FINMATICS
THE FUTURE OF FINANCE - TODAY

Anlage 3

Vereinbarung zur Auftragsverarbeitung

Zwischen

Dem **KUNDEN**, wie er im BESTELLFORMULAR angeführt wird
(im Folgenden der "**KUNDE**" oder der "**Verantwortliche**")

und
Finmatics GmbH
Lindengasse 41/10, 1070 Wien
(im Folgenden "**FINMATICS**" oder der "**Auftragsverarbeiter**")

1. DIE VERTRAGSPARTEIEN

1.1 Der KUNDE ist Verantwortlicher im Sinne des Art 4 Z 7 der Datenschutz-Grundverordnung (VO [EU] 2016/679 – "**DSGVO**") bzw Auftraggeber im Sinne des § 4 Z 4 DSG 2000 hinsichtlich jeglicher Informationen, die sich auf identifizierte oder identifizierbare natürliche Personen im Sinne des Art 4 Z 1 DSGVO ("**personenbezogene Daten**") beziehen, die an den Auftragsverarbeiter, im Rahmen der unter Punkt 2. genannten zu erbringenden Tätigkeiten überlassen werden.

1.2 FINMATICS ist als Auftragsverarbeiter im Sinne des Art 4 Z 8 DSGVO bzw als Dienstleister im Sinne des § 4 Z 5 DSG 2000 für den KUNDEN tätig.

2. GEGENSTAND, ART UND ZWECK DER VERARBEITUNG

FINMATICS verarbeitet die unter Abschnitt 4. beschriebenen personenbezogenen Daten, indem die FINMATICS-SOFTWARE diese Daten aus Belegen und sonstigen rechnungslegungsrelevanten Dokumenten scannt und entsprechend ausliest. Diese Verarbeitung dient dem Erstellen der Finanzbuchhaltung des KUNDEN oder von Geschäftspartnern des KUNDEN.

3. DAUER DER VERARBEITUNG

Die Daten werden von FINMATICS verarbeitet, solange ein Auftragsverhältnis zwischen FINMATICS und dem KUNDEN besteht.

4. ART DER PERSONENBEZOGENEN DATEN

Vor- und Nachname, Adresse, UID Nummer, Geburtsdatum, Telefonnummer, E-Mail-Adresse, Kundennummer.

5. KATEGORIEN DER BETROFFENEN PERSONEN

- Natürliche Personen, die in einer Geschäftsbeziehung zum KUNDEN stehen.
- Natürliche Personen, die als Dokumentenersteller, Dokumentenempfänger, Erfüllungsgehilfe, Geschäftspartner oder ähnliches auf den verarbeiteten Dokumenten oder Datensätzen angeführt sind.

6. PFLICHTEN DES AUFTRAGSVERARBEITERS

6.1 FINMATICS verarbeitet personenbezogene Daten ausschließlich im Rahmen dieser Vereinbarung oder auf gesonderte Anweisung des KUNDEN, es sei denn, FINMATICS ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. FINMATICS hat sämtliche Handlungen zu unterlassen, die der Position als Auftragsverarbeiter widersprechen. FINMATICS hat die sich aus dem anwendbaren Recht ergebenden Pflichten sorgfältig einzuhalten, insbesondere jene aus der DSGVO und dem Datenschutzgesetz idgF. Das Hochladen von Informationen in die Software von FINMATICS durch den KUNDEN gilt als Weisung im Sinne dieser Bestimmung. Die Weisung bezieht sich auf das Verarbeiten der Informationen nach den Vorgaben der AGB, denen diese Auftragsverarbeitervereinbarung als Anlage beigefügt ist. Mangels gegenteiliger Anweisung durch den KUNDEN ist FINMATICS nicht berechtigt oder verpflichtet, Informationen zu löschen, die der KUNDE in die Software von FINMATICS hochgeladen hat.

6.2 FINMATICS verpflichtet sich daher, personenbezogene Daten ausschließlich im Rahmen der dokumentierten Weisungen des KUNDEN zu verwenden und ausschließlich dem KUNDEN zurückzugeben oder nur nach dessen Weisung an Dritte zu übermitteln.

6.3 FINMATICS verarbeitet die personenbezogenen Daten nach dem Grundsatz der Datenminimierung gemäß Art 5 Abs 1 lit c DSGVO und daher nur soweit, als das zum Erbringen der unter Punkt 2. genannten Arbeiten erforderlich ist. Darüber hinaus verpflichtet sich FINMATICS ein nach Art 30 Abs 2 DSGVO erforderliches Verzeichnis von Verarbeitungstätigkeiten zu führen. FINMATICS hat sicherzustellen, dass personenbezogene Daten und andere eigene Daten der FINMATICS bzw ihrer Kunden getrennt verarbeitet werden.

6.4 FINMATICS erklärt rechtsverbindlich, dass sie alle mit der Datenverarbeitung beauftragten oder potentiell zugriffsberechtigten Personen vor Aufnahme ihrer Tätigkeit zur Wahrung des Datengeheimnisses im Sinne des Art 28 Abs 3 lit b DSGVO und des § 6 DSG verpflichtet hat. Insbesondere bleibt die Verschwiegenheitspflicht der mit der Datenverarbeitung beauftragten Personen auch nach Beenden ihrer Tätigkeit und Ausscheiden bei FINMATICS aufrecht.

6.5 FINMATICS trägt für die technischen und organisatorischen Voraussetzungen Vorsorge, sodass der KUNDE die Rechte der Betroffenen, insbesondere die Bestimmungen des Art 13 und 14 DSGVO (Informationspflicht), Art 15 DSGVO (Auskunftsrecht), Art 16 und 17 DSGVO (Recht auf Richtigstellung und Löschung), Art 18 DSGVO (Recht auf Einschränkung der Verarbeitung), Art 20 DSGVO (Recht auf Datenübertragbarkeit) und Art 21 DSGVO, (Recht auf Widerspruch) gegenüber einer betroffenen Person innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem KUNDEN alle dafür notwendigen Informationen.

6.6 FINMATICS erklärt rechtsverbindlich, einen Datenschutzbeauftragten benannt zu haben, sofern sie dazu nach Art 37 DSGVO verpflichtet ist. In diesem Fall werden dessen Kontaktdaten dem KUNDEN mitgeteilt. FINMATICS teilt dem KUNDEN auch einen Wechsel des Datenschutzbeauftragten unverzüglich mit.

6.7 FINMATICS ist verpflichtet, allfällige Anfragen oder Aufforderungen der Datenschutzbehörde ("**DSB**") oder anderer zuständiger Behörden Folge zu leisten und die internen Verarbeitungsvorgänge entsprechend anzupassen. Die Pflicht besteht unabhängig davon, ob solche Anfragen oder Aufforderungen direkt durch die Behörde erteilt werden oder über den KUNDEN an FINMATICS herangetragen werden.

6.8 Im Zusammenhang mit den in diesem Vertrag genannten Arbeiten kooperiert FINMATICS im größtmöglichen Umfang mit den zuständigen Behörden und dem KUNDEN, insbesondere bei der Erstellung des Verzeichnisses der Verarbeitungsvorgänge (Art 30 DSGVO), bei Datenschutz-Folgeabschätzungen (Art 35 DSGVO) und vorherigen Konsultationen der Aufsichtsbehörde (Art 36 DSGVO).

6.9 Der KUNDE wird hinsichtlich der Verarbeitung der überlassenen Daten das Recht der jederzeitigen Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen eingeräumt. FINMATICS verpflichtet sich gemäß Art 28 Abs 3 lit h DSGVO, dem KUNDEN jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

7. SUB-AUFTRAGSVERARBEITER

7.1 Der KUNDE erteilt FINMATICS hiermit die allgemeine schriftliche Genehmigung gemäß Art 28 Abs 2 DSGVO, dass diese andere Unternehmen/Personen für die Datenverarbeitungen heranziehen kann ("Sub-Auftragsverarbeiter"). Die Sub-Auftragsverarbeiter können auf folgender Website eingesehen werden: finmatics.com/privacy/data-processors. Wird ein neuer Sub-Auftragsverarbeiter herangezogen, hat FINMATICS diese Website vorab entsprechend zu aktualisieren und den KUNDEN rechtzeitig per E-Mail zu verständigen, sodass der KUNDE im Einklang mit Art 28 Abs 2 DSGVO allenfalls Einspruch erheben kann. Erhebt der KUNDE innerhalb von zwei Wochen ab Erhalt dieser E-Mail keinen Einspruch, so gilt die Heranziehung des neuen Sub-Auftragsverarbeiters als genehmigt.

7.2 Im Falle eines Einspruchs gegen die Heranziehung eines neuen Sub-Auftragsverarbeiter kommt FINMATICS ein Sonderkündigungsrecht nach Abschnitt 13.5 der AGB zu.

7.3 Sub-Auftragsverarbeiter außerhalb des EWR darf FINMATICS beauftragen, wenn (i) diese in einem Drittland niedergelassen sind, das über ein von der EU-Kommission mit Beschluss akzeptiertes angemessenes Datenschutzniveau verfügt (Angemessenheitsbeschluss) oder (ii) mit diesen die EU-Standardvertragsklauseln bzw diesen gleichgestellte durch die EU-Kommission erlassene Vertragsschablonen als geeignete Garantien im Sinne des Art 46 Abs 2 lit c und d DSGVO vereinbart wurden.

7.4 In jedem Fall bleibt FINMATICS dem KUNDEN vollumfänglich für die Leistungserbringung durch den hinzugezogenen Sub-Auftragsverarbeiter, seine Verpflichtungen und das Erfüllen der ihm zugewiesenen Aufgaben verantwortlich. Außerdem muss ein Vertrag zwischen FINMATICS und

dem Sub-Auftragsverarbeiter gemäß Art 28 Abs 4 DSGVO geschlossen werden, in dem sichergestellt ist, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die FINMATICS aufgrund dieser Vereinbarung obliegen. Darüber hinaus stellt FINMATICS sicher, dass der KUNDE dem Sub-Auftragsverarbeiter auch direkt Weisungen erteilen kann, sofern dies aus datenschutzrechtlicher Sicht erforderlich ist.

7.5 Kommt der Sub-Auftragsverarbeiter den Verpflichtungen aus der DSGVO nicht nach, so haftet hierfür FINMATICS gegenüber dem KUNDEN.

8. PFLICHTEN DER VERANTWORTLICHEN

Der KUNDE verpflichtet sich, FINMATICS unmittelbar von Änderungen der DSGVO und dem DSG und ergänzender Bestimmungen, die auf die gegenständige Datenverarbeitung anwendbar sind, zu unterrichten. Der KUNDE räumt FINMATICS eine angemessene Frist ein, sich organisatorisch, administrativ und technisch auf geänderte Datenschutzbestimmungen und neue Anforderungen einzustellen.

9. MITTEILUNGEN BEI VERSTÖßEN DES AUFTRAGSVERARBEITERS

9.1 FINMATICS erklärt rechtsverbindlich, den KUNDEN unverzüglich zu informieren, wenn FINMATICS eine Verletzung des Schutzes personenbezogener Daten bekannt wird bzw wenn Daten aus einer an FINMATICS überlassenen Datenanwendung systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht.

9.2 FINMATICS trifft daher technisch und organisatorisch Vorsorge dafür, dass der KUNDE insbesondere die Bestimmungen der Art 33 und 34 DSGVO ("Data Breach Notification") innerhalb der gesetzlichen Frist erfüllen kann. FINMATICS ist in diesem Zusammenhang dazu verpflichtet, dem KUNDEN unverzüglich sämtliche Informationen zur Verfügung zu stellen, die diese für eine Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und/oder die betroffene Person benötigt.

10. TECHNISCH-ORGANISATORISCHE MAßNAHMEN

10.1 FINMATICS gewährleistet, dass sie gemäß Art 32 DSGVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignete technische und organisatorische Maßnahmen getroffen hat, um ein dem Risiko angemessenes Schutzniveau sicherzustellen. Sofern sich diesbezüglich während der Zusammenarbeit notwendige Änderungen ergeben, wird FINMATICS adäquate Maßnahmen nachziehen.

10.2 FINMATICS gewährleistet insbesondere, dass die Verarbeitung in Übereinstimmung mit branchenüblichen Standards und den gesetzlichen Bestimmungen, insbesondere den datenschutzrechtlichen und regulatorischen Erfordernissen, erfolgt.

10.3 FINMATICS verpflichtet sich, die in Anhang ./1 dieser Anlage 3 genannten technisch-organisatorischen Maßnahmen einzuhalten, soweit diese aufgrund des Gegenstands und der Umstände der Verarbeitung anwendbar sind.

10.4 Sofern während der Zusammenarbeit Änderungen notwendig werden, wird FINMATICS die getroffenen Maßnahmen adäquat anpassen. Den KUNDEN trifft dabei die Pflicht, in regelmäßigen Abständen zu prüfen, ob durch geeignete technische und organisatorische Maßnahmen von FINMATICS ein angemessenes Datenschutzniveau gewährleistet ist.

10.5 Für den Fall, dass FINMATICS einen Sub-Auftragsverarbeiter heranzieht, stellt FINMATICS sicher, dass FINMATICS gleichwertige technische und organisatorische Maßnahmen mit dem Sub-Auftragsverarbeiter vereinbart. FINMATICS wird sich regelmäßig durch entsprechende Kontrollen davon vergewissern, dass diese Maßnahmen vom Sub-Auftragsverarbeiter zu jeder Zeit faktisch umgesetzt werden. Sollten sich hierbei Risiken zeigen, die FINMATICS nicht ausreichend abschwächen/steuern kann, hat sie den KUNDEN darüber in einer geeigneten Form zu informieren.

11. BEENDIGUNG DER VEREINBARUNG, LÖSCHUNG UND RÜCKGABE VON DATEN

11.1 FINMATICS ist verpflichtet nach Beendigung der Leistungserbringung, alle Verarbeitungsergebnisse und Unterlagen, die personenbezogene Daten enthalten, vollständig zu löschen. Alternativ kann der KUNDE von FINMATICS binnen angemessener Frist vor Beendigung der Leistungserbringung die Rückgabe dieser Daten verlangen. FINMATICS ist nicht berechtigt, personenbezogene Daten, Dokumente oder Teile davon weiter aufzubewahren. Hiervon ausgenommen sind Daten, zu deren Aufbewahrung FINMATICS verpflichtet ist sowie die Löschung von personenbezogenen Daten aus Sicherungskopien, da diesfalls eine Löschung vorab technisch nicht möglich ist. In Sicherungskopien gespeicherte personenbezogene Daten werden für einen Zeitraum von maximal drei Jahren gespeichert und anschließend gelöscht.

11.2 FINMATICS ist verpflichtet, die Rückgabe bzw Löschung auch bei Sub-Auftragsverarbeitern entsprechend herbeizuführen.

Anhang ./1
Technische und organisatorische Maßnahmen nach Art 32 DSGVO

1. Vertraulichkeit

FINMATICS trägt dafür Sorge, dass zu jeder Zeit die Vertraulichkeit der personenbezogenen Daten gegeben ist. Dazu werden insbesondere folgende Maßnahmen gesetzt:

a) Zutrittskontrolle

i) FINMATICS erteilt Zutrittsberechtigungen und prüft diese in regelmäßigen Abständen. Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

ii) FINMATICS hat alle Vorgaben zur physischen Sicherheit, die sich aus allfälligen Zertifizierungen bzw Branchenstandards ergeben einzuhalten.

b) Zugangskontrolle

i) FINMATICS trägt die Verantwortung dafür, dass Unbefugten die Nutzung der Datenverarbeitungssysteme nicht möglich ist.

ii) Insbesondere durch die Vergabe von individuellen Zugangsrechten muss sichergestellt werden, dass Mitarbeitern bzw sonstigen beauftragten Personen lediglich in jenem Ausmaß Zugang zu personenbezogenen Daten gewährt wird, der zur Erfüllung ihrer Aufgaben notwendig ist.

c) Zugriffskontrolle

i) FINMATICS hat dafür zu sorgen, dass berechtigte Personen nur auf jene Daten zugreifen können, die ihrer Zugriffsberechtigung unterliegen, und, dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

ii) Der Zugriff ist technisch auf jene Berechtigten einzuschränken, die zur effektiven Vertragserfüllung auf die Daten Zugriff haben müssen.

iii) Die Userlisten müssen gepflegt werden. Außerdem hat FINMATICS dafür Sorge zu tragen, dass nur User mit aufrechtem Vertragsverhältnis und der dafür vorgesehenen Stellung Zugriff auf personenbezogene Daten haben.

2. Integrität

FINMATICS trägt dafür Sorge, dass zu jeder Zeit die Integrität der personenbezogenen Daten gegeben ist. Dazu werden insbesondere folgende Maßnahmen gesetzt:

a) Weitergabekontrolle

FINMATICS hat sicherzustellen, dass "Data Breaches" verhindert werden. Hierfür hat FINMATICS dafür zu sorgen, dass personenbezogene Daten bzw Datenträger, auf denen personenbezogene Daten gespeichert sind, bei elektronischer Übertragung oder während ihres Transports nicht unbefugt gelesen, kopiert, verändert oder gelöscht/entfernt werden. Außerdem hat FINMATICS dafür zu sorgen, dass es feststellbar ist, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden sollen.

b) Eingabekontrolle

FINMATICS muss sicherstellen, dass festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt wurden.

3. Verfügbarkeit und Belastbarkeit

FINMATICS gewährleistet, dass seine Systeme entsprechend dem Branchenstandard bzw dem Stand der Technik verfügbar und belastbar sind.

a) Verfügbarkeit

i) FINMATICS hat dafür Sorge zu tragen, dass personenbezogene Daten vor zufälliger bzw mutwilliger Zerstörung oder Verlust geschützt werden.

ii) Sofern erhebliche Störungen mit den Systemen auftreten, hat sich FINMATICS mit dem Verantwortlichen abzustimmen.

iii) Es werden von FINMATICS regelmäßige Backups erstellt, um eine rasche Widerherstellung nach technischen und/oder physischen Zwischenfällen zu gewährleisten.

b) Belastbarkeit

FINMATICS ist dafür verantwortlich, dass deren Systeme bei technischen Angriffen geschützt sind und Kapazitäten vorhanden sind, die trotz unvorhersehbaren Belastungen einen reibungslosen Betrieb ermöglichen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. FINMATICS überprüft, bewertet und evaluiert in regelmäßigen Abständen ihre technischen und organisatorischen Maßnahmen. Auf diese Weise wird eine dauerhafte Sicherheit der Verarbeitung gewährleistet.

4.2. FINMATICS erklärt sich dazu bereit, ihre Sicherheitsmaßnahmen durch ihre Vertragspartner oder einen von diesem bevollmächtigten Sachverständigen überprüfen und bewerten zu lassen.