller and/or processor is subject to investigations or action by supervisory authorities, administrative or criminal proceedings or claims by data subjects or third parties in relation to order processing, the processor and/or sub processor shall assist him to the best of his ability.

n. The processor and/or sub processor shall inform the controller and/or processor without delay if an instruction violates the GDPR or other applicable data protection legislation. The processor and/or sub processor may suspend the execution of the relevant instruction until it is confirmed or changed by the controller and/or processor.

In the case of contradictions between the regulations of the contract and the regulations of this Agreement and its Appendixes on data protection this present Agreement shall prevail. Appendix 1 and 2 shall be an integral part of the Agreement.

If any parts of this Agreement or of its Appendixes are ineffective, effectiveness of the residual Agreement and its Appendixes shall not be affected

Annex 1: Technical and organizational measures
Annex 2: Data processing under the basic agreement

For the person responsible and/or the processor:	For the processor and/or sub-processor:
……	……
DI (FH) Arno GRUBER, CEO	Name, Signature
……	……
Andreas SIDLO, COO/CFO	..
	Place, Date
Vienna, …….	

Appendix 1

Technical and Organisational Measures

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

- **Physical Access Control**
  Protection against unauthorised access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, security staff, porter, alarm systems, video/CCTV Systems
- **Electronic Access Control**
  Protection against unauthorised use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords (including a relevant policy), automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media
- **Internal Access Control** No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g.: standard authorisation profiles on a need-to-know basis, standard procedure for granting authorisations, keeping access logs, periodical review of the authorisations granted, including but not limited to administrative user accounts; separated Processing of Data, which is collected for differing purposes, e.g. multiple Controller and/or Processor support, sandboxing
- **Pseudonymisation** (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)
  If expedient for the relevant data processing activities, the primary identification features of the personal data will be removed from the relevant data application and kept separately.
- **Data classification scheme**
  According to statutory obligations or self-assessment (secret/confidential/in-house/public).

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

- **Data Transfer Control**
  No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;
- **Data Entry Control**
  Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

- **Availability Control** Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS, diesel generator set), anti-virus program, firewall, reporting procedures and emergency planning; security checks at infrastructure and application level, multi-stage backup concept including encrypted outsourcing of backups to a backup data centre, standard processes for cases where staff changes or leaves the undertaking
- **Rapid Recovery** (Article 32 Paragraph 1 Point c GDPR);
- **Erasure periods**
  Both for the data itself and for meta data, such as log files and the like

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

- Data Protection Management, including regular staff training;
- Incident Response Management;
- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);

- Order or Contract Control
  No third party data processing as per Article 28 GDPR without corresponding instructions from the Controller and/or Processor, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.

Appendix 2 – Data processing under the basic agreement

Controller and/or Processor: **Raiffeisen Informatik Consulting GmbH**
Data Protection Officer RI-C: **Dr. Ulrike Haas, LL.M. /datenschutz@ri-c.at**

Processor and/or Sub Processor: **VENDOR**

Data Protection Officer: ……

Subject matter of the Agreement	Nature and purpose of the envisaged processing of data	Data Subject categories	Type of data
According to the basic agreement	1. Support The object of the processing is the maintenance, care and support of the Customer's systems in which the Contractor's software products are integrated and for which a maintenance contract has been concluded.	Staff Relatives of employees Applicants Contracting parties Persons affected by image processing Potential customers and prospects Clients Collateral giver Owner of the person responsible of the Controller Organs and functionaries of the Controller Visitors and other authorised persons Corporate bodies and employees of Group companies and sector institutions	Personal minimum information Personal details Household data and family circumstances Identification data of public authorities/organisations Contact Details Training data and technical, social and methodological qualification data CV data Data on occupation and employment relationship Residence Status Assessments, assessments in connection with employment relationship Wage and salary data Tax data and social security data Work organisation data Public mandates Shareholdings, executive functions, powers of representation

			Habits of life and consumption Electronic identification data Electronic location and movement data image recordings Sound recordings Creditworthiness data Financial identification data Data on lending business Data on deposit-taking business Financial Forward Derivatives Data Data on cash market or custody business, securities custody & administration insurance data Payment transaction and clearing data Data on leasing business Fleet management business data Data on property development business Rental business data AML (Anti Money Laundering) and Compliance Data Marketing and sales data Data on safes Racial and ethnic origin (S) Political opinion (S) Trade union membership (S) Religious or ideological beliefs (S) Genetic identification data (S) Biometric identification data (S) Health data (S) Data on sex life/orientation (S) Data on criminal convictions and offences (S) Physical description data (S)

	2. Licensing Processing of customer data and user data within the scope of Software as a Service (SaaS) licensing	Staff Relatives of employees Applicants Contracting parties Persons affected by image processing Potential customers and prospects Clients Collateral giver Owner of the person responsible of the Controller Organs and functionaries of the Controller Visitors and other authorised persons Corporate bodies and employees of Group companies and sector institutions	Personal minimum information Personal details Household data and family circumstances Identification data of public authorities/organisations Contact Details Training data and technical, social and methodological qualification data CV data Data on occupation and employment relationship Residence Status Assessments, assessments in connection with employment relationship Wage and salary data Tax data and social security data Work organisation data Public mandates Shareholdings, executive functions, powers of representation Habits of life and consumption Electronic identification data Electronic location and movement data image recordings Sound recordings Creditworthiness data Financial identification data Data on lending business Data on deposit-taking business Financial Forward Derivatives Data Data on cash market or custody business, securities custody & administration insurance data Payment transaction and clearing data Data on leasing business

			Fleet management business data Data on property development business Rental business data AML (Anti Money Laundering) and Compliance Data Marketing and sales data Data on safes Racial and ethnic origin (S) Political opinion (S) Trade union membership (S) Religious or ideological beliefs (S) Genetic identification data (S) Biometric identification data (S) Health data (S) Data on sex life/orientation (S) Data on criminal convictions and offences (S) Physical description data (S)

For the Controller and/or the Processor:

……
DI (FH) Arno GRUBER, CEO

……
Andreas SIDLO, COO/CFO

Vienna, ……

For the Processor and/or Sub-processor:

……
Name, Signature

…… ..
Place, Date

Outsourcing SCHEDULE

Raiffeisen Informatik Consulting GmbH as well as its Affiliates (hereinafter "*Customer*") and Supplier [*** INSERT NAME AND ADDRESS OF SUPPLIER] (hereinafter "*Supplier*") and together with the Customer the „*Parties*" and each a „*Party*") have entered on [***INSERT DATE OF AGREEMENT] into a [*** INSERT NAME OF THE AGREEMENT] (the „*Agreement*") on outsourcing specific services and activities of Customer (each an "*Outsourced Service*" and together the "*Outsourcing*" or the "*Outsourced Services*"), which Customer, without the Agreement, would have to perform on its own.

Since several Customer's Affiliates qualify as a „financial institution" pursuant to EU Regulation 2013/575 respectively under § 1 of the BWG (the Austrian Banking Act), Customer when outsourcing activities has to comply with outsourcing prerequisites. Inter alia Customer has to make sure that Supplier

a) when performing the Outsourced Services, will apply the same due diligence and service quality criteria, as Customer if Customer would not have outsourced the Services under the Agreement,

b) complies with specific rules and regulations and applies certain quality criteria and quality checks as described in Outsourcing Requirements, and

Having said so, the Parties herewith agree, that this Outsourcing Schedule is integral part of the Agreement. Terms used in this Schedule have, unless otherwise defined herein, the meaning as in the Agreement. If any provision in the Agreement stands in conflict with any of the provisions of this Schedule, the terms of this Schedule take precedence and thus, will and do amend, supersede and replace any of the provision of the Agreement being so in conflict or contradiction with the provision of this Schedule.

Supplier's Representations and Warranties

In addition to any other representations and warranties provided by Supplier under the Agreement, Supplier herewith represents and warrants to Customer that Supplier

a) is aware that, to the extent Customer is being made subject to or has to undertake, any crisis prevention or crisis management measure („eine Krisenpräventions- oder Krisenmanagementmaßnahme") or a reorganisation procedure („Abwicklungsverfahren") pursuant to Austria's federal legal act on the restructuring and reorganisation of banks („Bundesgesetzes über die Sanierung und Abwicklung von Banken", BGBl I 2018/37 („BaSAG") is being initiated in relation to it, the Agreement may, in accordance with the BaSAG, be made subject to termination provisions other than agreed to between the Parties and inter alia having the effect that the Agreement cannot be ended in accordance with its terms. In case of such termination provisions, Customer will pay all the outstanding Fees applicable under this Agreement, 75o GL[1]

b) has irrevocably and unconditionally entitled Customer to disclose a copy of the Agreement together with any amendments and changes made to it and any information related to any of the aforesaid to Customer's Competent Authorities, and

c) has available a business continuity plan inter alia indicating to which risks Supplier is being exposed to, which may have the effect of partial or full interruption or discontinuation of Supplier's services and the measures Supplier would put into effect to mitigate such risks. Supplier undertakes to provide Customer with a written copy of such plan, or a summary thereof, within, at the latest, one month after the date of the Agreement.

[1] EBA Guidelines on Outsourcing (EBA/GL/2019/02)

Outsourcing Requirements

Code of Conduct

Supplier is fully aware of Customer's „Code of Conduct" and confirms and acknowledges on its own behalf and on behalf of any sub-contractors Supplier may have assigned for performing the Outsourced Services to always act in compliance with the values as laid down in such Code of Conduct, act in an ethical and socially responsible manner and in such a way that international standards on human rights (e.g. the European Convention on Human Rights), environmental protection and appropriate working conditions, including the prohibition of child labor, are being adhered to; 73GL

Security

Supplier complies with the Customer's security standards and imposes these standards to its Subcontrators. Additional security related duties might arise and would be separately requested.

Performance Report

Supplier undertakes to furnish Customer at his own cost (unless the bearing of cost has been otherwise agreed in the Agreement) and at a minimum once a year (alternatively, if otherwise agreed in the Agreement, more often) and within thirty (30) business days upon Customer's demand with a written performance report, giving details about which specific Outsourced Services have been performed in which time and manner since the last such reporting 22b, 75h, i, j GL

Supplier will in this report provide Customer with information on any performance insufficiency or performance interruption as well as how Supplier dealt with any Customer reminder in relation to the details of any insufficiency or interruption (whether actually persisting or only assumed by Customer) so that a reader of such report will realize at which times or during which time periods such insufficiencies or interruptions persisted. In the report Supplier will also give details about which risks Supplier has identified, which may have the effect of a partial or full interruption or discontinuation of Supplier's services when performing the Outsourced Services and the measures Supplier has put into effect to mitigate or otherwise cope with such risks. In any event Supplier will give details about the risk of Supplier being unable to safeguard its own business continuity in relation to the outsourced services. If Supplier processes, stores or generates data received from or sent to Customer and such data gets lost or cannot be processed, stored, generated, received or sent within the time and/or quality limits as agreed between the parties, Supplier will without undue delay after realizing that any of the aforesaid insufficiencies subsist, inform Customer about such insufficiencies; 22b**, 23a,** 75h, i, j, k, 100, 104c, 105GL

Operational Monitoring and Shortcomings Reporting

Supplier undertakes to submit to an independent quality audit for the period in which the Outsourced Services is agreed to be performed and to ensure that such independent auditor will do a written audit report at least on an annual basis. The Supplier further ensures that the customer will be furnished with such report at the latest within fourteen days after its issuance. In case the Supplier has an internal audit unit, the Supplier will provide the Customer with any report (in addition to the quality reports mentioned hereabove) made by such audit unit and related to any of the Outsourced Services. Any such reports are due to be delivered on an annual basis at a minimum and at the latest within fourteen days after their issuance. On demand of the Customer the Supplier further undertakes to furnish the Customer at any time with any license or authorization required to have or any other decree or certificate required for performing the Outsourced Services. If any of such licenses, authorizations, decrees or certificates are being revoked, are outdated without being properly renewed or otherwise cease to be in effect, the Supplier undertakes to immediately thereafter give notice to this effect to the Customer. The Supplier confirms to have and undertakes at all times to keep (at its own cost) during the term of the Outsourcing all such licenses, authorizations, decrees or certificates (including, but not limited to any certificates in relation to IT-security); 22b, **23a**, 62, 72, 75j, 81, 100, **104bGL**

Data Privacy and Data Protection

Supplier is fully aware of the terms and provisions of Regulation (EU) 2016/679 (General Data Protection Regulation) as implemented pursuant to Austria's federal act on data protection ("Datenschutzgesetz idF BGBl I Nr. 14/2019"), the requirements to keep banking information secret pursuant to § 38 of Austria's federal law on banking ("Bankwesengesetz idF BGBl I Nr. 17/2018") and generally to keep corporate data secret inter alia according to Regulation (EU) 2016/943 as implemented pursuant to §§ 26a – 26j of Austria's federal act on unfair competition ("Bundesgesetz gegen den unlauteren Wettbewerb idF BGBl I Nr. 109/2018"). This awareness is also encompassing knowledge about which specific data protection and confidentiality duties Supplier is being bound to in relation to the Outsourcing. in the event Supplier processes, stores, or generates data received from or sent to Customer, Supplier undertakes to refrain from storing any such data in a cloud-computing environment or on any storage device which is located in or accessible from outside the EU without having, obtained the prior written consent of Customer; 54f, h, 84 GL (**IT**) 40d, 84 GL

Further details are provided in the GDPR Schedule of the Agreement.

Post-termination Support

In the event the Agreement is being terminated (and provided the outsourcing service fees are being paid when due and that Customer is in compliance with all of its major duties and liabilities according to the terms of the Agreement; notwithstanding its termination), Supplier undertakes to continue performing the Outsourced Services up to and until the point in time when Customer confirms to Supplier that Customer is performing such services on its own or that such services have been outsourced to another Supplier, [whichever is earlier]. Up to and until the time when Supplier actually (but in accordance with the terms of this Schedule) discontinues with the performance of the Outsourced Services, Supplier further undertakes, to put Customer (with Customer's assistance, and at Customer's cost and expense) back into a position in which Customer will be enabled again (and where such enablement shall include the return of all data, information and all other auxiliary material) to fully perform the Outsourced Services on its own (or to transfer the duty to perform such services to another Supplier); 40f, 42f, 70 m, 99 GL

CoC and other notifications

Supplier undertakes to inform Customer about any change in name, corporate seat, delivery address, unique identifier details, any of its other registration details or any change in its ownership structure as soon as reasonably possible after such change takes effect or becomes known to it; 54e GL

Subcontractors

Supplier confirms and undertakes to Customer to have and to keep at all times during the Outsourcing sufficient resources for properly performing the Outsourced Services. Further Supplier undertakes to abstain from any further outsourcing any of the Outsourced Services (sub-outsourcing, sub-contracting) to third parties without having obtained the prior written consent of Customer. If Customer agrees to any such sub-outsourcing, (i) Supplier undertakes already now to submit any of its sub-contractors to the same terms and duties, including, but not limited to the Outsourcing Requirements, to which Supplier has agreed under the Agreement and the terms of this Schedule 4 and to provide evidence thereof at any time upon request of Customer, and (ii) the Parties commit to agree under a separate agreement which part of the Outsourced Services (if any) will be exempted from such sub-outsourcing and which terms and conditions (if any) will apply towards those parts of the Outsourced Services which are being sub-outsourced. In such agreement Supplier will also commit to supervise the Outsourced Services being sub-outsourced so that it is ensured that the contractual rights and duties under the Agreement are being fulfilled. Notwithstanding the requirement to obtain prior written consent to any sub-outsourcing hereunder, Supplier will, as soon as reasonable practicable, but in any event prior to any sub-outsourcing or any material change in relation to any sub-outsourcing) notify Customer about (if so) its intention to sub-outsource the Outsourced Services in full or in part or to make any material change in relation to any sub-outsourced Outsourced Service; and 55g, 70, 78 c, e, f, g, 79, 80 GL

Auditing and examination rights

Supplier undertakes to co-operate with and assist Customer's internal audit units and its Competent Supervisors. For this purpose, Supplier will inter alia grant access to its business premises, its data processing and storage systems as well as its employees and external auditors, at such times and to such extent as is required or reasonable to allow for an audit by the competent audit units of the performance of the Outsourced.

Additional Termination rights

If either any of Customer's competent supervising authorities (being the ECB, EBA and the ESMA as well as the FMA (Austria's financial market authority) and the Austrian National Bank („OeNB"), or the respective local authorities of the Affiliates, together the "*Competent Supervisors*") is asking (whether by means of initiating any formal legal procedure or in any informal way) to terminate the relevant Agreement or legal acts coming into force, or court (including administrative court) rulings are being issued and which require (whether directly or indirectly) to terminate the Agreement.

Customer, in addition to any of its other rights under the Agreement, is entitled to give notice of termination in both cases listed above at any time. Any such notice of termination has to be provided to Supplier and has to indicate when, at the sole discretion of Customer, the notice will take either immediate effect or will cause the Agreement to terminate in accordance with terms specified in this Schedule 4. 75q, 98, 99, 105 GL