Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 Abs. 3 DSGVO

Der Verantwortliche

Der Auftragsverarbeiter

im Folgenden Auftraggeber

im Folgenden Auftragnehmer

(sofern nicht angegeben gelten als Auftraggeber und Auftragnehmer die Parteien des zugrundeliegenden necta Lizenz-/Mietvertrags)

1. GEGENSTAND DER VEREINBARUNG

Gegenstand dieses Auftrages ist der Betrieb von necta und zugehörigen Produkten. necta ist eine „Software as a Service“-Lösung, die den Auftraggeber im Küchenmanagement unterstützt. Dies betrifft die Bereiche Rezepte, Nährwertberechnungen, Allergenausweisung, Menüplanung, Bestellung, Warenwirtschaft und Produktionsplanung genauso wie betriebswirtschaftliche Auswertungen und Statistiken. Ebenso sind eine Kundenverwaltung mit integriertem Bestellsystem für die Kunden des Auftraggebers und ein Rechnungswesen integrale Bestandteile der Software. Für Einzelpersonen können Allergene und Unverträglichkeiten hinterlegt werden, welche im Rahmen des Bestellsystems berücksichtigt werden. Abgerundet wird die Lösung durch umfassende Schnittstellen zu Buchhaltungs- und Kassensystemen.

(a) Datenkategorien die verarbeitet werden

- Kontaktdaten
- Adressdaten
- Bankverbindungen
- Ernährungsspezifische Daten
- Allergien
- Bestelldaten
- Anwesenheitsinformationen
- Geburtsdaten
- Körpermaßdaten
- Rechnungsdaten
- Authentifizierungsdaten
- Zugriffsberechtigungen
- Kommunikationsdaten
- Lieferdaten
- Vertragsdaten
- Angaben zum Geschlecht
- Angaben zur beruflichen Funktion
- Log-Daten

(b) Kategorien betroffener Personen, die der Verarbeitung unterliegen (Die folgenden Personenkategorie verstehen sich immer in Bezug zum Auftraggeber)

- Kunden (Personen oder Organisationen)
- Kundenkontakte (belieferte Personen des Kunden)
- Lieferanten und deren Kontaktpersonen
- Ansprechpartner
- Mitarbeiter
- Benutzer der Software
- Rechnungsempfänger

2. DAUER DER VEREINBARUNG

Diese Vereinbarung gilt ab der Übertragung von Daten zur Vertragsanbahnung, während der Vertragslaufzeit des zugrundeliegenden necta Lizenz-/Mietvertrags und 3 Monate darüber hinaus. Wenn kein Vertag zustande kommt bzw. nach Ablauf des zugrundeliegenden Vertrags, werden die Daten nach Wahl des Auftraggebers innerhalb eines Monats zurückgegeben (CSV- oder Tabellenkalkulations-Format) oder gelöscht.

Liegen rechtlichen Gründe für eine weitere Aufbewahrung vor, werden die betroffenen Daten für die rechtlich begründete Dauer gespeichert. Sollen Daten darüber hinaus aufbewahrt werden, muss eine gesonderte schriftliche Vereinbarung getroffen werden, wobei der Auftraggeber die Rechtmäßigkeit der Aufbewahrung zu prüfen hat.

Es steht dem Auftragnehmer frei, anstelle der Löschung eine Anonymisierung der Daten durchzuführen. Der Auftragnehmer ist berechtigt seine mit einer Rückgabe der Daten verbundenen Aufwendungen (z.B. Datenexport, Datenträger, ...) dem Auftraggeber in Rechnung zu stellen.

3. PFLICHTEN DES AUFTRAGGEBERS

Für die Beurteilung der Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich.

Der Auftraggeber ist verpflichtet, alle im Rahmen dieser Vereinbarung erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen.

4. PFLICHTEN DES AUFTRAGNEHMERS

Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge auf Weisung des Auftraggebers zu verarbeiten.

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, ausgenommen anonymisierte statistische Auswertungen zum Zwecke der Produktentwicklung, des Betriebs und Marketinganalysen.

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 Verschwiegenheitspflicht unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat und die innerbetriebliche Organisation den Anforderungen des Datenschutzes entspricht. Einzelheiten sind der Anlage ./1 zu entnehmen.

Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) genannten Rechte der betroffenen Personen nachzukommen. Gespeicherte Daten werden gegebenenfalls in einem CSV- oder Tabellenkalkulations-Format zur Verfügung gestellt. Der Auftragnehmer ist berechtigt seine damit verbundenen Aufwendungen dem Auftraggeber in Rechnung zu stellen.

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.

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (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). Der Auftragnehmer ist berechtigt seine damit verbundenen Aufwendungen dem Auftraggeber in Rechnung zu stellen.

Der Auftragnehmer führt, für die vorliegende Auftragsverarbeitung, ein Verarbeitungsverzeichnis nach Art 30 DSGVO.

Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht 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. Dem Wunsch des Auftraggebers nach einer Inspektion wird nach gemeinsamer Terminvereinbarung innerhalb einer Frist von längstens zwei Monaten nachgekommen. Pro Jahr ist maximal eine Inspektion im Ausmaß eines Tages zulässig. Der Auftragnehmer ist berechtigt seine damit verbundenen Aufwendungen dem Auftraggeber in Rechnung zu stellen.

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, dass eine Weisung des Auftraggebers gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder des Mitgliedstaates verstößt.

5. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Alle Datenverarbeitungstätigkeiten die das Produkt necta betreffen werden ausschließlich innerhalb der EU und des EWR durchgeführt. Die unterstützenden Prozesse Helpdesk und Projektmanagement greifen auch auf Ressourcen außerhalb der EU zurück. Diese befinden sich ausschließlich in Ländern mit angemessenem Schutzniveau laut DSGVO Artikel 45 Absatz 3 oder es besteht ein Vertag mit den Unternehmen, welcher ein angemessenes Schutzniveau bestimmt.

6. SUB-AUFTRAGSVERARBEITER

Der Auftragnehmer kann Sub-Auftragsverarbeiter hinzuziehen, wobei der Auftragnehmer den Auftraggeber über die beabsichtigte Hinzuziehung oder Ersetzung der Sub-Auftragsverarbeiter zu informieren hat. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. 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.

Für den Auftraggeber (sofern diese Vereinbarung nicht unterzeichnet wurde, gilt diese mit dem zugrundeliegenden necta Lizenz-/Mietvertrag auf Basis des darin enthaltenen Software License Agreements (SLA) als abgeschlossen)	Für den Auftragnehmer
Datum: _____	Datum: 16.05.2018
Name: _____	Name: Reinhold Fenz
Funktion: _____	Funktion: Geschäftsführer
_____	_____
Unterschrift	Unterschrift

ANLAGE ./1 - Technisch-Organisatorische Maßnahmen

1. Organisationskontrolle

Das Datenschutz-Management wird durch die Entwicklungsleitung durchgeführt. Alle Mitarbeiter sind sich der wichtigen Aufgabe bewusst den Datenschutz zu wahren und werden zu jeder neuen Produktrelease über etwaige Änderung, oder notwendige Maßnahmen informiert. Neue Mitarbeiter werden entsprechend geschult und deren Wissen laufend überprüft.

Der zentrale Support des Auftragnehmers gewährleistet ein akkurates und lückenloses Incident-Response-Management. Das System selbst wird laufend proaktiv überwacht, erkannte Fehler in einem Ticket-System erfasst. Der Auftraggeber wird bei Störfällen informiert bzw. kann jederzeit selbst erkannte Fehlersituationen an unseren Support melden (via Helpdesk oder E-Mail).

In necta werden wichtige Daten des Auftraggebers verarbeitet, datenschutzfreundliche Voreinstellungen sind daher selbstverständlich bzw. Bestandteil des Systemdesigns.

Für die Auswahl von Unternehmen die Verarbeitungen für den Auftragnehmer durchführen gibt es einen Kriterienkatalog. Unternehmen mir Zertifizierungen bezüglich Datenschutz werden nach Möglichkeit bevorzugt und anderenfalls die technischen und organisatorischen Maßnahmen detailliert verhandelt. Ein Vertrag zur Auftragsdatenverarbeitung ist Voraussetzung für eine Zusammenarbeit.

Alle Mitarbeiter, sowohl Angestellte als auch freie Dienstnehmer, sind nach österreichischem bzw. deutschem DSG dem Datengeheimnis, auch über die Beschäftigung hinaus, verpflichtet.

Der Auftragnehmer hat einen zertifizierten internen Datenschutzbeauftragten nominiert.

2. Vertraulichkeit

(a) Zutrittskontrolle

Der Betrieb der necta Cloud Instanz erfolgt in einem Rechenzentrum der Firma ProfitBricks GmbH. ProfitBricks trifft hierbei alle wichtigen Vorkehrungen zum Schutz des physikalischen Zugriffs auf die Rechnersysteme und die dazugehörige Infrastruktur. Am Standort des Auftragnehmers befinden sich die Systeme für die Produktentwicklung sowie, für Test und Fehleranalyse.

Die dafür notwendige IT befindet sich in zu Betriebszeiten persönlich besetzten und überwachten Räumlichkeiten. Besuche erfolgen nur nach Voranmeldung, werden im zentralen Sekretariat erfasst und können sich in den sensiblen Bereichen nur unter Aufsicht bewegen. Außerhalb der Öffnungszeiten sind die Räumlichkeiten verschlossen (sowohl die Betriebsräume, als auch das gesamte Gebäude, welches zusätzlich über eine Video-Überwachung verfügt). Die den Mitarbeitern zur Verfügung gestellten Schlüssel werden personengebunden registriert, sowie die Schlüsselausgabe quittiert. Die Räumlichkeiten des Auftragnehmers sind im 2. Stock eines Technologie-Zentrums, der Zugang in das Gebäude ist mit elektronischem Schlüsselsystem ausgestattet und die Eingänge sind Videoüberwacht. Beim Auftragnehmer vor Ort befindet sich, neben den Entwicklungsgeräten, lediglich ein zentrales Server-Rack in einem getrennten, extra beaufsichtigten Raum. Auf diesem werden Daten nur temporär für die interne Qualitätskontrolle verarbeitet. Backups sind verschlüsselt und werden verschlossen aufbewahrt. Die gesamte interne Netzwerkstruktur befindet ausschließlich in verschlossenen Räumlichkeiten, die externe Kommunikation erfolgt immer verschlüsselt (VPN/SSL) und wird über moderne Firewalls geschützt.

(b) Zugangskontrolle

Neben dem Schutz vor physikalischem Zugriff, sind alle Systeme mit modernen Zugriffskontrollen gesichert und werden mit entsprechenden Einstellungen betrieben (beispielsweise automatischer Sperre unbesetzter Stationen, erzwungener Passwort-Wechsel inkl. Mindest-Komplexität, zwingender Einsatz sich laufend aktualisierender Virensoftware, automatische Updates der Betriebssysteme, uvm.). Die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) orientieren sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen (Berechtigungskonzept nach dem Need-to-Know-Prinzip).

Mobile Endgeräte, die Zugriff auf das System haben, werden nur partiell genutzt und sind zusätzlich mit einer entsprechenden Datenverschlüsselung ausgestattet. Obwohl die aktuellen Daten des Auftraggebers nur auf den Servern des externen Rechenzentrums verarbeitet werden, soll dadurch zusätzlich jedweder Zugang zu Informationen des Basisprodukts, oder der zugrundeliegenden Source Codes, abgewendet werden. Es haben ausschließlich Geräte, die unter der Administration des Auftragnehmers stehen Zugriff auf Unternehmensdaten. Private Geräte jeder Art wie auch Geräte von Gästen sind technisch abgetrennt. Alle Systeme mit Daten des Auftraggebers werden auf mittels IPS und IDS auf Unregelmäßigkeiten überwacht.

(c) Zugriffskontrolle

Bereits der Betreiber des genutzten Rechenzentrums (ProfitBricks) trifft umfangreiche Vorkehrungen den unerlaubten Zugriff auf die Systeme zu unterbinden, und auch erlaubte Zugriffe bereits von der Basis weg zu protokollieren. Unser darauf aufbauendes Produkt verfügt über ein umfassendes Programm an abgestuften Berechtigungen und Zugriffskontrollen. Es wird organisatorisch sichergestellt, dass immer nur der unbedingt nötige Personenkreis Zugriff hat. Der Auftraggeber hat damit nicht nur laufend Einsicht wer auf seine Daten zugreifen darf, sondern auch welche wichtigen Daten und Einstellungen während des Betriebs geändert wurden.

Zugriffe auf Systeme des Auftraggebers im Zuge des Supports sind nur unter aktiver Mitwirkung des Fernwartungs-Partners möglich, das Beenden einer Session kann von beiden Seiten erfolgen und ist einfach erkennbar.

Der Entzug von Rechten bei Änderung des Aufgabenbereichs von Mitarbeitern und Dienstleistern ist organisatorisch geregelt und dokumentiert.

(d) Pseudonymisierung

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung, soweit sinnvoll, entfernt, und gesondert aufbewahrt. Der Auftraggeber hat die Möglichkeit Daten pseudonymisiert zu erfassen. Personenbezogene Daten können auf Anforderung des Auftraggebers anonymisiert werden. Auf rechtliche Aufbewahrungsfristen wird dabei Rücksicht genommen. Für anfallende Meta-Daten (z.B. Logfiles) sind Löschfristen definiert, eine Pseudonymisierung findet nicht statt.

(e) Datenklassifikation

Alle personenbezogenen Daten, die vom Auftraggeber ins System eingegeben werden sind als vertraulich klassifiziert. Eine Weitergabe der Daten erfolgt ausschließlich zum Zweck der Auftragserfüllung und auf schriftliche Weisung des Auftraggebers oder wenn rechtlich zwingend erforderlich.

3. Integrität

(a) Weitergabekontrolle

Mittels durchgängiger Verschlüsselung bei der Übertragung von Daten wird unbefugtes Lesen, Kopieren, Verändern oder Entfernen verhindert. Für die Verschlüsselung der Verbindungen, sowie der Datenträger, werden nur als sicher geltende Verschlüsselungsalgorithmen verwendet. Die verwendete Software wird aktuell gehalten. Eine Verwendung von externen Datenträgern wird nach Möglichkeit vermieden und bevorzugt auf sichere Übertagungen auf Serverdienste zurückgegriffen.

E-Mails werden ausschließlich über den Dienst des Aufragnehmers gesendet bzw. empfangen und dabei protokolliert. Das Löschen bzw. die Vernichtung von Daten erfolgt mit entsprechenden Werkzeugen durch Aktenvernichter, mehrfaches Überschreiben oder entsprechende physikalische Zerstörung. Die Löschung selbst wird protokolliert, wobei festgehalten wird warum gelöscht wird.

(b) Eingabekontrolle

Die Konzeptionierung und Einrichtung neuer Systeme wird dokumentiert, Änderungen am necta-System obliegen einem Änderungsmanagement-Prozess. Die Änderungen werden ausschließlich durch die Leitung einer Abteilung genehmigt.

Die Erstellung, Änderung und Löschung von kritischen personenbezogenen Informationen wird protokolliert. Durch starke Authentifizierungsmechanismen wird sichergestellt, dass nur Befugte Änderungen vornehmen können.

Metadaten wie Verbindungsdaten, Zugriffs-Protokolle und System-Protokolle werden laufend automatisch überwacht und regelmäßig manuell überprüft. Der Zugriff ist entsprechend des Rollen-Konzepts eingeschränkt.

4. Verfügbarkeit und Belastbarkeit

Die vertraglich vereinbarte Verfügbarkeit wird durch teil-redundant ausgelegte Systeme gestützt. Die Infrastruktur ist bei namhaften Providern mit zugesicherter hoher Verfügbarkeit und hohen Sicherheitsstandards untergebracht.

Ein mehrstufiges Sicherungskonzept mit Generationensicherung und mehrerer Kopien an unterschiedlichen Standorten inklusive regelmäßig getesteter Wiederherstellungspläne fördert die rasche Wiederherstellbarkeit. Die Lagerung der Sicherungen erfolgt ausschließlich verschlüsselt, die zugehörigen Schlüssel und Passworte liegen in ausgedruckter Form vor.

Die Belastbarkeit der Systeme wir durch ein Monitoring-System überwacht, so dass Unregelmäßigkeiten im Betrieb schnell erkannt und Maßnahmen ergriffen werden können. Zur Erhaltung der Sicherheit des Systems finden regelmäßig interne Sicherheits-Überprüfungen statt.

Zur Behebung von Störungen gibt es einen Alarmierungsplan um auch außerhalb der Geschäftszeiten angemessen zu reagieren und die zugesagten SLAs einzuhalten. Für den Fall eines Desasters wird ein Notfallsystem verfügbar gehalten.