Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO haude Produktsupport

Abgeschlossen von und zwischen

einem haude Kunden

nachstehend Auftraggeber genannt
und

haude electronica Verlags-GmbH
Nestroyplatz 1, A-1020 Wien, FN 181372z, Handelsgericht Wien

nachstehend Auftragnehmer genannt –

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Auftragnehmer ist Anbieter von Finanzsoftware. Der Auftraggeber ist Kunde des Auftragnehmers im Rahmen einer bestehenden Geschäftsbeziehung und nutzt die Programme des Auftragnehmers für die Zwecke der Abwicklung seines Betriebes. Gegenstand des Vertrages zum Datenumgang ist daher, in Ergänzung zur (bereits bestehenden) Vertragsbeziehung zwischen Auftraggeber und Auftragnehmer, die Neuregelung der wechselseitigen Rechte und Pflichten zur Durchführung der im Rahmen des (bereits bestehenden) Vertrages bestehenden Pflicht des Auftragnehmers zur Verarbeitung von personenbezogenen Daten durch den Auftragnehmer im **Zuge des Produktsupports**.

(2) Dauer

Der Auftrag wird in laufender Geschäftsbeziehung zwischen Auftragnehmer und Auftraggeber ständig ausgeführt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten:
Der Zweck der Verarbeitung ist die Ermöglichung eines automationsunterstützten Produktsupports inkl. Fernwartung, insoweit zur jeweiligen Problembehebung notwendig, auf Grundlage des zwischen Auftraggeber (Verantwortlicher) und Auftragnehmer (Auftragsverarbeiter) bestehenden Vertrages in datenschutzkonformer Form.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien) insbesondere aber nicht ausschließlich:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- und Vertragshistorie, etc.)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Kundendaten
- Bilddaten Fernwartung

(3) Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen insbesondere aber nicht ausschließlich:

- Klienten des Auftraggebers
- Mitarbeiter von Klienten des Auftraggebers
- Kunden von Klienten des Auftraggebers
- Lieferanten von Klienten des Auftraggebers
- Mitarbeiter des Auftraggebers
- Lieferanten des Auftraggebers
- Auftraggeber
- Ansprechpartner

3. Technisch-organisatorische Maßnahmen

(1) Die in Anlage 1 genannten bestehenden und beim Auftragnehmer entsprechend dokumentierten technischen und organisatorischen Maßnahmen werden dem Auftraggeber hiermit als Grundlage des Auftrags zur Kenntnis gebracht und seitens des Auftraggebers als für den oben angeführten Zweck entsprechend angenommen.

(2) Der Auftragnehmer hat die Sicherheit gern. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den getroffenen Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines, dem Risiko angemessenen, Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei werden vom Auftragnehmer der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO berücksichtigt.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei wird das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen wird der Auftragnehmer dabei dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer wird die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter schriftlicher Weisung des Auftraggebers gegen Abgeltung der Aufwände des Auftragnehmers in diesem Zusammenhang berichtigen oder löschen und nur insofern, als dies zur Lösung eines Supportfalles notwendig ist (Beispiel „Übermittlung Betrieb"). Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen innerhalb einer Frist von 10 Werktagen ab Kenntnisnahme durch den Auftragnehmer an den Auftraggeber weiterleiten.

(2) Allfällige im Supportfall dem Auftragnehmer zugekommene bzw. übermittelte personenbezogene Daten des Auftraggebers werden vom Auftragnehmer so lange gespeichert, wie es der Zweck der Vertragserfüllung vernünftigerweise gebietet.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten als Auftragsverarbeiter gemäß den auf ihn zutreffenden Abschnitten der Art. 28 bis 33 DS-GVO; insofern gewährleistet er die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Für datenschutzrechtliche Belange werden Kontaktdaten im Impressum auf der Homepage des Auftragnehmers benannt.
b) Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO: Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend des Vertragszwecks verarbeiten, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO gemäß Anlage 1.
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Es erfolgt die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen und der Auftragnehmer Kenntnis hiervon hat. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, wird der Auftragnehmer den Auftraggeber bei Bedarf unterstützen. Hierfür gebührt ihm ein angemessenes Entgelt zur Abgeltung des Aufwandes.
g) Der Auftragnehmer wird regelmäßig seine internen Prozesse mit Bezug auf den Auftrag sowie die technischen und organisatorischen Maßnahmen mit Bezug auf den Auftrag prüfen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

6. Unterauftragsverhältnisse

Der Auftragnehmer nimmt Dienstleistungen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen sowie für die Erbringung von Supportleistungen in Anspruch.

(2) Festgehalten wird, dass aktuell uA die nachstehenden Dienstleister für den Auftragnehmer in diesem Bereich tätig sind.

- ProSaldo.net GmbH
- dvo Software Entwicklungs- und Vertriebs-GmbH
- Data Noah GmbH

(3) Nimmt der Auftragnehmer zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen (wie etwa Rechenzentrumsdienstleistungen) weitere oder andere als die oben genannten Dienstleister in Anspruch und gewährleisten diese Dienstleister den Schutz der personenbezogenen Daten und die Datensicherheit, dokumentiert in demselben oder einem höheren Ausmaß, wie der/die bisherigen Dienstleister des Auftragnehmers, so gilt die Zustimmung zur Inanspruchnahme weiterer oder anderer Dienstleister durch den Auftraggeber als erteilt. Ebenso gilt dies für Dienstleistungen wie etwa Telekommunikationsleistungen, Post- /Transportdienstleistungen, Programmier- Wartungs- und Benutzerservices oder die Entsorgung von Datenträgern

(4) Der Auftragnehmer wird mit Rücksicht auf das Risiko der Verarbeitungstätigkeit, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers bei der Inanspruchnahme von diesen oder weiteren Dienstleistern angemessene vertragliche Vereinbarungen und/oder Kontrollmaßnahmen ergreifen.

(5) Insoweit eine Inanspruchnahme weiterer Unterauftragnehmer im Hinblick auf eine inhaltliche Verarbeitungstätigkeit der personenbezogenen Daten des Auftraggebers notwendig wird, wird der Auftragnehmer jedenfalls die vorherige Zustimmung des Auftraggebers einholen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Einvernehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. In diesem Sinn kann er sich bei einer rechtzeitigen Voranmeldung des Prüfungstermins, der in Absprache mit dem Auftragnehmer festzusetzen ist, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb überzeugen.

(2) Alternativ kann der Nachweis der Maßnahmen, die den konkreten Auftrag und darüberhinausgehende Maßnahmen des Auftragnehmers betreffen, durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit erfolgen.

(3) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen angemessenen Anspruch auf Abgeltung der entstandenen Kosten geltend machen.

8. Mitteilung bei Verstößen

(1) Der Auftragnehmer unterstützt den Auftraggeber bei Bedarf bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören:

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen (gemäß Anlage 1), die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen;
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich ab Kenntnisnahme durch den Auftragnehmer an den Auftraggeber zu melden;
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen zur Verfügung zu stellen; dies nur soweit der Auftraggeber diese nicht selbsttätig abrufen kann und der Auftragnehmer davon Kenntnis hat;
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des vom Auftraggeber beim Auftragnehmer genützten Produktes enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers – Einwilligung durch Mitarbeiter des Auftraggebers

(1) Der Auftraggeber wird nur schriftliche Weisungen an den Auftragnehmer in Bezug auf diese Vereinbarung erteilen, um seiner Nachweispflicht entsprechen zu können.

(2) Der Auftragnehmer wird den Auftraggeber informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(3) Insofern ein Fern-Support (Fernwartungsfall) über Mitarbeiter des Auftraggebers abgewickelt wird, erklärt der Auftraggeber, dass er seine Mitarbeiter bevollmächtigt hat, Supportanfragen zu stellen und die für die Lösung des Supportfalls notwendigen Einwilligungen (etwa zur Bildschirmeinsicht) dem Auftragnehmer gegenüber rechtsverbindlich auszusprechen.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) 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) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber wird der Auftragnehmer, insofern keine gesetzliche Pflicht oder Notwendigkeit der vertraglichen Abwicklung zwischen dem Auftraggeber und dem Auftragnehmer besteht, zur weiteren Aufbewahrung sämtliche Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht löschen.

(3) Dokumentationen inklusive Bilddaten Fernwartung, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, können durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt und – das Einverständnis des Kunden vorausgesetzt - zur zukünftigen Fehlerbehebung bzw. Weiterentwicklung des Programmes weiterverarbeitet werden.

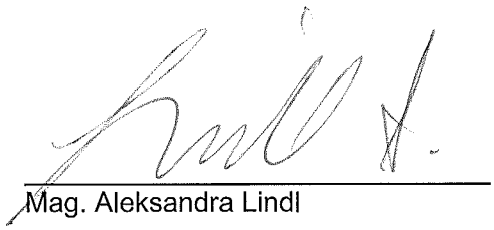
11. Einhaltung der Pflichten des Verantwortlichen durch den Auftraggeber

(1) Der Auftraggeber gewährleistet dem Auftragnehmer bei sonstiger Schad- und Klagloshaltung des Auftragnehmers, die ihm im Rahmen der DS-GVO obliegenden Pflichten einzuhalten.

12. Geltung des Vertrages zwischen Auftraggeber und Auftragnehmer

(1) Diese Vereinbarung ergänzt die (bestehenden) Vertragsbeziehungen zwischen Auftraggeber und Auftragnehmer in Bezug auf die Auftragsverarbeitung von Daten. Hierbei geht sie den übrigen Regelungen zwischen dem Auftraggeber und dem Auftragnehmer vor. Die Geltung der übrigen Vertragsbestandteile zwischen Auftraggeber und Auftragnehmer (insbesondere in Bezug auf Kündigung des Vertrages, Haftung für Schäden, Zahlung der Entgelte etc.) wird dadurch nicht berührt.

Auftragnehmer
Haude electronica Verlags-GmbH



Mag. Aleksandra Lindl

Wien am 12.05.2023

Anlage 1 Technisch-organisatorische Maßnahmen

Eine Zusammenfassung relevanter technisch organisatorischer Maßnahmen lt. EU-DSGVO bzw. AT-DSAG2018 im Kontext dieses Dokuments sind wie folgt aufgeführt.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

   a) Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen der haude Büroräumlichkeiten mittels elektronischem Zutrittssystem via Chipkarten sowie elektrischem Türöffner. Eine passive Absicherung erfolgt mittels Alarmanlage sowie Videoanlage.
   b) Zugangskontrolle: Keine unbefugte Systembenutzung des internen Netzwerks mittels sicherer und ablaufender Kennwörter bzw. z.T. Mehrfaktorauthentifizierung. Automatische Konten-Sperrmechanismen sowie Verschlüsselung von Datenträgern bei mobilen Geräten.
   c) Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems mittels granularer Berechtigungskonzepte und bedarfsgerechter Zugriffsrechte sowie Protokollierung von Systemanmeldungen.
   d) Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden mittels getrennt berechtigter Netzlaufwerke und mandantenfähiger Service- bzw. Drittsysteme.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

   a) Weitergabekontrolle: Es soll kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport stattfinden können. Dies wird bei der Verbindung zu allen externen Systemen durch zwingenden Einsatz von verschlüsselten Verbindungen ermöglicht, ggf. Verbindungsaufbau per Virtual Private Networks (VPN) sowie mehrstufige Sicherheitszonen- und Authentifizierungsgestaltung;
   b) Eingabekontrolle: Es soll festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

   a) Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust mittels dokumentierter Backup-Strategie (online/offline; on-site/off-site), Stromversorgungsredundanz, Virenschutz, Firewall, Meldewege und Notfallpläne.
   b) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO): Die Wiederherstellbarkeit einer operativen Betriebsumgebung in verschiedenen Desaster-Szenarien ist in internen Notfallplänen festgehalten. Die Systemarchitektur in Kombination mit Drittsystemen erlaubt auch georedundantes Operating.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

a) Datenschutz-Management: Liegt vor, siehe Inhalte dieses Dokuments, v.a. Punkt 5
b) Incident-Response-Management: Liegt vor, siehe Inhalte dieses Dokuments, v.a. Punkt 5 und 8.
c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO): Werden großteils von eingesetzter Drittanbieter-Software ermöglicht bzw. unterstützt.
d) Auftragskontrolle: Es erfolgt keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B. durch eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl von Drittanbietern und ggf. Sub-Dienstleistern, Vorabüberzeugung, Nachkontrollen. Siehe dazu Inhalte des vorliegenden Dokuments, v.a. Punkt 4, 5, 7 und 9.