VERTRAG ZUR AUFTRAGSDATENVEREINBARUNG

Dieser **Vertrag zur Auftragsdatenverarbeitung** (**„der Vertrag"**) wurde zwischen der TSHK (**„der Datenverarbeiter"**) und dem Kunden (**„der Verantwortliche"**) geschlossen.

Der Datenverarbeiter und der Verantwortliche werden einzeln als **„Partei"** und gemeinsam als **„Parteien"** bezeichnet.

HINTERGRUND

(A) Dieser Vertrag ist Bestandteil der AGB des Datenverarbeiters, die wiederum Teil eines Dienstleistungsvertrags zwischen dem Datenverarbeiter und dem Verantwortlichen sind (**„der Dienstleistungsvertrag"**). Im Rahmen des Dienstleistungsvertrags verarbeitet der Datenverarbeiter Personenbezogene Daten im Auftrag des Verantwortlichen, um die im Dienstleistungsvertrag vereinbarten Leistungen zu erbringen.

(B) Der Verantwortliche ist für die Verarbeitung der Personenbezogenen Daten verantwortlich. Der Datenverarbeiter ist Auftragsdatenverarbeiter und verarbeitet Personenbezogene Daten im Auftrag des Verantwortlichen. Dienstleistungsverträge, die eine Verarbeitung Personenbezogener Daten im Auftrag des Verantwortlichen beinhalten, sind in der Anlage 1 zum Vertrag unter dem Punkt „Kategorien Personenbezogener Daten" näher spezifiziert.

1 UNTERLAGEN

Dieser Vertrag besteht aus dem Hauptvertrag mit folgenden Anlagen:

Anlage 1 – Die Anweisungen des Verantwortlichen zur Datenverarbeitung

Anlage 2 – Sicherheitsmaßnahmen

Anlage 3 – Genehmigte Unter-Datenverarbeiter

2 DEFINITIONEN

In diesem Vertrag haben die Ausdrücke, welche mit Großbuchstaben beginnen, folgende Bedeutung. Im Übrigen gelten die Definitionen, welche in den Geltenden Gesetzen angegeben werden.

DSGVO	meint die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, inklusive eventuellen zukünftigen Änderungen und Ergänzungen.
Personenbezogene Daten	meint personenbezogene Daten (wie sie in den Geltenden Gesetzen definiert werden), die in Anlage 1 spezifiziert sind.
Geltende Gesetze	meint (DSGVO und geltende ergänzende Gesetze zu DSGVO.

Dienstleistungsvertrag meint den Vertrag, der in dem Punkt „Hintergrund (A)" in diesem Vertrag definiert ist.

3 ANWEISUNGEN

3.1 Der Datenverarbeiter hat die Personenbezogenen Daten gemäß den dokumentierten Anweisungen des Verantwortlichen, die sich aus Anlage 1 ergeben, zu verarbeiten. Die Anweisungen sollen zumindest folgende Informationen enthalten:

(i) Der Zweck der Verarbeitung,

(ii) die Art der Verarbeitung,

(iii) die Dauer der Verarbeitung bzw. wie die Dauer festgelegt werden soll,

(iv) welche Kategorien von Personenbezogenen Daten verarbeitet werden sollen und

(v) welche Kategorien von Registrierten in die Verarbeitung einbezogen sind.

3.2 Der Datenverarbeiter darf die Personenbezogenen Daten nicht für andere Zwecke verarbeiten als in den Anweisungen des Verantwortlichen angegeben. Die Parteien sollen Anlage 1 bei neuen oder geänderten Anweisungen aktualisieren. Der Datenverarbeiter hat Anspruch auf Vergütung nach laufender Rechnung gemäß der jeweils aktuellen Preisliste für Dienstleistungen des Datenverarbeiters für solche Arbeit, die der Datenverarbeiter zum Zwecke der Befolgung veränderter Anweisungen des Verantwortlichen ausführt.

3.3 Ungeachtet des Vorstehenden hat der Datenverarbeiter das Recht, in angemessenem Umfang laufende Maßnahmen ohne die ausdrückliche Anweisung des Verantwortlichen auszuführen, vorausgesetzt, dass der Datenverarbeiter für die und im Rahmen der Zwecke, die sich aus Anlage 1 ergeben, agiert.

3.4 Für den Fall, dass der Datenverarbeiter der Ansicht ist, dass eine Anweisung gegen die Geltenden Gesetze verstößt, soll der Datenverarbeiter die Anweisung nicht befolgen, den Verantwortlichen unverzüglich unterrichten und geänderte Anweisungen abwarten.

4 DIE PFLICHT DES VERANTWORTLICHEN ZUR RECHTMÄSSIGEN VERARBEITUNG PERSONENBEZOGENER DATEN

4.1 Der Verantwortliche hat sicherzustellen, dass für die Verarbeitung von Personenbezogenen Daten ein rechtlicher Grund vorliegt. Der Verantwortliche hat zudem alle weiteren Pflichten zu erfüllen, welche ihm durch die Geltenden Gesetze auferlegt werden (einschließlich der Verpflichtung zur Information der betroffenen Personen über die Verarbeitung von Personenbezogenen Daten).

4.2 Die Anweisungen des Verantwortlichen zur Verarbeitung personenbezogener Daten müssen den Geltenden Gesetzen entsprechen. Der Verantwortliche haftet dafür, dass die Personenbezogenen Daten wahrheitsgemäß sind und dass deren Verarbeitung und Erhebung rechtmäßig ist.

5 SICHERHEITSMASSNAHMEN

5.1 Der Datenverarbeiter hat geeignete Sicherheitsmaßnahmen zu treffen, um den Schutz der Personenbezogenen Daten gegen Zerstörung, Änderung und Verbreitung sicherzustellen.

Der Datenverarbeiter hat zudem sicherzustellen, dass Personenbezogene Daten gegen unbefugtes Eindringen geschützt sind und dass der Zugang zu den Daten protokolliert wird und sich zurückverfolgen lässt. Die Sicherheitsmaßnahmen sind in Anlage 2 beschrieben. Der Verantwortliche billigt diese Sicherheitsmaßnahmen als geeignet, ausreichend und angemessen.

5.2 Der Datenverarbeiter hat sicherzustellen, (i) dass nur befugte Personen Zugang zu den Personenbezogenen Daten haben, (ii) dass die befugten Personen die Personenbezogenen Daten nur im Einklang mit dem Vertrag und den Anweisungen des Verantwortlichen verarbeiten und (iii) dass jede befugte Person zur Geheimhaltung, welcher der Geheimhaltungsvereinbarung dieses Vertrages entspricht, verpflichtet ist.

5.3 Der Datenverarbeiter hat den Verantwortlichen unverzüglich zu unterrichten, wenn er Kenntnis von einer Verletzung des Schutzes der Personenbezogenen Daten erhält. Der Datenverarbeiter hat den Verantwortlichen in der Erfüllung der Pflichten des Verantwortlichen zu unterstützen, indem er gemäß der Geltenden Gesetze (i) jede Verletzung des Schutzes der Personenbezogenen Daten dokumentiert, (ii) der zuständigen Aufsichtsbehörde jede Verletzung Personenbezogener Daten mitteilt, und (iii) die betroffene Person über eine solche Verletzung des Schutzes der Personenbezogenen Daten informiert.

6 PFLICHT DES DATENVERARBEITERS, DEN VERANTWORTLICHEN ZU UNTERSTÜTZEN

6.1 Der Datenverarbeiter hat den Verantwortlichen unter Beachtung der Art der Verarbeitung durch angemessene technische und organisatorische Maßnahmen soweit wie möglich zu unterstützen, damit dieser seiner Verpflichtung nachkommen kann, Anfragen der betroffenen Personen zur Ausübung ihrer Rechte gemäß Kapitel III der DSGVO zu beantworten. Diese Rechte umfassen (i) das Recht, der Bearbeitung zu widersprechen und seine Personenbezogenen Daten gelöscht zu bekommen, (ii) das Recht, Informationen über und Zugang zu den Personenbezogenen Daten zu bekommen, (iii) soweit technisch möglich, das Recht zur Datenportabilität bei Direktüberführung von Personenbezogenen Daten an einen neuen Verantwortlichen, und (iv) das Recht auf Berichtigung der Personenbezogenen Daten.

6.2 Der Datenverarbeiter hat den Verantwortlichen unter Beachtung der Art der Verarbeitung und der dem Datenverarbeiter zugänglichen Information den Verantwortlichen weiterhin in der Erfüllung seiner Pflichten gemäß Art. 32-36 der DSGVO zu unterstützen. Die Pflichten beinhalten (i) die Sicherstellung einer sicheren Verarbeitung, (ii) die Durchführung von Datenschutz-Folgeabschätzungen und (iii) vorherige Konsultation der Aufsichtsbehörde.

7 UNTER-DATENVERARBEITER

7.1 Der Datenverarbeiter darf einen Dritten hinzuzuziehen, um die gesamte oder Teile der Verarbeitung der Personenbezogenen Daten nach diesem Vertrag auszuführen (**„Unter-Datenverarbeiter"**), wenn der Datenverarbeiter den Verantwortlichen schriftlich darüber informiert hat und der Verantwortliche nicht innerhalb von zehn Tagen, nachdem der Datenverarbeiter die Information an den Verantwortlichen weitergegeben hat,

widersprochen hat. In einem solchen Fall wird der Unter-Datenverarbeiter ein **„Genehmigter Unter-Datenverarbeiter"**. Genehmigte Unter-Datenverarbeiter werden in Anlage 3 (die bei Änderungen der Genehmigten Unter-Datenverarbeiter aktualisiert wird) angegeben. Anlage 3 soll folgende Information über jeden Genehmigten Unter-Datenverarbeiter beinhalten:

(i) Name, Kontaktinformation, Gesellschaftsform und geographischer Ort des Genehmigten Unter-Datenverarbeiters,

(ii) eine Beschreibung der Dienstleistung, die der Genehmigte Unter-Datenverarbeiter erbringt,

(iii) der geographische Ort für die Verarbeitung der Personenbezogenen Daten.

7.2 Der Datenverarbeiter hat einen schriftlichen Vertrag mit jedem Unter-Datenverarbeiter einzugehen, nach welchem der Unter-Datenverarbeiter die Verpflichtungen übernimmt, welche den nach diesem Vertrag übernommen Verpflichtungen des Datenverarbeiters entsprechen.

7.3 Für den Fall, dass der Verantwortliche gemäß Punkt 7.1 oben einem neuen Unter-Datenverarbeiter widerspricht, hat der Datenverarbeiter davon abzusehen, diesen Unter-Datenverarbeiter für die Verarbeitung der personenbezogenen Daten zu beauftragen. Der Datenverarbeiter hat dann zu versuchen, angemessene Maßnahmen zur Veränderung der für den Verantwortlichen zu erbringenden Dienste zu ergreifen, um eine Verarbeitung personenbezogener Daten durch den aktuellen Unter-Datenverarbeiter zu verhindern. Wenn der Datenverarbeiter der Ansicht ist, dass eine solche Änderung praktisch oder kommerziell nicht möglich oder angemessen ist, kann der Datenverarbeiter den Vertrag mit einer Ankündigungsfrist von 45 Tagen kündigen. Eine solche Kündigung muss spätestens 45 Tage, nachdem dem Verantwortlichen ein schriftlicher Einwand gegen den neuen Unter-Datenverarbeiter zugegangen ist, vorgenommen werden.

7.4 Wenn der Verantwortliche den Unter-Datenverarbeiter genehmigt hat, verliert der Verantwortliche das Recht, gegen den Unter-Datenverarbeiter Einwände zu erheben.

8 ÜBERMITTLUNG IN DRITTLÄNDER

Der Datenverarbeiter darf die Personenbezogenen Daten ohne die schriftliche Genehmigung des Verantwortlichen nicht außerhalb der EU/des EWR übermitteln. Eine solche Übertragung darf zudem nur dann erfolgen, wenn mindestens eine der folgenden Voraussetzungen erfüllt ist:

(i) das Empfängerland stellt ein angemessenes Schutzniveau für Personenbezogene Daten gemäß Beschluss der Europäischen Kommission sicher,

(ii) der Verantwortliche bestätigt, dass die betroffene Person ihre Zustimmung zur Übermittlung erteilt hat,

(iii) die Übermittlung unterliegt den Standardvertragsklauseln der Europäischen Kommission für die Übermittlung von Personenbezogenen Daten in Drittländer,

(iv) sowohl der Datenverarbeiter als auch der Empfänger im Drittland ist an verbindliche Unternehmensregelungen (Binding Corporate Rules) gebunden, oder

(v) bei Übermittlungen in die USA ist der Empfänger gemäss Pricay Shield zertifiziert.

9 KONTROLLE

9.1 Auf Anfrage des Verantwortlichen hat der Datenverarbeiter dem Verantwortlichen solche Informationen bereitzustellen, die zeigen, dass der Datenverarbeiter seinen Verpflichtungen nach den Geldenden Gesetzen nachkommt.

9.2 Der Verantwortliche hat das Recht, nach schriftlicher Ankündigung 20 Tage im Voraus eine Prüfung der Verarbeitung der Personenbezogenen Daten durch den Datenverarbeiter und diesbezüglich relevanter Information vorzunehmen, um zu zeigen, dass sich der Datenverarbeiter an diesen Vertrag und die Geltenden Gesetze hält. Der Datenverarbeiter soll den Verantwortlichen unterstützen und die Informationen zugänglich machen, die zur Durchführung einer solchen Prüfung durch den Verantwortlichen notwendig sind. Der Verantwortliche trägt die Kosten für eine solche Prüfung.

9.3 Wenn eine Aufsichtsbehörde eine Prüfung des Datenverarbeiters durchführt, die die Verarbeitung Personenbezogener Daten mitumfasst, hat der Datenverarbeiter dies dem Verantwortlichen umgehend mitzuteilen.

10 VERGÜTUNG

10.1 Der Datenverarbeiter hat Anspruch auf Vergütung für die Verarbeitung der Personenbezogenen Daten gemäß der zwischen den Parteien gesondert vereinbarten Vergütung oder der jeweils gültigen Preisliste für die Dienstleistungen, die der Datenverarbeiter ausführt.

10.2 Der Verantwortliche hat den Datenverarbeiter weiterhin gemäß jeweils aktuell geltender Preisliste für Beratungsdienstleistungen zu vergüten, um Veränderungen von oder Ergänzungen in den Anweisungen des Verantwortlichen Rechnung zu tragen sowie um die Anweisungen des Verantwortlichen bezüglich der Personenbezogenen Daten und deren Verarbeitung zu erfüllen.

11 HAFTUNG UND HAFTUNGSBEGRENZUNG

Die Haftung des Datenverarbeiters unter diesem Vertrag wird von den Haftungsbegrenzungen im Dienstleistungsvertrag umfasst.

12 GEHEIMHALTUNG

12.1 Der Datenverarbeiter verpflichtet sich, Geheimhaltung zu wahren und keine Personenbezogenen Daten oder Informationen, die sich auf Personenbezogene Daten beziehen, Dritten gegenüber zu enthüllen oder mit diesen zu teilen. Genehmigte Unter-Datenverarbeiter werden nicht als Dritte im Sinne dieses Punktes 12 angesehen.

12.2 Ungeachtet Punkt 12.1 darf der Datenverarbeiter solche Informationen enthüllen, wenn er dazu gesetzlich, durch ein Gerichtsurteil oder einen Behördenbeschluss verpflichtet ist. Der Datenverarbeiter hat den Verantwortlichen umgehend schriftlich zu unterrichten, wenn

eine solche Verpflichtung entsteht, es sei denn, die Geltenden Gesetze verbieten eine solche Unterrichtung.

12.3 Die Geheimhaltungsverpflichtung besteht auch nach Beendigung dieses Vertrages fort.

12.4 Im Übrigen bewahrt der Datenverarbeiter Verschwiegenheit im Hinblick auf personenbezogene Daten gemäß Punkt 13 der AGB des Datenverarbeiters.

13 LÖSCHUNG VON PERSONENBEZOGENEN DATEN

13.1 Bei Beendigung des Dienstleistungsvertrages hat der Verantwortliche den Datenverarbeiter schriftlich dazu anzuweisen, ob Personenbezogene Daten an den Verantwortlichen überführt werden sollen oder nicht. Eine solche Überführung ist in einem allgemein benutzten und maschinenlesbaren Format vorzunehmen.

13.2 Der Datenverarbeiter hat ungeachtet Punkt 13.1 oben die Personenbezogenen Daten frühestens innerhalb von 30 Tagen und spätestens 40 Tage nach Beendigung des Dienstleistungsvertrages aus seinen Systemen zu löschen.

14 LAUFZEIT DES VERTRAGES

Für sämtliche Verträge, die vor dem 25. Mai 2018 abgeschlossen wurden, ist Vertragsdatum für den Vertrag der 25. Mai 2018. In allen übrigen Fällen wird der Vertrag an dem Tag geschlossen, an dem der Dienstleistungsvertrag nebst AGB zwischen den Parteien abgeschlossen wird.

Unabhängig von der Laufzeit des Dienstleistungsvertrages tritt dieser Vertrag in Kraft, wenn der Datenverarbeiter die Verarbeitung der Personenbezogenen Daten für den Verantwortlichen einleitet, und endet, wenn der Datenverarbeiter die Personenbezogenen Daten gemäß Punkt 13.1 oben gelöscht hat.

ANLAGE 1 – ANWEISUNGEN

Jede Verarbeitung Personenbezogener Daten durch den Datenverarbeiter soll gemäß folgenden Anweisungen vorgenommen werden. Für den Fall, dass die Verarbeitung Personenbezogener Daten entgegen dieser Anweisungen vorgenommen wird, wird der Datenverarbeiter als Verantwortlicher für Personenbezogene Daten für eine solche Verarbeitung angesehen.

	ANWEISUNGEN
Zweck der Verarbeitung	Um die Pflichten nach dem Dienstleistungsvertrag zu erfüllen.
Art der Verarbeitung	Der Datenverarbeiter verarbeitet die Personenbezogenen Daten für den Verantwortlichen zu dem Zweck, die Dienste nach dem Dienstleistungsvertrag bereitzustellen. Die Verarbeitung kann bei bestimmten Dienstleistungen sensible Personenbezogene Daten umfassen, z.B. um Gehaltsauszahlungen zu administrieren, außerdem kann die Verarbeitung die Personennummer umfassen. Was im Einzelfall gilt, ergibt sich unten aus der Kategorie der Personenbezogenen Daten für die jeweilige Dienstleistung.
Dauer der Verarbeitung	Die Verarbeitung findet während der Dauer des Dienstleistungsvertrages statt.
Kategorien der registrierten Personen	Je nach Art und Umfang des Dienstleistungsvertrags kann der Verantwortliche Personenbezogene Daten von registrierten Personen folgender Kategorien verarbeiten: Angestellte des Verantwortlichen, Vertreter des Verantwortlichen (Vorstandsmitglieder, Geschäftsführer und Zeichnungsbefugte), Kontaktpersonen des Verantwortlichen.
Kategorien der Personenbezogenen Daten	Kategorien personenbezogener Daten, die im Rahmen der Erfüllung des Dienstleistungsvertrags verarbeitet werden, können je nach Dienstleistung folgende sein: **<u>Für alle nachfolgenden Dienstleistungen:</u>** Name, E-Mail-Adresse, Telefonnummer **<u>Bezahlung von Kundenrechnungen (Finanzbuchhaltung):</u>** Siehe oben. **<u>Gehaltsabrechnung:</u>** Titel, Nationalität, Geschlecht, Geburtsdatum, Alter, Personennummer,

	sonstige nationale Identifikationsnummer, (z.B. CPR, Sozialversicherungsnummer, Steuerregistrierungsnummer oder Passnummer), Wohnanschrift, persönliche E-Mailadresse, Konto- und Kreditkartendaten, Krankheit, Abwesenheit (Urlaub, Elternzeit, Freistellung etc.), Zeiterfassung, Gehaltsdokumentation, Zeiterfassung, Gehaltsabrechnungen, Personaldokumentation **Dienstleistungen im Rahmen des virtuellen Büros:** Titel, Nationalität, Geschlecht, Geburtsdatum, Alter, Personennummer, sonstige nationale Identifikationsnummer, Wohnanschrift, persönliche E-Mail-Adresse, Konto- und Kreditkartendaten
Andere Anweisungen	Keine Angaben.

ANLAGE 2 – SICHERHEITSMASSNAHMEN

Technische und organisatorische Sicherheitsmaßnahmen

Der Datenverarbeiter ist verantwortlich für die technischen und organisatorischen Sicherheitsmaßnahmen in seinem System. Der Datenverarbeiter arbeitet kontinuierlich mit Datenschutzfragen in Bezug auf Programme, Dienstleistungen und Prozesse.

Dazu gehört auch, dass der Datenverarbeiter dafür Sorge trägt, dass die erforderliche Sicherheit bspw. bei der Kryptierung, Steuerung von Zugangsberechtigungen etc. vorliegt. Der Datenverarbeiter hat ein Konzept für die Löschung von Daten und erfüllt auch sonstige Anforderungen an Datenschutz und Privatsphäre.

Zugang zu den Räumlichkeiten

Der Datenverarbeiter verarbeitet Personenbezogene Daten in eigenen Räumlichkeiten. Der Zugang zu den Räumlichkeiten erfolgt über ein personengebundenes Chipsystem, das unterschiedliche Zugangsberechtigungen ermöglicht. Die Räumlichkeiten sind durch ein Alarmsystem geschützt. Zugang zu der jeweiligen Speicherung von Personenbezogenen Daten und/oder Servern haben nur befugte Mitarbeiter. Besucher werden von der Rezeption empfangen und haben keinen Zutritt zu den Abteilungen, in denen die Verarbeitung Personenbezogener Daten erfolgt. Die Räumlichkeiten sind brandschutzangepasst.

Zugang zu Datensystemen

Sämtliche Rechte werden ausschließlich durch den IT-Support des Datenverarbeiters verwaltet. Sämtliche Datensysteme sind passwortgeschützt, dabei sind die Anforderungen an das Sicherheitsniveau in einer internen Richtlinie geregelt. Zugang zu den Datensystemen hat nur das mit der Angelegenheit befasste Personal, das über unterschiedliche restriktive Befugnisse verfügt.

Speicherung und Backups

Der Datenverarbeiter hat eigene Server in seinen Räumlichkeiten. Die Speicherung von Backups erfolgt mit voller Redundanz an zwei unterschiedlichen Orten in Stockholm, Backups werden täglich erstellt. Nur zugelassenes Personal hat physischen Zugang zu den Servern. Die Server und das Netzwerk des Datenverarbeiters werden durch Firewalls und Antivirussoftware geschützt.

Schutz von Erkenntnissen und Informationen

Das Personal des Datenverarbeiters ist über Datenschutz und Datenprivatsphäre informiert und durch Verschwiegenheitsverpflichtungen gebunden, die eine Verbreitung von Daten, Informationen sowie Personenbezogener Daten der Kunden und Nutzer des Datenverarbeiters verhindern. Nur befugtes Personal hat Zugang zu den Daten und die Zulassung wird durch den IT-Support des Datenverarbeiters gesteuert. Auch externe Dienstleister, wie z.B. Reinigungspersonal, sind sorgfältig ausgewählt und durch Verschwiegenheitsverpflichtungen gebunden.

Handhabung von sicherheitsrelevanten Vorfällen

Bei einem sicherheitsrelevanten Vorfall, der den Verantwortlichen betrifft oder betreffen kann, ergreift der Datenverarbeiter umgehend geeignete Maßnahmen und erstattet umgehend Bericht an die Kontaktperson des Verantwortlichen.

ANLAGE 3 – GENEHMIGTE UNTER-DATENVERARBEITER

Der Datenverarbeiter verwendet folgende genehmigte Unter-Datenverarbeiter bei den Dienstleistungen der jeweiligen Abteilungen:

Abteilung Löhne & Gehälter:

Flexapplications Sverige AB, Drottninggatan 22, 702 10 Örebro, Schweden

Org.-Nr.: 556616-1948

Dienstleistung: Erfassung von Zeit und Reiseabrechnungen zum Gehalt

Die Verarbeitung der Personenbezogenen Daten erfolgt in Schweden.

Fortnox AB, Box 427, 351 06 Växjö, Schweden

Org.-Nr.: 556469-6291

Dienstleistung: Gehaltssystem

Die Verarbeitung der Personenbezogenen Daten erfolgt in Schweden.

Abteilung Finanzbuchhaltung:

Fortnox AB, Box 427, 351 06 Växjö, Schweden

Org.-Nr.: 556469-6291

Dienstleistung: Finanzbuchhaltungssystem

Die Verarbeitung der Personenbezogenen Daten erfolgt in Schweden.