Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Abgeschlossen von und zwischen

einem Data Noah Kunden
-nachstehend Auftraggeber genannt -
und

Data Noah GmbH
Nestroyplatz 1, A-1020 Wien, FN 217244b, Handelsgericht Wien

nachstehend Auftragnehmer genannt.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Auftragnehmer ist Anbieter von Online Datensicherungssoftware und IT-Infrastrukturdienstleistungen für Unternehmen aller Art. Der Auftraggeber ist Kunde des Auftragnehmers im Rahmen einer Geschäftsbeziehung und nutzt

Data Noah Online Backup bzw. IT-Infrastruktur Dienstleistungen

für die Zwecke der Datensicherung bzw. zur IT-Unterstützung seines Betriebes. Gegenstand des Vertrages zum Datenumgang ist daher in Ergänzung zur Vertragsbeziehung zwischen Auftraggeber und Auftragnehmer die Regelung der wechselseitigen Rechte und Pflichten zur Durchführung der im Rahmen des Vertrages bestehenden Pflicht des Auftragnehmers zur Verarbeitung von personenbezogenen Daten durch den Auftragnehmer.

(2) Dauer

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

2. Konkretisierung des Auftragsinhalts

(1) Zweck und Art der vorgesehenen Verarbeitung von Daten:

Der Zweck der Verarbeitung ist die Ermöglichung eines Datensicherungsprozesses und zur IT-Unterstützung auf dieser und der gesonderten vertraglichen Grundlage zwischen Auftraggeber („Verantwortlicher“) und Auftragnehmer („Auftragsverarbeiter“) in datenschutzkonformer Form.

Der Auftragnehmer wird dabei die personenbezogenen Daten des Auftraggebers in technisch organisatorischer Form (dh für die Bereitstellung von IT-Dienstleistungen und Wartung der automationsunterstützten Datensicherungsprozesse) mit Hilfe automationsunterstützter Prozesse verarbeiten. Der Auftragnehmer verarbeitet mit Ausnahme der unten angeführten Datenarten zur IT-Unterstützung ausschließlich anonyme bzw. vollverschlüsselte Daten und damit solche, die nicht dem Anwendungsbereich der DSG-VO unterliegen. Der nähere Umfang der Art der technisch-organisatorischen Datenverarbeitung des Auftragnehmers ergibt sich aus den einzelnen Leistungsbeschreibungen der jeweiligen Produkte Whitepapers/Beschreibungen des Online Backup Produkts sowie der technisch

organisatorischen Maßnahmen anbei, wobei Erstere auf der Webseite des Auftragnehmers veröffentlicht sind bzw. dem Auftraggeber jederzeit ausgefolgt werden können und zwischen den Parteien dieses Vertrages als bekannt gelten.

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

Der Auftragnehmer verarbeitet die nachstehenden personenbezogenen Datenarten des Auftraggebers:

- Personenstammdaten
- Benutzerstammdaten
- Kommunikationsdaten
- Bilddaten (Fernwartung)

(3) Kategorien betroffener Personen

Insbesondere aber nicht ausschließlich:

- Mitarbeiter des Auftraggebers
- Lieferanten des Auftraggebers
- Ansprechpartner
- Auftraggeber

(4) Empfängerkreise der personenbezogenen Daten

Auf Seiten des Auftragnehmers ergeben sich im Hinblick auf die Verarbeitungstätigkeit aufgrund der Zusammenarbeit mit der Firma dvo Software Entwicklungs- und Vertriebs-GmbH nachstehende Empfängerkreise:

- dvo Software Entwicklungs- und Vertriebs-GmbH

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) 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 Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Aus der technisch organisatorischen Natur der Verarbeitungstätigkeit des Auftragnehmers von personenbezogenen Daten für den Auftraggeber ergibt sich, dass der Auftragnehmer solche Daten des Auftraggebers weder in eigener Verantwortung berichtigt oder die Verarbeitungstätigkeit im datenschutzrechtlichen Sinn einschränkt. Eine diesbezügliche Weisungsbefugnis des Auftraggebers an den Auftragnehmer besteht mangels vertraglicher Pflichten hierrüber nicht. Hiervon ausgenommen sind jene Fälle wo der Auftragnehmer aufgrund vertraglicher Verpflichtungen eine entsprechende Verarbeitung durchzuführen hat (etwa Anlage und Wartung von Benutzerstammdaten des Auftraggebers). Der Auftragnehmer wird die Löschung personenbezogener Daten des Auftraggebers nur in technisch-organisatorischer Form automationsunterstützt nach eindeutiger technischer Anweisung des Auftraggebers durchführen; dies nach den in der Leistungsbeschreibung der einzelnen Produkte angeführten näheren Bedingungen und Möglichkeiten.

(3) Es obliegt mit Rücksicht auf die Art der Verarbeitungstätigkeit des Auftragnehmers dem Auftraggeber die vertragsgegenständlichen Dienste für die Umsetzung eines Löschkonzepts, das Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft selbst unmittelbar zu nützen.

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.

6. Unterauftragsverhältnisse

(1) Der Auftragnehmer nimmt Dienstleistungen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen (wie etwa Rechenzentrumsdienstleistungen) in Anspruch.

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

- next layer Telekommunikationsdienstleistungs- und Beratungs-GmbH
- Linz AG Telekom
- dvo Software Entwicklungs- und Vertriebs-GmbH
- haude electronica Verlags-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

(1) Der Auftraggeber wird dort, wo ein Weisungsrecht für die Verarbeitung von personenbezogenen Daten des Auftraggebers besteht (etwa Anlage und Wartung von Benutzerstammdaten), solche Weisungen nur schriftlich erteilen.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich 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 oder 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 (Redundanz, Backup, etc. - siehe Leistungsbeschreibungen) erforderlich sind.

(2) Die Löschung von personenbezogenen Daten und anonymen/vollverschlüsselten Daten erfolgt nach den in der Leistungsbeschreibung zum Produkt Data Noah Backup bzw. der Leistungsbeschreibung zur IT-Unterstützung näher angeführten Umständen.

11. Einhaltung der Pflichten des Verantwortlichen durch den Auftraggeber

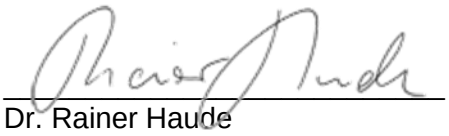
(1) Der Auftraggeber gewährleistet dem Auftragnehmer bei sonstiger Schad- und Klagloshaltung des Auftragnehmers, die ihm im Rahmen der DS-GVO obliegenden Pflichten als Verantwortlicher einzuhalten.

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 im Bezug auf Kündigung des Vertrages, Haftung für Schäden, Zahlung der Entgelte etc.) wird dadurch nicht berührt.

Auftragnehmer
Data Noah GmbH



Dr. Rainer Haude

Wien am 13.06.2023

ANLAGE 1: Zusammenfassung technisch-organisatorische Maßnahmen im Data Noah Rechenzentrum lt. EU-DSGVO bzw. AT-DSAG2018

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)
    a. Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen innerhalb des Data Noah Rechenzentrum; Chipkarten, Schlüssel, elektrische Türöffner, Schleuse, Pförtner, Alarmanlagen, Videoanlagen;
    b. Zugangskontrolle: Keine unbefugte Systembenutzung innerhalb des Data Noah Rechenzentrum durch zwangsweise sichere Kennwörter, automatische Sperrmechanismen ab mehrmaliger Falscheingabe, teilweise mehrstufige Authentifizierung oder Mehrfachauthentifizierung, Verschlüsselung von allen eingehenden Verbindungen;
    c. Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch Netzwerk- und Mikrosegmentierung, Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte auf allen Ebenen, Protokollierung von Anmeldungen auf Ebene der Authentifizierung;
    d. Trennungskontrolle: Im Rechenzentrum erfolgt grundsätzlich eine getrennte Verarbeitung von Daten, die in den jeweiligen Bereichen von unterschiedlichen Mandanten und zu unterschiedlichen Zwecken erhoben und verarbeitet wurden, dies wird durch den vollmodularen Aufbau der Architektur und aller Produkte im Data Noah Rechenzentrum gewährleistet;
    e. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO): Auf Ebene der Speicherung aller Daten innerhalb des Data Noah Rechenzentrum erfolgt die Ablage ausschließlich modular auf dedizierte Enterprise-Storagesysteme, welche die aufgenommenen Daten ausschließlich auf Blockebene ablegen, replizieren und assoziieren. Ohne das Heranziehen mehrschichtiger Logikelemente sind die gespeicherten Daten nicht zuordenbar.
    Die Verarbeitung personenbezogener Daten innerhalb von Drittanbieter-Anwenderprogrammen sollte in einer Weise erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen – dies muss jedoch von der entsprechenden Drittanbieter-Software ermöglicht bzw. gewährleistet werden; Data Noah Online Backup überträgt und speichert alle zu sichernden Daten ausschließlich hochverschlüsselt ab der Sicherungsquelle, alle diesbezüglichen Daten gelten somit als anonymisiert/pseudonymisiert.
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 in das Data Noah Rechenzentrum ermöglicht durch zwingenden Einsatz von verschlüsselten Verbindungen, Verbindungsaufbau per Virtual Private Networks (VPN), mehrstufige Sicherheitszonen- und Authentifizierungsgestaltung je nach Produkt sofern anwendbar (siehe LB des Produkts);
    b. Eingabekontrolle: Es soll festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, dies erfolgt z.B. durch Protokollierung. Jedoch muss dies von der entsprechenden Drittanbieter-Software ermöglicht bzw. unterstützt werden und ist nicht Bestandteil der gegenständlichen, gehosteten Produkte.
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)
    a. Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), Stromversorgungsredundanz, Virenschutz, Firewall, Meldewege und Notfallpläne – bei Hosting nur für Infrastruktur lt. LB.
    b. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO) – bei Hosting nur für Infrastruktur lt. LB.
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 und wird gemäß Auftragsverarbeiter-Vereinbarung verwaltet.
    b. Incident-Response-Management: Liegt vor.
    c. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO); Dies muss ausschließlich von der entsprechenden Drittanbieter-Software ermöglicht bzw. unterstützt werden.
    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.