Vereinbarung über eine Auftragsverarbeitung gemäß Art. 28 DSGVO

Der Verantwortliche:	Der Auftragsverarbeiter:
	Nubesso e.U. Kammern 1074 6863 Egg
(im Folgenden Auftraggeber)	(im Folgenden Auftragnehmer)

1. Gegenstand der Vereinbarung

(1) Gegenstand

Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Der Auftragnehmer stellt dem Auftraggeber eine Cloudlösung nuMobile/nuComplete für die Bereiche ERP/Zeiterfassung zur Verfügung

(2) Art und Zweck der Verarbeitung von Daten

Der Auftragnehmer bietet die Cloudlösung inklusive Support, Wartung und Datensicherung an. Dadurch kann es erforderlich sein, dass der Auftragnehmer zu Support- und Wartungszwecken personenbezogene Daten auswertet und analysiert.

(3) Art der Daten und der betroffenen Personen

Folgende Datenkategorien werden verarbeitet:
Kunden, Interessenten, Lieferanten, Ansprechpartner, Mitarbeiter

2. Dauer der Vereinbarung

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und hat solange Gültigkeit, bis die Nutzung der angebotenen Cloudlösung gekündigt wird.

3. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung

erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(3) Wahrung der Vertraulichkeit und Verschwiegenheit: Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(4) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32ff DSGVO ergriffen hat. Konkret handelt es sich hierbei um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Einzelheiten hierzu finden sich im Anhang (Technisch-organisatorische Maßnahmen).

(5) Mitwirkungspflicht bei Betroffenenrechten: Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Betroffenenrechte nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen.
Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(6) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer durchzuführen (sicherzustellen).

(7) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten. Dazu gehören Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von

einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation.

(8) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu erstellen hat.

(9) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(10) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, sämtliche in seinem Besitz gelangten Unterlagen, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten[1]. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

(11) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. Technisch-organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen (TOMs) unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren. Einzelheiten sind dem Anhang zu entnehmen.

5. Ort der Durchführung der Datenverarbeitung

Ausschließliche Durchführung innerhalb der EU/des EWR
Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

---

6. Sub-Auftragsverarbeiter

Der Auftragnehmer ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter zur unmittelbaren Erbringung der Hauptdienstleistung hinzuziehen:
Host Europe GmbH; Hansestraße111; 51149 Köln

Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- die erforderlichen Vereinbarungen zwischen dem Auftragnehmer und dem Sub-Auftragsverarbeiter gemäß des Art. 28 Abs. 4 DSGVO abgeschlossen werden. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

[Ort], am [Datum]
Für den Auftraggeber:

.....
[Name und Firmenstempel]

[Ort], am [Datum]
Für den Auftragnehmer:

Egg, 23.5.2018 R. Lingg

nubesso®
simply-simple

.....
[Name und Firmenstempel]

nubesso e.U.
Kammern 1074
6863 Egg
www.nubesso.com

Anhang - Technisch-organisatorische Maßnahmen (TOMs)

Vertraulichkeit

- Zutrittskontrolle: Durch unseren Sub-Auftragsverarbeiter Host Europe sind alle Server durch ein elektronisches Zutrittssystem und 24h Videoüberwachung vor unbefugtem Zutritt gesichert;
- Zugangskontrolle: Alle Zugangsdaten auf Server und auch locale PC's des Auftragnehmers sind mit starken Kennwörtern geschützt, die alle 3 Monate neu vergeben werden
- Zugriffskontrolle: Jeder Zugriff auf die Server wird mitprotokolliert. Weiters ist der Zugriff auf die Server durch eine Firewall gesichert
- Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind durch eine strenge Mandantentrennung gewährleistet

Integrität

- Weitergabekontrolle: Um unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Daten bei elektronischer Übertragung zwischen Cloudserver und dem Client des Auftraggebers erfolgt eine Verschlüsselung der transportierten Daten;
- Eingabekontrolle: Jede Datensatzänderung wird in einer Historie gespeichert mit dem Informationen, wann und wer welchen Datensatz geändert hat;

Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle: Durch unseren Sub-Auftragsverarbeiter Host Europe ist eine hohe Verfügbarkeit laut SLA gegeben (Virtualisierung, Snapshot-Backups, unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall)
- Rasche Wiederherstellbarkeit: Durch die erstellten Snapshotbackups des Betriebssystems und der täglichen Datensicherungen ist eine rasche Wiederherstellung gegeben
- Löschungsfristen: Wird die Nutzung der Cloudlösung durch einen Auftraggeber beendet, so werden, wenn nicht anders vereinbart, die Daten laut unserer AGB noch 6 Monate gespeichert und danach unwiderruflich gelöscht.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Die Mitarbeiter werden einmal im Jahr im Bereich Datenschutz-Management geschult
- Incident-Response-Management erfolgt nach dem SLA unseres Sub-Auftragsverarbeiters Host Europe;