

Vertragliche Regelungen zur Projekt- und Portfoliomanagementsoftware WORKSPACE.PM

Inhalt:

Allgemeine Geschäftsbedingungen	Seite 2
Lizenzbedingungen	Seite 6
Servicelevel und Support-Vertrag	Seite 9
Backup-Konzept	Seite 13
Auftragsverarbeitungsvertrag	Seite 17

Serviceanbieter

AMNAU GmbH
Kronenstraße 13
30161 Hannover
Deutschland

Geschäftsführung

Benjamin Bolzmann

Rechtliche Angaben

Die AMNAU GmbH ist ein beim Amtsgericht
Hannover eingetragenes Unternehmen: HRB 228100

USt-ID: DE450283837

AMNAU ist eine beim Deutschen Patent- und
Markenamt eingetragene Marke (DE302024226913)

Allgemeine Geschäftsbedingungen

1. Geltungsbereich

(1) Diese allgemeinen Geschäftsbedingungen („AGB“) regeln das Verhältnis zwischen der AMNAU GmbH, Kronenstraße 13, 30161 Hannover („Lizenzgeber“) und dem Vertragspartner des Lizenzvertrages sowie mit dem Vertragspartner verbundene Unternehmen, soweit diese laut Lizenzvertrag zur Nutzung des Vertragsproduktes berechtigt sind (insgesamt gemeinsam bezeichnet als „Lizenznehmer“). Lizenzgeber und Lizenznehmer werden jeweils einzeln auch als „Partei“ und gemeinsam als „Parteien“ bezeichnet.

(2) Alle zwischen Lizenzgeber und Lizenznehmer im Zusammenhang mit dem Lizenzvertrag getroffenen Vereinbarungen ergeben sich aus dem Lizenzvertrag und diesen AGB.

(3) Maßgeblich ist die jeweils bei Abschluss des Vertrags gültige Fassung der AGB.

(4) Abweichende Bedingungen des Lizenznehmers werden nicht akzeptiert. Dies gilt auch, wenn der Lizenzgeber der Einbeziehung nicht ausdrücklich widerspricht.

2. Mängelgewährleistung

(1) Ist der Lizenznehmer Unternehmer und nutzt WORKSPACE.PM als On Premises-Variante, hat er die Vertragssoftware unverzüglich nach Erhalt, soweit dies nach ordnungsgemäßigem Geschäftsgang tunlich ist, auf offensichtliche Mängel zu überprüfen und diese bei Vorliegen dem Lizenzgeber unverzüglich, spätestens jedoch innerhalb von 14 Tagen nach Erhalt der Software, schriftlich mitzuteilen. Verdeckte Mängel sind unverzüglich nach ihrer Entdeckung schriftlich zu rügen. Versäumt der Lizenznehmer die ordnungsgemäße Untersuchung und/oder Mängelanzeige, gilt die gelieferte Software als genehmigt, es sei denn, der Mangel war bei der Untersuchung nicht erkennbar. Dies gilt nicht für Mängel, die der Lizenzgeber arglistig verschwiegen hat. Im Übrigen gelten die gesetzlichen Bestimmungen, insbesondere §§ 377, 381 HGB.

(2) Es gelten die gesetzlichen Bestimmungen über die Mängelgewährleistung unter Berücksichtigung der folgenden besonderen Regelungen:

(a) Die Verjährungsfrist für Mängelgewährleistungsansprüche beträgt bei Softwarekauf ein Jahr ab Lizenzausstellung des jeweiligen Vertragsprodukts, wenn an dem Geschäft kein Verbraucher beteiligt ist.

(b) Bei der Überlassung im Rahmen von Softwaremiete wird der Lizenzgeber die Betriebsbereitschaft während der Vertragslaufzeit durch Bereitstellung von Updates aufrechterhalten.

(c) Im Rahmen der Mängelgewährleistung wird der Lizenzgeber selbst oder über von ihm beauftragte Dritte zunächst versuchen, den Fehler zu beheben (Nacherfüllung). Sofern die Nachbesserung binnen angemessener Frist nicht erfolgreich durchgeführt wird, kann der Lizenznehmer vom Vertrag zurücktreten oder Minderung (Herabsetzung der Lizenzgebühr) nach den gesetzlichen Vorschriften sowie Schadensersatz bzw.

Ersatz vergeblicher Aufwendungen geltend machen. Macht der Lizenznehmer Schadensersatz oder Ersatz vergeblicher Aufwendungen geltend, so haftet der Lizenzgeber nach Ziff. 3.

Wenn an dem Geschäft kein Verbraucher beteiligt ist, haben Minderungsansprüche Vorrang, soweit die Leistung nicht mehr nachgeholt werden kann.

(d) Soweit vorstehend nichts anderes geregelt, ist eine weitergehende Mängelgewährleistung des Lizenzgebers ausgeschlossen. Insbesondere entfällt die Mängelgewährleistung, wenn und soweit die Vertragsprodukte durch den Lizenznehmer unsachgemäß behandelt oder in einer defekten oder nicht kompatiblen Hard- oder Softwareumgebung benutzt werden. Gleiches gilt, wenn der Lizenznehmer unberechtigt Änderungen der Vertragsprodukte vornimmt.

(3) Im Falle der Mängelbeseitigung, insbesondere im Rahmen der Nachlieferung oder Nachbesserung, werden die erforderlichen Aufwendungen für die Arbeiten des Lizenzgebers oder von ihm beauftragter Dritter sowie für etwaige Transportkosten, die durch den Lizenznehmer verauslagt werden, durch den Lizenzgeber getragen bzw. erstattet. Dies gilt nicht, soweit sich diese Aufwendungen dadurch erhöhen, dass die Vertragsprodukte an einen anderen Ort als den Ort der Erstlieferung verbracht wurden.

(4) Für die Nutzung von Open Source Komponenten oder deren Konfigurationsdateien, die zusammen mit dem Vertragsprodukten ausgeliefert werden, ohne dass diese von Vertragsprodukten aktiviert, genutzt oder verlinkt werden, ist die Mängelgewährleistung des Lizenzgebers ausgeschlossen.

3. Haftung

(1) Die Mängelgewährleistung des Lizenzgebers richtet sich ausschließlich nach vorstehender Ziffer 2.

(2) Für Ansprüche des Lizenznehmers auf Schadensersatz gelten die folgenden Haftungsregelungen:

(a) Bei Geltendmachung von Schadensersatzansprüchen durch den Lizenznehmer haftet der Lizenzgeber nach den gesetzlichen Vorschriften, soweit den Ansprüchen eine Verletzung zugrunde liegt, die auf Vorsatz oder grober Fahrlässigkeit des Lizenzgebers, für eine vereinbarte Beschaffenheit der Vertragsprodukte, für eine Verletzung von Leben, Leib oder Gesundheit, nach den Vorschriften des Produkthaftungsgesetzes sowie im Umfang einer von dem Lizenzgeber übernommenen Garantie beruht. Soweit dem Lizenzgeber keine vorsätzliche Vertragsverletzung angelastet wird, ist die Haftung auf den vorhersehbaren, typischerweise eintretenden Schaden begrenzt.

(b) Der Lizenzgeber haftet zusätzlich nach den gesetzlichen Bestimmungen, soweit er schuldhaft, also auch bei Vorliegen leichter Fahrlässigkeit, eine wesentliche Vertragspflicht (Kardinalspflicht) verletzt; deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Lizenznehmer regelmäßig vertrauen kann. In diesem Fall ist die Schadensersatzhaftung auf den vorhersehbaren, typischerweise eintretenden Schaden begrenzt.

(c) Der Lizenzgeber haftet gegenüber dem Lizenznehmer, soweit nicht Vorsatz, grobe Fahrlässigkeit oder die Verletzung

einer Kardinalspflicht vorliegt in jedem Fall nur beschränkt bis maximal der dreifachen Höhe der Lizenzgebühr. Diese Haftungsobergrenze gilt nicht für typischerweise vorhersehbare Schäden.

(3) Eine weitergehende Haftung des Lizenzgebers besteht nicht.

(4) Die vorstehende Haftungsbeschränkung gilt auch für Vertreter oder Erfüllungsgehilfen des Lizenzgebers.

4. Allgemeine Haftungsregelungen

(1) Klarstellend wird darauf hingewiesen, dass vorstehende Haftungsbeschränkung gemäß Ziff. 4 in keinem Fall die gesetzlichen Ansprüche nach dem Produkthaftungsgesetz einschränken. Die Haftung für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer schuldhaften Pflichtverletzung des Lizenzgebers oder einer vorsätzlichen oder fahrlässigen Pflichtverletzung eines Vertreters oder Erfüllungsgehilfen des Lizenzgebers beruhen, wird durch vorstehende Haftungsregelungen ebenfalls nicht berührt.

(2) Der Lizenznehmer wird darauf hingewiesen, dass er im Rahmen seiner Sorgfaltspflichten vor einer ersten Verwendung der Vertragsprodukte prüfen muss, ob die Installation der Vertragsprodukte zu besonderen Interferenzen mit bereits installierter Software führen könnte, und weiter für eine Sicherung seiner Daten vor der ersten Installation und während des laufenden Betriebes zu sorgen hat und im Falle eines vermuteten Softwarefehlers alle zumutbaren zusätzlichen Sicherungsmaßnahmen ergreifen muss.

(3) Eine weitergehende Haftung auf Schadensersatz als in vorstehenden Haftungsregelungen vorgesehen, ist – ohne Rücksicht auf die Rechtsnatur des geltend gemachten Anspruchs – ausgeschlossen. Dies gilt insbesondere im Hinblick auf Schadensersatzansprüche aus Verschulden bei Vertragsabschluss, wegen sonstiger Pflichtverletzungen oder wegen deliktischer Ansprüche auf Ersatz von Sachschäden.

(4) Soweit die Schadensersatzhaftung des Lizenzgebers ausgeschlossen oder eingeschränkt ist, gilt dies auch im Hinblick auf die persönliche Schadensersatzhaftung seiner Angestellten, Arbeitnehmer, Mitarbeiter, Vertreter und Erfüllungsgehilfen.

5. Geheimhaltung

(1) Die Parteien einschließlich aller verbundenen Unternehmen, Tochterunternehmen, Niederlassungen, Berater, Mitarbeiter und aller ähnlichen Personen, Unternehmen oder natürlichen oder juristischen Personen verpflichten sich im Hinblick auf vertrauliche Informationen der jeweils anderen Partei (wie unten stehend definiert und ohne Rücksicht auf das Datum der ersten Bekanntgabe solcher vertraulichen Informationen), diese vertraulichen Informationen unbefristet geheim zu halten und nur insoweit im eigenen Unternehmen einschließlich aller verbundenen Unternehmen, Tochterunternehmen, Niederlassungen, Berater, Mitarbeiter und aller ähnlichen Personen, Unternehmen oder sonstigen natürlichen oder juristischen Personen zu verwerten/verwerten zu lassen oder selbst oder durch Dritte in sonstiger Weise zu nutzen/nutzen zu lassen, als dies zur Erfüllung von Pflichten einer Vertragspartei unumgänglich erfordert oder es sich um eine Weitergabe an beruflich zur Verschwiegenheit verpflichtete Berater handelt.

(2) Im Rahmen dieses Vertrages gelten als vertrauliche Information, insbesondere jedes Betriebsgeheimnis und sonstige, nicht öffentlich zugängliche oder vertrauliche Informationen bezüglich Produkten, Prozessen, Know-how, Design, Formeln, Entwicklungen, Forschungen, Computerprogrammen, Datenbanken, anderer urheberrechtlich geschützter Werke oder im Hinblick auf die Geschäftstätigkeit der Parteien und deren Mitarbeiter, Berater, Lizenznehmer oder anderer den Parteien zuzuordnenden Personen, die im Rahmen des Lizenz- und/oder Wartungs- und Supportvertrag oder der Überlassung von Vertragsprodukten bekannt gegeben oder in sonstiger Weise in schriftlicher oder mündlicher Form mitgeteilt werden.

(3) Der Lizenznehmer erkennt an, dass vom Lizenzgeber im Rahmen dieses Vertrages im direkten Zusammenhang mit einem Vertragsprodukt bekannt gegebene vertrauliche Informationen (z.B. Schnittstelleninformationen, Quellcode, etc.) für diesen einen erheblichen Wert bzw. Geschäftswert darstellen und daher der Lizenzgeber bei einem Verstoß gegen die Bestimmungen dieser Geheimhaltungsregelung erheblicher Schaden entstehen kann. Jeder Lizenznehmer verpflichtet sich daher hiermit für sich selbst, Schäden, die dem Lizenzgeber aus einem vorsätzlichen oder fahrlässigen Verstoß gegen die in diesem Vertrag enthaltene Geheimhaltungsverpflichtung entstehen, zu ersetzen. Darüber hinaus hat der Lizenzgeber Anspruch auf Ersatz aller entstehenden Schäden aus dem Verstoß gegen diese Geheimhaltungsverpflichtung gegen den jeweiligen Lizenznehmer, wobei Schaden auch jedwede Folgeschäden, materielle und immaterielle Schäden sowie entgangenen Gewinn umfasst. Die in diesen AGB enthaltenen Haftungsbeschränkungen gelten nicht im Falle eines Verstoßes gegen die Geheimhaltungspflicht durch einen oder einen diesen Parteien zuzuordnenden Dritten.

(4) Jede nach dieser Vereinbarung durch eine der Parteien bekannt gegebene Information ist und bleibt das alleinige und ausschließliche geistige Eigentum dieser Partei einschließlich aller Verwertungs- und sonstiger Nutzungsrechte. Mit der Bekanntgabe von Informationen an die jeweils anderen Parteien werden keine Rechte – gleich welcher Art – weder ausdrücklich noch stillschweigend an diese übertragen.

(5) Vorstehende Geheimhaltungsverpflichtungserklärung gem. Ziff. 5 Abs. 1 gilt nicht für solche Informationen,

(a) welche bereits vor Vertragsschluss gemeinfrei oder veröffentlicht waren,

(b) welche die jeweilige Partei bereits zum Zeitpunkt der Überlassung ohne Verpflichtung zur Geheimhaltung besessen hat,

(c) welche aufgrund einer zusätzlichen schriftlichen Vereinbarung zur Weitergabe freigegeben wurden.

Die Geheimhaltungsverpflichtung gem. Ziff. 5 Abs. 1 gilt ferner nicht, wenn eine Partei gesetzlich, auf Grund eines rechtskräftigen Urteils eines deutschen Gerichtes oder behördlich verpflichtet ist, Informationen zu offenbaren, sofern eine solche Pflicht vor Offenlegung dem Vertraulichkeitsberechtigten schriftlich mitgeteilt wird. Vorstehende Vertraulichkeitserklärung gilt weiter nicht für Open Source Komponenten, soweit nach den jeweils gültigen Lizenzbestimmungen eine Offenlegung gestattet oder vorgeschrieben ist.

(6) Die Parteien werden durch geeignete Vorkehrungen, insbesondere durch geeignete Verträge mit Mitarbeitern und Beratern und sonstigen Dritten, derer sich die Parteien zur Erfüllung im Rahmen dieses Vertrages bedienen, sicherstellen, dass die vorstehenden Geheimhaltungsregelungen eingehalten werden.

(7) Die Parteien verpflichten sich, der jeweils anderen Partei unverzüglich nach Kenntniserlangung eines tatsächlichen oder drohenden unbefugten Gebrauchs oder Offenlegung von vertraulichen Informationen zu unterrichten und alle angemessenen Maßnahmen zu ergreifen, um einen solchen Gebrauch oder Offenlegung zu verhindern oder zu beenden.

6. Referenzkundennennung

(1) Mit Durchführung einer Bestellung oder nach einer ununterbrochenen Nutzungsdauer von mindestens sechs (6) Monaten von WORKSPACE.PM, unabhängig davon, ob diese kostenpflichtig oder im Rahmen einer Schulung kostenfrei zur Verfügung gestellt wurde, erteilt der Kunde dem Anbieter folgende Rechte:

- Das Recht, ihn als Referenzkunden zu benennen.
- Die ausdrückliche, unentgeltliche und widerrufbare Genehmigung zur Nutzung des Unternehmensnamens und -logos des Kunden für Referenzzwecke. Diese Genehmigung umfasst insbesondere das Recht, den Unternehmensnamen und das Logo auf der Webseite des Anbieters zu verwenden.

(2) Der Kunde versichert, zur Erteilung dieser Rechte zum Zeitpunkt der Bestellung befugt zu sein.

(3) Der Kunde kann dieser Referenznennung und Logonutzung jederzeit, also bereits zum Bestellvorgang formlos widersprechen. Eine Referenzkundennennung von Unternehmen aus besonders sensiblen oder besonders risikobehafteten Branchen (z.B. Rüstungsindustrie, Politik, Finanzwirtschaft) ist grundsätzlich ausgeschlossen.

(4) Diese Vereinbarung zur Referenzkundennennung und Logonutzung lässt sonstige Vertraulichkeitsverpflichtungen zwischen den Parteien unberührt. Der Anbieter verpflichtet sich, bei der Nutzung des Kundennamens und -logos die Reputation des Kunden zu wahren und diese niemals in einem negativen oder rufschädigenden Kontext zu verwenden.

7. Fristlose Kündigung

Jede Vertragspartei hat unbeschadet aller sonstigen Ansprüche (z. B. Schadensersatzansprüche) das Recht auf fristlose Kündigung des Lizenz- oder des Wartungs- und Supportvertrages durch schriftliche Mitteilung an die andere Partei, ohne dass die kündigende Partei eine weitere Mitteilung machen muss, falls die verletzende Partei eine Vertragsverletzung in einem solchen Maße begeht, dass es für die andere Partei nicht zumutbar ist, an den bestehenden Vereinbarungen festzuhalten. Dies gilt insbesondere, wenn:

eine abhilfefähige Verletzung nach den zwischen den Parteien bestehenden Vereinbarungen begangen und innerhalb von 45 Tagen, nachdem die verletzte Partei von der verletzenden Partei eine Mitteilung über diese Verletzung erhalten hat, keine Abhilfe geschaffen wurde;

eine nicht abhilfefähige Verletzung nach den zwischen den Parteien bestehenden Vereinbarungen begangen wurde; oder

im Verhalten ein sonstiger wichtiger Grund vorliegt.

8. Datenschutz

(1) Der Lizenznehmer stimmt hiermit ausdrücklich zu, dass der Lizenzgeber Daten und Informationen über den Lizenznehmer (wie z.B. Namen, Adresse und E-Mail-Adresse) erhebt, speichert, verwendet und verarbeitet. Es wird darauf hingewiesen, dass, soweit sich der Lizenzgeber zur Erfüllung seiner vertraglichen oder außervertraglichen Pflichten Dritter bedient, diesen die erhobenen Daten zur Erfüllung dieser Pflichten übertragen werden können. Beispiele für solche Dritte können sein: Reseller, Lieferunternehmen, Marketingbeauftragte sowie Finanzierungsunternehmen. Genauere, jeweils aktuelle Informationen zum Datenschutz werden durch den Lizenzgeber auf Anforderung zur Verfügung gestellt.

(2) Für die Einhaltung der Datenschutzvorschriften für die Inhalte, die der Lizenznehmer mit der Software bearbeitet, insbesondere bei Nutzung von SaaS, ist der Lizenznehmer allein verantwortlich. Der Lizenznehmer ist verpflichtet, den Lizenzgeber auf Besonderheiten des Datenschutzes im Zusammenhang mit seiner Softwarenutzung hinzuweisen und entsprechende Vorkehrungen zu treffen.

9. Force Majeure

(1) Leistungs-, Liefer- und Abnahmehindernisse infolge von Naturkatastrophen, Krieg, Arbeitskampfmaßnahmen, fehlender Rohstoffversorgung oder sonstiger Fälle höherer Gewalt im eigenen bzw. verbundenen Unternehmen oder Unternehmen, die mit der Ausführung Unteraufträgen betraut sind sowie durch Anordnungen von hoher Hand oder durch sonstige Umstände, die abzuwenden, nicht in der Macht der Vertragsparteien liegt bzw. die auch mit einem angemessenen technischen und wirtschaftlichen Aufwand nicht abgewendet oder ausgeglichen werden können, entbinden die Vertragspartner für die Dauer des Ereignisses von der Erfüllung der Vertragspflichten.

(2) Die an der Erfüllung des Vertrages gehinderte Partei ist verpflichtet, die andere Partei unverzüglich unter Darlegung der sie an der Erfüllung des Vertrages hindernden Umstände zu benachrichtigen; sie wird darüber hinaus alles in ihrer Macht stehende und wirtschaftlich Vertretbare unternehmen, um das Leistungs- bzw. Lieferungs Hindernis so schnell wie möglich zu beseitigen.

10. Übertragbarkeit

Der Lizenz- und/oder Wartungs- und Supportvertrag sowie Ansprüche hieraus dürfen ohne vorherige schriftliche Zustimmung der anderen Partei nicht ganz oder teilweise übertragen oder abgetreten werden, wobei jedoch die Zustimmung der anderen Partei nicht aus unbilligen Gründen verweigert werden darf. Vorbehaltlich des bisher Ausgeführten, verpflichten die Bestimmungen und Bedingungen ebenfalls die Rechtsnachfolger und Übernehmer der Parteien und sind auch für diese wirksam.

11. Schlussbestimmungen

(1) Änderungen und Ergänzungen des Lizenz- und/oder Wartungs- und Supportvertrages sowie dieser Bedingungen bedürfen der Textform.

(2) Die Nichteinhaltung einer Verpflichtung durch eine der Parteien darf nicht als Verzicht hierauf oder auf die Vereinbarung als Ganzes oder einer anderen Verpflichtung aus dem Lizenz- und/oder Wartungs- und Supportvertrages sowie dieser Bedingungen angesehen werden.

(3) Sollten einzelne Bestimmungen unwirksam sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen hierdurch nicht berührt. Anstelle der unwirksamen Bestimmung oder zur Ausfüllung eventueller Lücken soll eine wirksame und angemessene Regelung treten, die dem am nächsten kommt, was die Parteien nach der wirtschaftlichen Zielsetzung gewollt haben.

(4) Erfüllungsort sowie ausschließlicher Gerichtsstand ist Hannover, sofern jede Partei Unternehmer ist oder keinen allgemeinen Gerichtsstand in Deutschland hat.

(5) Auf das gesamte Vertragsverhältnis findet das Recht der Bundesrepublik Deutschland, mit Ausnahme des Kollisionsrechts sowie des UN-Kaufrechtes, Anwendung. Ein Verbraucher kann sich trotz der Rechtswahl auf die für ihn günstigeren Regelungen seines Heimatrechts berufen. Die Anwendung der „Convention for the international sale of goods“ (CISG) vom 11.04.1980 in ihrer jeweils gültigen Fassung ist ausgeschlossen.

Lizenzbedingungen

1. Geltungsbereich und Vertragsgegenstand

Diese Lizenzbedingungen regeln die rechtlichen Rahmenbedingungen für die Nutzung der workspace.pm Software (nachfolgend „Software“ genannt) der AMNAU GmbH (nachfolgend „Lizenzgeber“ genannt) durch den Kunden (nachfolgend „Lizenznehmer“ genannt). Sie gelten für alle Verträge zwischen dem Lizenzgeber und dem Lizenznehmer über die Nutzung der Software, unabhängig davon, ob diese als OnPrem-Lösung oder als Managed Cloud-Dienst bereitgestellt wird. Mit der Nutzung der Software erklärt sich der Lizenznehmer mit diesen Bedingungen einverstanden.

2. Definitionen

2.1 OnPrem (On Premises)

Bei der OnPrem-Lösung wird die Software auf der eigenen IT-Infrastruktur des Lizenznehmers installiert und betrieben. Der Lizenznehmer ist für die Bereitstellung und Wartung der erforderlichen Hardware sowie für die Installation und Aktualisierung der Software verantwortlich.

2.2 Managed Cloud

Bei der Managed Cloud-Lösung wird die Software vom Lizenzgeber in einer sicheren Cloud-Umgebung gehostet und dem Lizenznehmer über das Internet zur Verfügung gestellt. Der Lizenzgeber ist für die Bereitstellung, Wartung und Aktualisierung der Software sowie der zugrunde liegenden Infrastruktur verantwortlich.

2.3 Pilotumgebung

Die Pilotumgebung ist eine zeitlich begrenzte Bereitstellung der Software zur Evaluierung durch den Lizenznehmer. Sie kann für einen Zeitraum von 3 bis 12 Monaten eingerichtet werden, wobei die Dauer vom Lizenznehmer bestimmt wird.

2.4 Weitere relevante Begriffe

„Nutzer“ bezeichnet jede natürliche Person, die vom Lizenznehmer zur Nutzung der Software autorisiert wurde.

„Lizenzgebühr“ bezeichnet das vom Lizenznehmer zu entrichtende Entgelt für die Nutzung der Software. „Vertragslaufzeit“ bezieht sich auf den Zeitraum, für den dem Lizenznehmer das Recht zur Nutzung der Software eingeräumt wird.

3. Lizenzgewährung

3.1 OnPrem-Lizenzen

Für die OnPrem-Lösung gewährt der Lizenzgeber dem Lizenznehmer ein nicht-exklusives, nicht übertragbares und zeitlich begrenztes Recht zur Installation und Nutzung der Software auf der eigenen IT-Infrastruktur des Lizenznehmers. Die Anzahl der autorisierten Nutzer und die Dauer der Lizenz werden im Lizenzvertrag festgelegt.

3.2 Managed Cloud-Lizenz

Für die Managed Cloud-Lösung gewährt der Lizenzgeber dem Lizenznehmer ein nicht-exklusives, nicht übertragbares und zeitlich begrenztes Recht zum Zugriff auf die Software über das Internet und zu deren Nutzung. Die Anzahl der autorisierten

Nutzer und die Dauer der Lizenz werden im Lizenzvertrag festgelegt.

3.3 Pilotumgebung

Für die Pilotumgebung gewährt der Lizenzgeber dem Lizenznehmer ein nicht-exklusives, nicht übertragbares und zeitlich begrenztes Recht zur Evaluierung der Software. Sofern der Lizenznehmer den Vertrag nicht vor Ablauf der Pilotphase kündigt, geht der Vertrag in die Produktivumgebung über. Der Lizenzgeber informiert den Lizenznehmer hierüber vierzehn Tage vor Übergang via E-Mail. Die Berechnung erfolgt gemäß der vorher kommunizierten Preisliste und dem unterbreiteten Angebot.

4. Konditionen, Preise, Zahlungsbedingungen

4.1 Lizenzgebühren

Der Lizenznehmer verpflichtet sich zur Zahlung der im Lizenzvertrag vereinbarten Lizenzgebühren. Diese können je nach gewähltem Modell (OnPrem oder Managed Cloud) und Anzahl der Nutzer variieren. Alle Preise verstehen sich zuzüglich der gesetzlichen Mehrwertsteuer.

4.2 Zahlungsmodalitäten

Die Lizenzgebühren sind, sofern nicht anders vereinbart, monatlich zu entrichten. Rechnungen sind innerhalb von 14 Tagen nach Rechnungsstellung ohne Abzug zur Zahlung fällig. Bei Zahlungsverzug behält sich der Lizenzgeber das Recht vor, den Zugang zur Software zu sperren. Bei einem Zahlungsverzug von mehr als 45 Tagen ist der Lizenzgeber zu einer ausserordentlichen Kündigung berechtigt.

4.3 Preisänderungen

Der Lizenzgeber behält sich das Recht vor, die Lizenzgebühren mit einer Ankündigungsfrist von drei Monaten zum Ende der jeweiligen Vertragslaufzeit anzupassen. Im Falle einer Preiserhöhung hat der Lizenznehmer das Recht zur außerordentlichen Kündigung innerhalb von 30 Tagen nach Mitteilung der Preiserhöhung.

5. Lieferung und Bereitstellung

5.1 OnPrem-Lieferung

Bei der OnPrem-Lösung stellt der Lizenzgeber dem Lizenznehmer die Software zum Download bereit. Der Lizenznehmer erhält die erforderlichen Zugangsdaten und Installationsanweisungen per E-Mail. Die Bereitstellung erfolgt innerhalb von 5 Werktagen nach Eingang der Zahlung der Lizenzgebühr.

5.2 Managed Cloud-Bereitstellung

Bei der Managed Cloud-Lösung richtet der Lizenzgeber die Software in seiner Cloud-Umgebung ein und stellt dem Lizenznehmer die Zugangsdaten per E-Mail zur Verfügung. Die Bereitstellung erfolgt innerhalb von 2 Werktagen nach Eingang der Zahlung der Lizenzgebühr.

6. Nutzungsbedingungen

6.1 Allgemeine Nutzungsrechte und -beschränkungen

Der Lizenznehmer darf die Software nur für eigene Geschäftszwecke und nur im Rahmen der erworbenen Lizenzen nutzen. Eine Übertragung der Nutzungsrechte an Dritte, eine Unterlizenzierung oder eine Nutzung der Software über die vereinbarte Anzahl von Nutzern hinaus ist ohne vorherige schriftliche Zustimmung des Lizenzgebers nicht gestattet. Der Lizenznehmer ist nicht berechtigt, die Software zu kopieren, zu modifizieren, zu dekompileieren oder zurückzuentwickeln, es sei denn, dies ist gesetzlich ausdrücklich erlaubt.

6.2 OnPrem-spezifische Bedingungen

Bei der OnPrem-Lösung ist der Lizenznehmer für die Installation, den Betrieb und die Wartung der Software auf seiner eigenen IT-Infrastruktur verantwortlich. Er verpflichtet sich, die vom Lizenzgeber bereitgestellten Updates und Patches zeitnah zu installieren, um die Sicherheit und Funktionalität der Software zu gewährleisten. Der Lizenznehmer ist berechtigt, eine Sicherungskopie der Software zu erstellen, die ausschließlich zu Sicherungs- und Archivierungszwecken verwendet werden darf.

6.3 Managed Cloud-spezifische Bedingungen

Bei der Managed Cloud-Lösung ist der Lizenznehmer für die Sicherheit und Vertraulichkeit seiner Zugangsdaten verantwortlich. Er verpflichtet sich, diese Daten geheim zu halten und nicht an Dritte weiterzugeben. Der Lizenznehmer erkennt an, dass der Lizenzgeber berechtigt ist, regelmäßige Wartungsarbeiten und Updates durchzuführen, die zu vorübergehenden Unterbrechungen des Dienstes führen können. Der Lizenzgeber wird sich bemühen, solche Unterbrechungen auf ein Minimum zu beschränken und den Lizenznehmer im Voraus darüber zu informieren.

6.4 Open Source Komponenten

Die Software kann Open Source Komponenten enthalten, die anderen Lizenzbedingungen unterliegen. Der Lizenzgeber stellt dem Lizenznehmer auf Anfrage eine Liste dieser Komponenten und die entsprechenden Lizenzbedingungen zur Verfügung. Der Lizenznehmer verpflichtet sich, diese zusätzlichen Lizenzbedingungen einzuhalten.

7. Schutzrechte Dritter

7.1 Zusicherungen des Lizenzgebers

Der Lizenzgeber sichert zu, dass die Software frei von Rechten Dritter ist, die einer vertragsgemäßen Nutzung entgegenstehen. Er gewährleistet, dass er über alle erforderlichen Rechte verfügt, um dem Lizenznehmer die in diesem Vertrag eingeräumten Nutzungsrechte zu gewähren.

7.2 Freistellung und Rechtsverteidigung

Sollte die vertragsgemäße Nutzung der Software durch den Lizenznehmer die Rechte Dritter verletzen, wird der Lizenzgeber den Lizenznehmer von allen daraus resultierenden Ansprüchen Dritter freistellen. Der Lizenzgeber übernimmt die Rechtsverteidigung auf eigene Kosten und stellt den Lizenznehmer von allen damit verbundenen Kosten frei, vorausgesetzt, der

Lizenznehmer informiert den Lizenzgeber unverzüglich schriftlich über geltend gemachte Ansprüche und überlässt dem Lizenzgeber die Kontrolle über die Rechtsverteidigung und Vergleichsverhandlungen.

8. Laufzeit und Kündigung

8.1 Vertragsbeginn

Der Vertrag tritt mit Unterzeichnung des Lizenzvertrages oder, falls früher, mit der ersten Bereitstellung der Software in Kraft.

8.2 Pilotumgebung

Die Laufzeit der Pilotumgebung beträgt 3 bis 12 Monate, abhängig von der Auswahl des Lizenznehmers. Die Pilotumgebung kann vom Lizenznehmer jederzeit während der Pilotphase gekündigt werden. Der Lizenznehmer nimmt vor Ende der Pilotphase ggf. notwendige Sicherungen vor. Der Lizenzgeber ist verpflichtet, alle Daten und sämtliche Kopien des Lizenznehmers zu löschen, sofern sich der Lizenznehmer nicht innerhalb von 30 Tagen nach Ablauf der Pilotumgebung für eine Produktivumgebung entscheidet. Dies beinhaltet ebenfalls bestellte Domains.

8.3 Laufzeit

Die Mindestvertragslaufzeit beträgt, sowohl für die OnPrem- als auch für die Managed Cloud-Lösung, 12 Monate ab Vertragsbeginn. Nach Ablauf der Mindestvertragslaufzeit verlängert sich der Vertrag automatisch um jeweils weitere 12 Monate, sofern er nicht fristgerecht gekündigt wird.

8.4 Ordentliche Kündigung

Der Vertrag kann von beiden Parteien mit einer Frist von 3 Monaten zum Ende der jeweiligen Vertragslaufzeit schriftlich gekündigt werden. Bei der Managed Cloud-Lösung endet mit der Kündigung auch das Recht zur Nutzung der Software. Bei der OnPrem-Lösung ist der Lizenznehmer verpflichtet, die Software nach Vertragsende von allen Systemen zu entfernen und sämtliche Kopien zu löschen.

8.5 Außerordentliche Kündigung

Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn eine Partei gegen wesentliche Vertragspflichten verstößt und den Verstoß trotz Abmahnung nicht innerhalb einer angemessenen Frist behebt. Im Falle einer außerordentlichen Kündigung durch den Lizenzgeber aufgrund eines Verstoßes des Lizenznehmers hat dieser keinen Anspruch auf Rückerstattung bereits gezahlter Lizenzgebühren.

9. Anpassungen und Beratungsleistungen

9.1 Beauftragte Anpassungen

Individuelle Anpassungen oder Erweiterungen der Software können zwischen den Parteien gesondert vereinbart werden. Solche Anpassungen unterliegen separaten Vereinbarungen und können zusätzliche Kosten verursachen. Der Lizenzgeber behält sich das Recht vor, Anpassungswünsche abzulehnen, wenn diese technisch nicht umsetzbar sind oder den Kern der Software beeinträchtigen würden.

9.2 Abnahmeprozess

Nach Fertigstellung explizit beauftragter Anpassungen oder Beratungsleistungen wird der Lizenzgeber den Lizenznehmer zur Abnahme auffordern. Der Lizenznehmer ist verpflichtet, die Leistungen innerhalb von 14 Tagen zu prüfen und abzunehmen, sofern keine wesentlichen Mängel vorliegen. Erfolgt innerhalb dieser Frist keine Rückmeldung des Lizenznehmers, gelten die Leistungen als abgenommen. Bei Managed Cloud-Lösungen gelten Anpassungen als abgenommen, wenn sie 30 Tage lang produktiv genutzt wurden, ohne dass wesentliche Mängel gemeldet wurden.

10. Datenschutz und Vertraulichkeit

10.1 Datenschutz

Der Lizenzgeber verpflichtet sich, die geltenden Datenschutzgesetze einzuhalten. Bei der Verarbeitung personenbezogener Daten im Auftrag des Lizenznehmers (insbesondere bei der Managed Cloud-Lösung) wird eine separate Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO geschlossen. Der Lizenznehmer bleibt für die Rechtmäßigkeit der Datenverarbeitung verantwortlich und holt erforderliche Einwilligungen ein.

10.2 Vertraulichkeit

Beide Parteien verpflichten sich, alle im Rahmen des Vertragsverhältnisses erlangten vertraulichen Informationen, Geschäfts- und Betriebsgeheimnisse der jeweils anderen Partei streng vertraulich zu behandeln und nur für Zwecke der Vertragserfüllung zu verwenden. Diese Verpflichtung besteht auch nach Beendigung des Vertragsverhältnisses fort. Ausgenommen hiervon sind Informationen, die öffentlich bekannt sind oder ohne Verschulden der empfangenden Partei öffentlich bekannt werden.

11. Haftungsbeschränkungen

11.1 Unbeschränkte Haftung

Der Lizenzgeber haftet unbeschränkt für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer vorsätzlichen oder fahrlässigen Pflichtverletzung des Lizenzgebers, seiner gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen, sowie für Schäden, die auf Vorsatz oder grober Fahrlässigkeit des Lizenzgebers, seiner gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen.

11.2 Beschränkte Haftung

Für leicht fahrlässig verursachte Sach- und Vermögensschäden haftet der Lizenzgeber nur bei Verletzung wesentlicher Vertragspflichten (Kardinalpflichten), jedoch der Höhe nach beschränkt auf die bei Vertragsschluss vorhersehbaren und vertragstypischen Schäden. Wesentliche Vertragspflichten sind solche, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Lizenznehmer regelmäßig vertrauen darf. Die Haftung für mittelbare und unvorhersehbare Schäden, Produktions- und Nutzungsausfall, entgangenen Gewinn, ausgebliebene Einsparungen und Vermögensschäden wegen Ansprüchen Dritter ist im Falle leichter Fahrlässigkeit ausgeschlossen.

12. Schlussbestimmungen

12.1 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Lizenzbedingungen unwirksam oder undurchführbar sein oder werden, bleibt davon die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien verpflichten sich, unwirksame oder undurchführbare Bestimmungen durch neue Bestimmungen zu ersetzen, die dem in den unwirksamen oder undurchführbaren Bestimmungen enthaltenen wirtschaftlichen Regelungsgehalt in rechtlich zulässiger Weise gerecht werden.

12.2 Anwendbares Recht

Für diese Lizenzbedingungen und die gesamten Rechtsbeziehungen zwischen Lizenzgeber und Lizenznehmer gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts (CISG).

12.3 Gerichtsstand

Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesen Lizenzbedingungen ist, soweit gesetzlich zulässig, der Sitz des Lizenzgebers.

12.4 Änderungen der Lizenzbedingungen

Der Lizenzgeber behält sich das Recht vor, diese Lizenzbedingungen zu ändern, soweit dies aus triftigen Gründen, insbesondere aufgrund einer geänderten Rechtslage oder höchstrichterlichen Rechtsprechung, technischer Änderungen oder Weiterentwicklungen, neuer organisatorischer Anforderungen des Massenverkehrs, Regelungslücken in den Lizenzbedingungen, Veränderung der Marktgegebenheiten oder anderen gleichwertigen Gründen erforderlich ist und den Lizenznehmer nicht unangemessen benachteiligt. Änderungen der Lizenzbedingungen werden dem Lizenznehmer mindestens sechs Wochen vor ihrem Inkrafttreten schriftlich oder per E-Mail mitgeteilt. Die Änderungen werden wirksam, wenn der Lizenznehmer nicht innerhalb dieser Frist von sechs Wochen (beginnend mit dem Tag der Zustellung der Mitteilung) schriftlich oder per E-Mail widerspricht und der Lizenzgeber den Lizenznehmer auf diese Rechtsfolge in der Änderungsmitteilung hingewiesen hat.

Servicelevel und Support-Vertrag

1. Einleitung und Vertragsparteien

Dieses Service Level und Support Agreement (nachfolgend „Vereinbarung“) wird geschlossen zwischen der AMNAU GmbH, Kronenstraße 13, 30161 Hannover (nachfolgend „Anbieter“) und dem Kunden (nachfolgend „Kunde“). Anbieter und Kunde werden einzeln als „Partei“ und gemeinsam als „Parteien“ bezeichnet. Diese Vereinbarung regelt die Bedingungen für die Bereitstellung von Dienstleistungen, einschließlich Support und Wartung, im Zusammenhang mit der Software „workspace.pm“ (nachfolgend „Software“). Die Allgemeinen Geschäftsbedingungen, Lizenzbedingungen und Datenschutzerklärung bleiben hiervon unberührt.

2. Definitionen

- Betriebszeit bezeichnet die Zeit, in der die Software verfügbar und funktionsfähig ist.
- Incident bezeichnet jede Unterbrechung oder Qualitätsminderung des Dienstes, die vom Kunden gemeldet oder vom Anbieter festgestellt wird.
- Reaktionszeit bezeichnet die Zeit zwischen dem Eingang einer Supportanfrage und der ersten Reaktion des Anbieters.
- Lösungszeit bezeichnet die Zeit zwischen dem Eingang einer Supportanfrage und der Bereitstellung einer Lösung oder eines Workarounds.
- Service Credits bezeichnet Gutschriften, die dem Kunden bei Nichteinhaltung der vereinbarten Service Levels gewährt werden.

3. Vertragsgegenstand und Geltungsbereich

Gegenstand dieser Vereinbarung ist die Festlegung von Service Levels und Supportbedingungen für die Nutzung der Software durch den Kunden. Diese Vereinbarung gilt für alle Versionen und Bereitstellungsmodelle der Software, einschließlich On-Premises-Installationen und Cloud-Dienste, sofern nicht ausdrücklich anders angegeben. Sie regelt die Qualität der zu erbringenden Dienstleistungen, die Verantwortlichkeiten beider Parteien sowie die Verfahren zur Problemlösung und Eskalation.

4. Leistungsbeschreibung

4.1 Softwarenutzung

Der Anbieter stellt dem Kunden die Software „workspace.pm“ zur Nutzung bereit. Die Software dient dem Multiprojekt- und Portfoliomanagement und bietet eine flexible, sichere Arbeitsumgebung für Unternehmen und Organisationen. Je nach gewähltem Modell wird die Software entweder als On-Premises-Lösung auf der IT-Infrastruktur des Kunden installiert oder als Managed Cloud-Dienst über das Internet zur Verfügung gestellt.

4.2 Supportleistungen

Der Anbieter bietet Support für die Software, um eine reibungslose Nutzung zu gewährleisten. Dies umfasst technische Unterstützung bei Problemen, Hilfe bei der Konfiguration und Beantwortung von Fragen zur Funktionalität. Der Support wird über definierte Kanäle (E-Mail, Telefon, Ticketsystem) während der festgelegten Supportzeiten bereitgestellt. Die Details zu

Reaktionszeiten und Problemlösungsprozessen werden in den folgenden Abschnitten spezifiziert.

4.3 Wartung und Updates

Der Anbieter führt regelmäßige Wartungsarbeiten durch, um die Leistungsfähigkeit und Sicherheit der Software zu gewährleisten. Dies beinhaltet die Bereitstellung von Updates, Fehlerbehebungen und Sicherheitspatches. Bei der Managed Cloud-Lösung werden diese Aktualisierungen vom Anbieter durchgeführt, während bei der On-Premises-Lösung der Kunde für die Installation verantwortlich ist, wobei der Anbieter Unterstützung und Anleitung bietet.

5. Service Levels

5.1 Verfügbarkeit des Dienstes

Für die Managed Cloud-Lösung garantiert der Anbieter eine Verfügbarkeit von 99,7% im Jahresdurchschnitt, gemessen über einen Zeitraum von 12 Monaten. Die Verfügbarkeit wird wie folgt berechnet: $(\text{Gesamtzeit} - \text{Ausfallzeit}) / \text{Gesamtzeit} \times 100$. Geplante Wartungsarbeiten, die im Voraus angekündigt wurden, werden nicht als Ausfallzeit gewertet. Für die On-Premises-Lösung liegt die Verantwortung für die Verfügbarkeit beim Kunden, wobei der Anbieter Unterstützung bei der Optimierung der Systemkonfiguration bietet.

5.2 Performance-Metriken

Der Anbieter verpflichtet sich, die folgenden Performance-Metriken für die Managed Cloud-Lösung einzuhalten:

- Durchschnittliche Antwortzeit für Standardanfragen: < 2 Sekunden
- Durchschnittliche Antwortzeit für komplexe Datenbankabfragen: < 5 Sekunden
- Maximale Dauer für Batch-Verarbeitungen: < 30 Minuten

Für die On-Premises-Lösung bietet der Anbieter Empfehlungen zur Optimierung der Performance, die finale Performance hängt jedoch von der IT-Infrastruktur des Kunden ab.

5.3 Wartungsfenster

Für die Managed Cloud-Lösung führt der Anbieter regelmäßige Wartungsarbeiten in einem festgelegten wöchentlichen Zeitfenster durch. Dieses Wartungsfenster findet jeden Mittwoch von 15:00 bis 16:00 Uhr (MEZ/MESZ) statt. Während dieses Zeitraums können Einschränkungen in der Verfügbarkeit oder Leistung des Systems auftreten. Eine gesonderte Benachrichtigung über diese regulären Wartungsarbeiten erfolgt nicht, da es sich um ein feststehendes, wiederkehrendes Zeitfenster handelt.

Kritische (Sicherheits-)Updates werden vom Anbieter unverzüglich und ohne vorherige Ankündigung eingespielt, um die Sicherheit des Systems zu gewährleisten. Dies kann auch außerhalb des regulären Wartungsfensters geschehen.

Die Gesamtdauer aller Wartungsarbeiten, einschließlich des regulären Wartungsfensters und etwaiger kritischer Sicherheitsupdates, wird zwei Stunden pro Monat nicht überschreiten. Der Anbieter bemüht sich, die Auswirkungen auf den Betrieb des Kunden so gering wie möglich zu halten.

Für die On-Premises-Lösung liegt die Planung und Durchführung von Wartungsarbeiten in der Verantwortung des Kunden. Der Anbieter stellt jedoch regelmäßig Updates und Sicherheitspatches zur Verfügung und empfiehlt deren zeitnahe Installation.

6. Supportbedingungen

6.1 Supportkanäle

Der Anbieter stellt folgende Supportkanäle zur Verfügung:

E-Mail-Support: support@workspace.pm

Telefon-Support: +49 (0)511 8765050

Online-Ticketsystem: <https://workspace.pm/support>

Anfragen für technischen Support bei On-Premises-Lösungen müssen explizit als solche gekennzeichnet werden und werden nach den im Abschnitt ‚Kosten und Gebühren‘ aufgeführten Sätzen berechnet.

Alle Supportanfragen werden über diese Kanäle entgegengenommen und im Ticketsystem erfasst. Der Kunde erhält für jede Anfrage eine eindeutige Ticket-Nummer zur Nachverfolgung. Für kritische Probleme wird die Nutzung des Telefon-Supports empfohlen.

6.2 Supportzeiten

Der reguläre Support steht an Werktagen (Montag bis Freitag, ausgenommen gesetzliche Feiertage in Niedersachsen) von 9:00 Uhr bis 17:00 Uhr MEZ/MESZ zur Verfügung. Außerhalb dieser Zeiten wird ein Bereitschaftsdienst für kritische Probleme (Priorität 1) angeboten. Der Bereitschaftsdienst ist täglich von 17:00 Uhr bis 22:00 Uhr sowie an Wochenenden und Feiertagen von 9:00 Uhr bis 17:00 Uhr erreichbar. Die Nutzung des Bereitschaftsdienstes kann zusätzliche Kosten verursachen, die im Abschnitt „Kosten und Gebühren“ spezifiziert sind.

6.3 Priorisierung von Supportanfragen

Supportanfragen werden nach folgenden Prioritätsstufen klassifiziert:

Priorität 1 (Kritisch): Kompletter Systemausfall oder schwerwiegende Störung, die den Geschäftsbetrieb erheblich beeinträchtigt, alle Störungen, welche die Sicherheit beeinträchtigen.

Priorität 2 (Hoch): Wesentliche Funktionen sind beeinträchtigt, aber ein Workaround ist verfügbar.

Priorität 3 (Mittel): Nicht-kritische Funktionen sind beeinträchtigt oder funktionieren nicht wie erwartet.

Priorität 4 (Niedrig): Allgemeine Fragen, Verbesserungsvorschläge oder kosmetische Probleme.

Die initiale Priorisierung erfolgt durch den Kunden bei der Erstellung des Tickets, kann jedoch vom Support-Team des Anbieters angepasst werden, wenn dies als angemessen erachtet wird. Der Kunde wird über jede Änderung der Priorität im Kundenportal informiert.

6.4 Unterscheidung zwischen regulärem Support und technischem Support

Der Anbieter unterscheidet zwischen zwei Arten von Support:

Regulärer Support: Dieser umfasst die Unterstützung bei der Nutzung von workspace, einschließlich Fragen zur Funktionalität, Hilfe bei der Konfiguration und Behebung von softwarebezogenen Problemen. Dieser Support ist in den Lizenzgebühren enthalten.

Technischer Support für On-Premises-Lösungen: Dieser bezieht sich auf Unterstützung, die über den regulären Support hinausgeht und spezifisch für die Installation, Wartung und Fehlerbehebung der On-Premises-Infrastruktur erforderlich ist. Dies kann Hilfe bei Serverproblemen, Datenbankoptimierung, Netzwerkkonfiguration oder anderen infrastrukturbezogenen Themen umfassen. Dieser technische Support ist kostenpflichtig und wird separat berechnet.

7. Incident Management

7.1 Störungsklassifizierung

Incidents werden entsprechend ihrer Auswirkung auf den Geschäftsbetrieb des Kunden klassifiziert:

Klasse A (Kritisch): Vollständiger Ausfall des Systems oder einer Kernfunktionalität ohne Workaround oder Störungen, welche die Sicherheit beeinträchtigen.

Klasse B (Schwerwiegend): Erhebliche Beeinträchtigung wichtiger Funktionen, Workaround verfügbar.

Klasse C (Bedeutend): Beeinträchtigung einzelner Funktionen, die die Arbeitsabläufe stören, aber nicht verhindern.

Klasse D (Gering): Minimale Auswirkung auf den Betrieb, kosmetische Probleme oder Fragen zur Bedienung. Die Klassifizierung erfolgt in Abstimmung zwischen Kunde und Anbieter und bestimmt die Dringlichkeit der Bearbeitung.

7.2 Reaktionszeiten

Der Anbieter verpflichtet sich zu folgenden maximalen Reaktionszeiten:

- Klasse A: 1 Stunde (während der Supportzeiten)
- Klasse B: 4 Stunden (während der Supportzeiten)
- Klasse C: 1 Arbeitstag
- Klasse D: 2 Arbeitstage

Die Reaktionszeit beginnt mit dem Eingang der Störungsmeldung und endet mit der ersten qualifizierten Rückmeldung des Supports an den Kunden. Bei der On-Premises-Lösung können sich die Reaktionszeiten verlängern, wenn der Zugriff auf das System des Kunden erforderlich ist.

7.3 Lösungszeiten

Der Anbieter strebt folgende Lösungszeiten an:

- Klasse A: 4 Stunden für einen Workaround, 24 Stunden für eine vollständige Lösung
- Klasse B: 8 Stunden für einen Workaround, 3 Arbeitstage für eine vollständige Lösung

- Klasse C: 7 Arbeitstage oder mit dem nächsten geplanten Update
- Klasse D: 21 Arbeitstage oder mit dem nächsten geplanten Update

Diese Zeiten gelten ab dem Zeitpunkt der ersten Reaktion. Bei komplexen Problemen oder solchen, die von Drittanbietern abhängen, können längere Lösungszeiten erforderlich sein. In solchen Fällen wird der Kunde regelmäßig über den Fortschritt informiert.

7.4 Eskalationsverfahren

Sollte ein Incident nicht innerhalb der angestrebten Lösungszeit behoben werden können oder ist der Kunde mit der Bearbeitung unzufrieden, steht folgendes Eskalationsverfahren zur Verfügung:

- Stufe: Eskalation an den Teamleiter Support (innerhalb von 4 Stunden nach Überschreitung der Lösungszeit)
- 2. Stufe: Eskalation an den technischen Direktor (innerhalb von 24 Stunden nach Stufe 1)
- 3. Stufe: Eskalation an die Geschäftsführung (innerhalb von 48 Stunden nach Stufe 2)

Der Kunde kann eine Eskalation durch Kontaktaufnahme über die bereitgestellten Supportkanäle initiieren. Der Anbieter verpflichtet sich, auf jede Eskalation innerhalb von 2 Stunden während der regulären Supportzeiten zu reagieren.

8. Problemlösungsprozess

Der Anbieter folgt einem strukturierten Problemlösungsprozess:

- Erfassung: Detaillierte Aufnahme der Problembeschreibung und aller relevanten Informationen.
- 2. Analyse: Untersuchung der Ursache durch qualifizierte Supportmitarbeiter.
- 3. Lösung: Entwicklung und Implementierung einer Lösung oder eines Workarounds.
- 4. Test: Überprüfung der Lösung in Zusammenarbeit mit dem Kunden.
- 5. Abschluss: Dokumentation der Lösung und Bestätigung durch den Kunden.

Bei komplexen Problemen kann der Anbieter zusätzliche Informationen oder Zugriff auf das System des Kunden anfordern. Der Kunde wird über alle wesentlichen Schritte im Problemlösungsprozess informiert.

9. Service Credits und Entschädigungen

Bei Nichteinhaltung der vereinbarten Service Levels gewährt der Anbieter Service Credits:

- Verfügbarkeit: 5% der monatlichen Gebühr für je 0,1% Unterschreitung der zugesicherten Verfügbarkeit.
- Reaktionszeiten: 2% der monatlichen Gebühr pro Stunde
- Überschreitung bei Klasse A Incidents: 5% der monatlichen Gebühr pro Stunde
- Lösungszeiten: 3% der monatlichen Gebühr pro Tag Überschreitung bei Klasse A und B Incidents.

Service Credits werden automatisch berechnet und in der nächsten Rechnung gutgeschrieben. Die maximale Höhe der Service

Credits ist auf 50% der monatlichen Gebühr begrenzt. Service Credits gelten nicht für die On-Premises-Lösung, es sei denn, die Nichteinhaltung ist direkt auf einen Fehler in der Software zurückzuführen.

10. Mitwirkungspflichten des Kunden

Der Kunde verpflichtet sich zur Mitwirkung bei der Erbringung der Supportleistungen:

- Bereitstellung vollständiger und genauer Informationen bei Supportanfragen
- Durchführung grundlegender Fehlerbehebungsschritte auf Anweisung des Supports
- Gewährung des erforderlichen Zugriffs auf Systeme und Daten zur Problemlösung
- Benennung qualifizierter Ansprechpartner für die Kommunikation mit dem Support
- Zeitnahe Installation von bereitgestellten Updates und Patches (bei On-Premises-Lösungen)
- Einhaltung der empfohlenen Systemvoraussetzungen und Best Practices
- Bei On-Premises-Lösungen: Bereitstellung von Fernzugriff, Logs und Datenbankzugang auf Anfrage des Supports zur effizienten Problemlösung.

Bei Nichteinhaltung dieser Mitwirkungspflichten behält sich der Anbieter das Recht vor, vereinbarte Service Levels auszusetzen.

11. Remote-Support und Zugriff auf Kundensysteme

Für eine effiziente Problemlösung kann ein Remote-Zugriff auf die Systeme des Kunden erforderlich sein. Dieser erfolgt nur nach vorheriger Zustimmung des Kunden und unter Einhaltung strenger Sicherheitsmaßnahmen:

- Nutzung verschlüsselter Verbindungen (SSH mit Public Key-Verfahren)
- Temporäre, zweckgebundene Zugriffsrechte
- Protokollierung aller Zugriffe und Aktionen
- Option für den Kunden, den Zugriff jederzeit zu beenden

Der Kunde stellt sicher, dass die notwendigen technischen Voraussetzungen für den Remote-Zugriff gegeben sind. Alle während des Remote-Zugriffs erlangten Informationen werden vertraulich behandelt.

12. Schulungen und Dokumentation

Der Anbieter stellt umfassende Schulungs- und Dokumentationmaterialien zur Verfügung:

- Video-Tutorials: Kurze, themenbezogene Anleitungsvideos in der Software integriert
- Wissensdatenbank: Sammlung von FAQs, Troubleshooting-Guides und Best Practices
- Individuelle Schulungen: Auf Anfrage und gegen zusätzliche Gebühr

Der Kunde verpflichtet sich, seine Mitarbeiter angemessen zu schulen, um eine effiziente Nutzung der Software zu gewährleisten. Der Anbieter empfiehlt, dass mindestens ein Mitarbeiter pro Abteilung eine vertiefte Schulung absolviert.

13. Lizenz- und Versionssupport

Der Anbieter unterstützt ausschließlich die aktuelle Version der Software workspace. Die Software wird kontinuierlich weiterentwickelt und verbessert, ohne feste Veröffentlichungstermine für neue Versionen.

Für Nutzer der Cloud-Lösung werden alle Verbesserungen automatisch und sofort bereitgestellt. So arbeiten alle Kunden immer mit der neuesten Version.

Kunden der On-Premises-Lösung erhalten zeitgleich mit den Managed-Cloud-Instanzen diese Aktualisierungen. Es liegt in ihrer Verantwortung, diese zeitnah zu installieren, um von den neuesten Funktionen und Sicherheitsverbesserungen zu profitieren.

Der Support umfasst:

- Laufende Fehlerbehebungen und Sicherheitsupdates
- Neue Funktionen und Verbesserungen
- Hilfe bei technischen Fragen zur aktuellen Version
- Unterstützung bei der Aktualisierung von On-Premises-Installationen

Der Anbieter kann die Unterstützung für veraltete On-Premises-Installationen einschränken und wird in solchen Fällen ein Update empfehlen. Durch dieses Modell stellt der Anbieter sicher, dass alle Kunden von den neuesten Entwicklungen profitieren, unabhängig davon, ob sie die Cloud- oder On-Premises-Lösung nutzen.

14. Kosten und Gebühren

Die Supportleistungen sind im Rahmen der regulären Lizenzgebühren wie folgt abgedeckt:

- Standard-Support während der regulären Supportzeiten
- Zugang zur Online-Dokumentation und Wissensdatenbank
- Regelmäßige Updates und Sicherheitspatches

Technischer Support für On-Premises-Lösungen (gilt nur für Supportleistungen, die über den regulären workspace-Support hinausgehen und sich auf die kundenspezifische Infrastruktur beziehen)

- 40 € pro angefangene 15 Minuten / 1.280 € pro Personentag
- Abrechnung erfolgt in 15-Minuten-Intervallen
- Zeiterfassung beginnt mit der ersten Supporthandlung und endet mit Abschluss der Supportleistung
- Vorbereitungs- und Nachbereitungszeiten werden mit eingerechnet
- Eine detaillierte Aufstellung der Supportleistungen wird mit der Rechnung bereitgestellt

Der reguläre Support für die workspace-Software selbst bleibt von diesen Gebühren unberührt und ist weiterhin in den Lizenzgebühren enthalten.

Zusätzliche Support-Entgelte fallen an für:

- Support außerhalb der regulären Zeiten: 40 € / 15 Min (Abrechnung in 15-Minuten-Intervallen)
- Individuelle Schulungen: 1.280 € / Tag pro Consultant
- Vor-Ort-Einsätze: 1.480 € / Tag zzgl. Reisekosten

- Erweiterte technische Unterstützung: Nach individuellem Angebot

Für On-Premises-Kunden fallen die Supportgebühren zusätzlich zu den regulären Lizenzgebühren an und werden monatlich in Rechnung gestellt. Alle Preise verstehen sich zuzüglich der gesetzlichen Mehrwertsteuer. Der Anbieter behält sich vor, die Preise jährlich anzupassen.

Backup- und Wiederherstellungskonzept – Managed Hosting –

1. Zielsetzung

Die Daten, die Sie uns im Rahmen der Nutzung unserer Projekt- und Portfoliomanagement-Software WORKSPACE.PM anvertrauen, stellen für Ihre Organisation einen unschätzbaren Wert dar. Sie sind die Grundlage für strategische Entscheidungen, operative Planung und die erfolgreiche Abwicklung Ihrer Projekte. Das Bewusstsein für diese immense Verantwortung prägt unser gesamtes Handeln als Ihr Dienstleister. Die Gewährleistung der Vertraulichkeit, Integrität und vor allem der ständigen Verfügbarkeit dieser Daten ist daher der zentrale Pfeiler unseres Serviceversprechens. Mit diesem Dokument möchten wir Ihnen in vollständiger Transparenz darlegen, welche umfassenden und durchdachten Maßnahmen wir ergreifen, um Ihre Daten vor Verlust, Beschädigung oder unbefugtem Zugriff zu schützen und ihre schnelle Wiederherstellbarkeit in jedem denkbaren Szenario zu sichern.

Dieses Datensicherungskonzept dient als informative Grundlage und beschreibt detailliert die Architektur, die Prozesse und die Technologien, die wir für die Sicherung Ihrer WORKSPACE.PM-Instanz im Rahmen unseres Managed-Hosting-Angebots implementiert haben. Es soll Ihnen das Vertrauen und die Gewissheit geben, dass Ihre geschäftskritischen Informationen bei uns in sicheren Händen sind. Wir erläutern nicht nur, welche Sicherungen wir durchführen, sondern auch die strategischen Überlegungen, die dieser Konzeption zugrunde liegen. Unser Ziel ist es, Ihnen eine verständliche und nachvollziehbare Übersicht über ein robustes System zu geben, das auf Redundanz, geografischer Trennung und mehrstufigen Sicherheitsmechanismen basiert, um den höchsten Anforderungen an die Datensicherheit, wie sie insbesondere von kleinen und mittleren Unternehmen sowie dem öffentlichen Dienst gestellt werden, gerecht zu werden.

2. Die technologische Grundlage: Unsere Hosting-Infrastruktur

Die Leistungsfähigkeit und Sicherheit Ihrer WORKSPACE.PM-Anwendung beginnt mit der Qualität der zugrundeliegenden Infrastruktur. Aus diesem Grund haben wir uns für das Hosting Ihrer Instanz in den hochsicheren Rechenzentren unseres Partners Hetzner Online GmbH entschieden, einem der führenden und renommiertesten Anbieter in Europa mit Sitz in Deutschland. Diese Wahl stellt sicher, dass Ihre Daten physisch und digital nach den höchsten Industriestandards geschützt sind und dem strengen deutschen Datenschutzrecht unterliegen. Die Rechenzentren von Hetzner sind nach der international anerkannten Norm für Informationssicherheit, ISO/IEC 27001, zertifiziert.

Diese Zertifizierung bürgt für ein umfassendes Sicherheitsmanagement, das alle relevanten Bereiche abdeckt. Dazu gehört eine strikte, mehrstufige Zutrittskontrolle, die gewährleistet, dass ausschließlich autorisiertes Fachpersonal physischen Zugang zu den Server-Systemen erhält. Eine lückenlose Videoüberwachung der sicherheitskritischen Bereiche sowie moderne Einbruchmeldesysteme ergänzen diesen Schutz. Darüber hinaus ist die gesamte Infrastruktur durch fortschrittliche

Brandfrüherkennungs- und automatische Löschsysteme gegen Feuer geschützt. Um eine unterbrechungsfreie Verfügbarkeit zu gewährleisten, sind die Rechenzentren mit einer redundanten Stromversorgung ausgestattet, die sowohl auf eine Anbindung an mehrere Stromnetze als auch auf leistungsfähige unterbrechungsfreie Stromversorgungen (USV) und Notstromdieselaggregate zurückgreift. Eine redundante Netzwerkanbindung an die wichtigsten Internet-Knotenpunkte sichert eine schnelle und ausfallsichere Konnektivität.

Ihre WORKSPACE.PM-Software wird in einer professionell verwalteten, virtuellen Serverumgebung betrieben. Dieser "Managed Hosting"-Ansatz ermöglicht es uns, die Systemressourcen optimal zu steuern, die Leistung kontinuierlich zu überwachen und Sicherheitsupdates zeitnah einzuspielen, ohne den laufenden Betrieb zu beeinträchtigen. Diese gekapselte virtuelle Umgebung bildet die technologische Basis für die erste Stufe unseres Sicherungskonzepts: die Erstellung von kompletten System-Snapshots.

3. Unsere mehrstufige Datensicherungsstrategie

Ein wirksames Datensicherungskonzept darf sich niemals auf eine einzige Maßnahme verlassen. Ein einzelner Fehlerpunkt, sei er technischer oder menschlicher Natur, könnte sonst katastrophale Folgen haben. Aus diesem Grund basiert unsere Strategie auf einem mehrstufigen Ansatz, der Redundanz und Diversität in den Mittelpunkt stellt. Dieses Vorgehen orientiert sich an der in der IT-Sicherheitsbranche als Goldstandard etablierten "3-2-1-Regel". Diese Regel besagt, dass zu jeder Zeit mindestens drei Kopien der Daten existieren sollten, diese auf zwei unterschiedlichen Medientypen gespeichert werden und eine dieser Kopien an einem externen, geografisch getrennten Ort aufbewahrt wird. Unser Konzept erfüllt und übertrifft diese Anforderung, indem es drei klar definierte Sicherungsebenen mit unterschiedlichen Zielen, Frequenzen und Aufbewahrungsfristen kombiniert.

Stufe 1: Kurzfristige operative Sicherung auf Hypervisor-Ebene

Die erste und unmittelbarste Ebene unserer Datensicherung dient der schnellen operativen Wiederherstellung. Sie ist darauf ausgelegt, die Auswirkungen von kleineren, alltäglichen Zwischenfällen, wie beispielsweise dem versehentlichen Löschen von Daten durch einen Benutzer oder einer fehlerhaften Konfigurationsänderung, minimal zu halten. Um dies zu gewährleisten, führt unser Hosting-Provider Hetzner vollautomatisch eine tägliche Sicherung des gesamten virtuellen Servers durch. Diese Sicherung erfolgt in Form eines sogenannten Snapshots. Ein Snapshot ist ein komplettes, konsistentes Abbild des Servers zu einem exakten Zeitpunkt, das sowohl die Anwendungsdateien von WORKSPACE.PM als auch die gesamte Datenbank und die Systemkonfiguration umfasst.

Dieser Sicherungsvorgang wird bewusst in ein Zeitfenster mit erfahrungsgemäß sehr geringer Nutzeraktivität gelegt, typischerweise um etwa 4 Uhr nachts. Dadurch stellen wir sicher, dass der laufende Betrieb Ihrer Organisation nicht beeinträchtigt wird und die Datenkonsistenz zum Zeitpunkt der Sicherung maximal ist. Es werden stets die Sicherungen der letzten sieben Tage vorgehalten. Diese siebentägige Aufbewahrungsfrist

bietet ein ausreichend großes Zeitfenster, um kurzfristig bemerkte Fehler schnell und mit minimalem Datenverlust zu korrigieren. Die Wiederherstellung aus einem solchen Snapshot ist der schnellste Weg, um den Zustand des Vortages oder eines anderen Zeitpunktes innerhalb der letzten Woche wiederherzustellen.

Stufe 2: Mittelfristige taktische Sicherung auf einem externen System

Während die täglichen Snapshots eine exzellente Absicherung für den Kurzzeitbereich darstellen, sind sie allein nicht ausreichend für ein vollumfängliches Schutzkonzept. Sie lagern zwar am selben Standort wie Ihr Server, meist in einem anderen Gebäude, bietet jedoch keinen ausreichenden Schutz vor einem großflächigen (regionalen) Aus- oder Katastrophenfall. Aus diesem Grund haben wir eine zweite, vollständig unabhängige Sicherungsebene etabliert. Diese Ebene dient der mittelfristigen Datensicherung und ist ein zentraler Baustein unserer Strategie zur Notfallvorsorge (Disaster Recovery).

Für diese zweite Stufe nutzen wir ein dediziertes Backup-System auf Basis einer Synology NAS (Network Attached Storage), das sich in unseren eigenen Geschäftsräumen und somit geografisch vollständig getrennt vom Hetzner-Rechenzentrum befindet. Auf dieses System wird einmal pro Woche ein vollständiges Backup der WORKSPACE.PM-Daten übertragen. Hierfür setzen wir die spezialisierte Software "Synology Active Backup for Business" ein, die eine anwendungskonsistente Sicherung der Datenbanken und Dateien gewährleistet. Von diesen wöchentlichen Sicherungen bewahren wir stets die letzten vier Versionen auf. Dies gibt uns die Möglichkeit, auf den Datenbestand von bis zu vier Wochen in die Vergangenheit zurückzugreifen. Ein solcher Rückgriff ist beispielsweise dann notwendig, wenn eine schleichende Datenkorruption erst nach mehr als sieben Tagen bemerkt wird und die kurzfristigen Snapshots den Fehler bereits enthalten.

Stufe 3: Langfristige strategische Archivierung

Die dritte und letzte Stufe unseres Konzepts dient der langfristigen Archivierung und der Erfüllung von Compliance-Anforderungen, wie sie beispielsweise im öffentlichen Sektor oder in regulierten Branchen üblich sind. Diese Archive sind nicht primär für die schnelle operative Wiederherstellung gedacht, sondern als strategische Reserve und für Auditzwecke. Sie stellen sicher, dass auch über einen langen Zeitraum hinweg definierte Datenstände rekonstruiert werden können, sei es für interne Revisionen, gesetzliche Nachweispflichten oder zur Analyse von lange zurückliegenden Vorgängen.

Diese Archivierung erfolgt ebenfalls über unser externes Synology NAS-System, jedoch in einem anderen Rhythmus und mit einer deutlich längeren Vorhaltezeit und die Speicherung erfolgt auf externen Speichermedien, welche nur bei Bedarf verbunden werden. Einmal pro Quartal wird eine vollständige und als solche gekennzeichnete Archiv-Sicherung erstellt. Diese quartalsweisen Sicherungspunkte werden für die Dauer von einem vollen Jahr aufbewahrt. Konkret bedeutet dies, dass wir zu jedem Zeitpunkt über vier strategische Sicherungspunkte verfügen, die jeweils den Zustand zum Ende eines Quartals abbilden. Diese Trennung von operativen, taktischen und strategischen Backups sorgt für eine klare Struktur und stellt

sicher, dass für jeden denkbaren Anwendungsfall die passende Datensicherung zur Verfügung steht.

4. Der Wiederherstellungsprozess im Bedarfsfall

Die sorgfältigste Anfertigung von Datensicherungen ist wertlos, wenn kein klar definierter und erprobter Prozess für deren Wiederherstellung existiert. Unser Wiederherstellungskonzept ist daher ebenso strukturiert wie unsere Sicherungsstrategie und orientiert sich an der Art und dem Umfang des jeweiligen Störfalls. Jeder Wiederherstellungsprozess wird von unserem Fachpersonal sorgfältig geplant, begleitet und dokumentiert, um einen reibungslosen Ablauf und die schnellstmögliche Wiederaufnahme des Normalbetriebs für Sie zu gewährleisten.

4.1. Initiierung und Analyse eines Wiederherstellungsfalls

Ein Wiederherstellungsprozess wird entweder durch eine Schadensmeldung Ihrerseits oder durch die proaktive Erkennung eines Problems durch unsere internen Überwachungssysteme (Monitoring) ausgelöst. In jedem Fall ist der erste Schritt eine unverzügliche und sorgfältige Analyse des Vorfalles. Unser technisches Team bewertet die Situation, um das genaue Ausmaß des Datenverlusts oder der Systemstörung zu ermitteln. Basierend auf dieser Analyse wird entschieden, welche Sicherungsebene und welcher spezifische Sicherungspunkt für die Wiederherstellung am besten geeignet ist. Ziel ist es stets, den Datenverlust so gering wie möglich zu halten (Recovery Point Objective, RPO) und das System so schnell wie möglich wieder in einen funktionsfähigen Zustand zu versetzen (Recovery Time Objective, RTO).

4.2. Szenario 1: Wiederherstellung bei operativen Datenverlust

Dieses Szenario ist das häufigste und betrifft typischerweise den Verlust oder die unbeabsichtigte Veränderung einer begrenzten Datenmenge, beispielsweise durch eine Fehlbedienung. Wenn der Fehler innerhalb von sieben Tagen bemerkt wird, greifen wir in der Regel auf die täglichen Snapshots der Stufe 1 zurück. Der Prozess sieht vor, dass der relevante Snapshot des Vortages oder eines früheren Datums verwendet wird um das System vollständig wiederherzustellen. Dieser gezielte Eingriff minimiert die Ausfallzeit.

4.3. Szenario 2: Wiederherstellung nach einem Teilausfall des Systems

Sollte ein schwerwiegenderes Problem auftreten, beispielsweise eine Beschädigung des Dateisystems oder der Datenbank, die durch die Snapshots nicht behoben werden kann, oder wenn der Fehler älter als sieben Tage ist, kommt unsere zweite Sicherungsebene zum Einsatz. In diesem Fall wird auf die wöchentlichen Backups auf unserem externen Synology-System zurückgegriffen. Je nach Schwere des Schadens kann dies bedeuten, dass wir den gesamten Datenbestand der WORKSPACE.PM-Anwendung aus dem Backup wiederherstellen. Dieser Prozess ist wesentlich aufwendiger als die Wiederherstellung aus einem Snapshot und wird eine geplante, Nichtverfügbarkeit der Anwendung erfordern, die wir selbstverständlich im Vorfeld mit Ihnen abstimmen.

4.4. Vorgehen im Katastrophenfall (Disaster Recovery)

Das unwahrscheinlichste, aber zugleich kritischste Szenario ist ein Totalausfall des primären Rechenzentrums, beispielsweise durch eine Naturkatastrophe oder einen anderen großflächigen Störfall. Für diesen Fall ist unser Konzept der geografisch getrennten Sicherung auf dem Synology NAS entscheidend. In einer solchen Situation würden wir den Notfallplan für die Wiederherstellung (Disaster Recovery Plan) aktivieren. Dieser sieht vor, eine neue, funktionale Serverumgebung bei einem alternativen Hosting-Anbieter oder in einem anderen, nicht betroffenen Rechenzentrum von Hetzner aufzusetzen. Anschließend würden wir das letzte verfügbare, integre Backup (wöchentlich oder quartalsweise) von unserem externen System auf die neue Infrastruktur übertragen und das System dort vollständig wiederherstellen. Dieser Prozess ist naturgemäß der zeitaufwendigste, stellt aber sicher, dass selbst im Falle einer Katastrophe Ihre wertvollen Daten nicht verloren sind und der Betrieb Ihrer Organisation nach einer angemessenen Zeit wieder aufgenommen werden kann.

5. Sicherheit und Integrität der Sicherungsdaten

Die Sicherungskopien Ihrer Daten sind ebenso schützenswert wie Ihre produktiven Daten selbst. Ein unbefugter Zugriff auf Backups könnte ebenso verheerende Folgen haben wie ein Angriff auf das Livesystem. Daher legen wir höchsten Wert auf die Sicherheit und die nachweisbare Integrität unserer gesamten Backup-Infrastruktur.

5.1. Verschlüsselung der Backup-Daten

Alle Sicherungsdaten werden durchgängig nach dem Stand der Technik verschlüsselt. Dies betrifft sowohl die Übertragung der Daten vom Produktivserver zu unserem externen Backup-System ("Encryption in Transit") als auch die Speicherung der Daten auf den Backup-Medien selbst ("Encryption at Rest"). Für die Übertragung nutzen wir gesicherte Protokolle (SSH). Auf dem Synology NAS-System sind die Festplatten, auf denen die Backups lagern, vollverschlüsselt. Dies stellt sicher, dass selbst im höchst unwahrscheinlichen Fall eines physischen Diebstahls des Backup-Systems die darauf befindlichen Daten für Unbefugte unlesbar und somit wertlos sind.

5.2. Zugriffskontrolle und Berechtigungsmanagement

Der Zugriff auf die Backup-Systeme und die darauf befindlichen Daten ist streng reglementiert. Es gilt das Prinzip der minimalen Rechtevergabe (Principle of Least Privilege). Das bedeutet, dass nur ein sehr kleiner, speziell autorisierter Kreis von Systemadministratoren die Berechtigung hat, auf die Backup-Konfigurationen zuzugreifen oder Wiederherstellungsprozesse durchzuführen. Jeder Zugriff wird protokolliert und überwacht. Für die Verwaltung der Systeme werden sichere Passwörter und eine Zwei-Faktor-Authentifizierung eingesetzt, um das Risiko eines unbefugten Zugriffs weiter zu minimieren.

5.3. Regelmäßige Überprüfung der Wiederherstellbarkeit

Ein Backup, das sich im Ernstfall nicht wiederherstellen lässt, ist nutzlos. Aus diesem Grund führen wir in regelmäßigen Abständen proaktive Tests zur Überprüfung der Integrität und Wiederherstellbarkeit unserer Sicherungen durch. Die von uns

eingesetzte Software "Synology Active Backup for Business" bietet hierfür automatisierte Verifizierungsfunktionen. Darüber hinaus führen wir in geplanten Intervallen manuelle Test-Wiederherstellungen in einer isolierten Testumgebung durch. Dabei wird ein komplettes Backup auf einem Testsystem wiederhergestellt, um den Prozess zu erproben und zu verifizieren, dass die Daten konsistent und vollständig sind. Diese Tests liefern uns die Gewissheit, dass unsere Sicherungsmechanismen im Ernstfall wie erwartet funktionieren.

6. Rollen und Verantwortlichkeiten

Ein erfolgreiches Datensicherungskonzept basiert auf einer klaren und partnerschaftlichen Zusammenarbeit zwischen Ihnen als unserem Kunden und uns als Ihrem Dienstleister. Die Definition der jeweiligen Rollen und Verantwortlichkeiten ist entscheidend, um im Bedarfsfall schnell, effizient und ohne Missverständnisse handeln zu können.

6.1. Unsere Verantwortung als Ihr Dienstleister

Als Ihr Managed-Hosting-Partner für WORKSPACE.PM tragen wir die vollumfängliche Verantwortung für die technische Umsetzung und den Betrieb des in diesem Dokument beschriebenen Datensicherungskonzepts. Unsere Aufgaben umfassen insbesondere die ordnungsgemäße und pünktliche Durchführung aller definierten Sicherungsläufe auf allen drei Ebenen. Wir sind verantwortlich für die kontinuierliche Überwachung der Backup-Prozesse, um fehlgeschlagene Sicherungen umgehend zu erkennen und zu beheben. Die Wartung und Absicherung der gesamten Backup-Infrastruktur, einschließlich der externen Systeme, liegt ebenfalls in unserem Verantwortungsbereich. Im Falle eines von Ihnen gemeldeten oder von uns festgestellten Datenverlusts sind wir dafür zuständig, den unter Punkt 4 beschriebenen Wiederherstellungsprozess einzuleiten, durchzuführen und Sie über den Fortschritt transparent zu informieren.

6.2. Ihre Mitwirkung als unser Kunde

Ihre Rolle in diesem Prozess ist ebenso wichtig. Ihre Hauptverantwortung liegt darin, uns unverzüglich zu informieren, sobald Sie einen Datenverlust oder eine Unregelmäßigkeit in Ihrer WORKSPACE.PM-Instanz feststellen. Eine frühzeitige Meldung ist entscheidend, da sie uns ermöglicht, auf die aktuellsten und am besten geeigneten Sicherungen zurückzugreifen und den potenziellen Datenverlust zu minimieren. Für einen erfolgreichen Wiederherstellungsprozess sind wir auf Ihre Mithilfe angewiesen, um den Vorfall genau zu spezifizieren: Welche Daten sind betroffen? Zu welchem Zeitpunkt ist der Fehler mutmaßlich aufgetreten? Nach einer erfolgten Wiederherstellung bitten wir Sie, die wiederhergestellten Daten zu überprüfen und uns eine Bestätigung zu geben, dass das System wieder wie erwartet funktioniert. Das Verständnis für die Funktionsweise des Konzepts, insbesondere der Wiederherstellungspunkte (z.B. dass bei einer Wiederherstellung vom Vortag alle nach dem Sicherungszeitpunkt getätigten Änderungen verloren gehen), ist ebenfalls Teil Ihrer Mitwirkungspflicht.

7. Zusammenfassung

Die Sicherung Ihrer Daten in WORKSPACE.PM ist eine Aufgabe, der wir mit höchster Priorität und größter Sorgfalt nachkommen. Wie in diesem Dokument ausführlich dargelegt, haben wir ein robustes, mehrstufiges Datensicherungskonzept implementiert, das auf bewährten Industriestandards, moderner Technologie und einem klaren Prozessdenken basiert. Durch die Kombination aus täglichen, operativen Snapshots, wöchentlichen taktischen Backups auf einem geografisch getrennten System und quartalsweisen strategischen Archiven stellen wir sicher, dass wir für jedes denkbare Szenario – vom kleinen Bedienfehler bis hin zur Katastrophe im Rechenzentrum – einen definierten und erprobten Wiederherstellungsplan haben.

Die Sicherheit Ihrer Daten wird durch konsequente Verschlüsselung, strikte Zugriffskontrollen und regelmäßige Integritätstests gewährleistet. Dieses umfassende Konzept gibt Ihnen die Sicherheit und das Vertrauen, dass Ihre geschäftskritischen Projekt- und Portfoliodaten bei uns sicher und jederzeit wiederherstellbar sind.

Die Welt der Informationstechnologie ist jedoch einem ständigen Wandel unterworfen. Neue technologische Möglichkeiten entstehen, und gleichzeitig entwickeln sich auch die Bedrohungen weiter. Aus diesem Grund verstehen wir dieses Datensicherungskonzept nicht als ein statisches Dokument, sondern als einen lebendigen Prozess. Wir verpflichten uns, unsere Strategien und Technologien regelmäßig zu überprüfen, zu bewerten und bei Bedarf anzupassen, um Ihnen auch in Zukunft stets ein Schutzniveau zu bieten, das dem aktuellen Stand der Technik entspricht.

Vertragliche Regelungen zur Auftragsverarbeitung gemäß Art. 28 EU-DSGVO

zwischen

– im Folgenden Auftraggeber genannt –

und

AMNAU GmbH

Kronenstraße 13, 30161 Hannover

– im Folgenden Auftragnehmer genannt –

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem WORKSPACE.PM – Lizenzvertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 – Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags, sowie Art und Zweck der Verarbeitung. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

Im Rahmen der Nutzung von WORKSPACE.PM können insbesondere folgende Arten personenbezogener Daten verarbeitet werden: Stammdaten (z.B. Name, Vorname, Anrede, Titel), Kontaktdaten (z.B. E-Mailadresse, Telefonnummer), Organisationsdaten (z.B. Abteilung, Teamzugehörigkeit, Rollen), Zugangsdaten (z.B. Password-Hash, Token), Kommunikations- und Inhaltsdaten (z.B. Projektbeschreibungen, Aufgaben, Kommentare, Anhänge, interne Notizen, Protokolle), Nutzungsdaten (z.B. Logfiles, Zeitstempel von Aktivitäten, Audit-Log).

Die Verarbeitung erfolgt bezogen auf folgende Kategorien betroffener Personen: Mitarbeiter des Auftraggebers (z.B. Projektmitarbeiter, Administratoren, Nutzer), externe Dienstleister / Partner (sofern diese im System als Nutzer erfasst werden), Ansprechpartner und sonstige natürliche Personen, deren personenbezogene Daten in den von den Nutzern in

WORKSPACE.PM eingegebenen Inhalten enthalten sind (z.B. in Freitextfeldern, Anhängen).

§ 2 – Anwendungsbereich und Verantwortlichkeit

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).
- (2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 – Pflichten des Auftragnehmers

- (1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
- (2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutzgrundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.
- (3) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten. Der Auftragnehmer unterstützt den Auftraggeber – soweit vereinbart und möglich – bei der Durchführung einer Datenschutzfolgeabschätzung nach Art. 35 DSGVO, sowie bei etwaigen Konsultationen mit der Aufsichtsbehörde nach Art. 36 DSGVO.
- (4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten.

Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

- (5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
- (6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
- (7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
- (8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Daten-trägern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Daten-träger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.
- (9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. Die Löschung bzw. Rückgabe hat spätestens innerhalb von 30 Tagen nach Vertragsende in einem strukturierten, gängigen und maschinenlesbaren Format zu erfolgen. Die Löschung wird vom Auftragnehmer dokumentiert und dem Auftraggeber auf Wunsch nachgewiesen.
- (10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 4 – Pflichten des Auftraggebers

- (1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. Datenschutzrechtlicher Bestimmungen feststellt.
- (2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt § 3 Abs. 10 entsprechend.
- (3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Der Ansprechpartner des

Auftragnehmers ist Benjamin Bolzmann (Telefon: 0511 / 5154545601, E-Mail: b.bolzmann@amnau.de)

§ 5 – Anfragen betroffener Personen

- (1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 – Nachweismöglichkeiten

- (1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.
- (2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen, wenn dies im Vertrag vereinbart ist. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.
- (3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 – Subunternehmer (weitere Auftragsverarbeiter)

- (1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.
- (2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer

durchgeführt: Schlund Technologies GmbH, Regensburg und OVH GmbH, Köln (Domains); Hetzner Online GmbH, Gunzenhausen (Server-Hosting), OpenAI Ireland Ltd., Dublin, Irland (optionale AI-Features, explizites Trainings-Opt-Out)

- (3) Soweit bei der Beauftragung von Subunternehmern eine Datenverarbeitung in einem Drittstaat erfolgt, stellt er Auftragnehmer sicher, dass ein angemessenes Datenschutzniveau gem. Kapitel V DSGVO gewährleistet ist (z.B. durch Abschluss von Standardvertragsklauseln oder Teilnahme am Data Privacy Framework).
- (4) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Der Auftraggeber wird über geplante Änderungen bezüglich der Hinzuziehung oder Ersetzung von Subunternehmern in Textform rechtzeitig informiert, sodass er innerhalb von 14 Tagen widersprechen kann.

§ 8 – Informationspflichten, Schriftformklausel, Rechtswahl

- (1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutzgrundverordnung liegen.
- (2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Form-erfordernis.
- (3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
- (4) Es gilt deutsches Recht. Der Gerichtsstand ist Hannover.

§ 9 – Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

Anlage: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Ort: Geschäftsräume der AMNAU GmbH

Kronenstraße 13, 30161 Hannover

Stand: 01.02.2025

Zutrittskontrolle

- Sicherheitsschlösser (teilweise Transponder)

Zugangskontrolle

- Authentifizierung mit persönlichem Benutzernamen und Passwort
- Einsatz von Antiviren-Software
- Einsatz mehrstufiger Firewalls
- Einsatz von VPN-Technologie
- Einsatz von Mehrfaktorauthentifizierung
- Zentrale Verwaltung der Benutzerberechtigungen
- Zentrale Benutzerprofile
- Initiale Passwortvergabe und Anwendung von Passwortregeln (alphanumerisch mit Sonderzeichen)

Zugriffskontrolle

- Einsatz von Aktenvernichtern (DIN 66399) mit einer Mindestschutzstufe 4
- Physikalische Zerstörung von Datenträgern
- Anzahl der Administratoren auf zwei begrenzt
- Anwendung Berechtigungskonzept
- Zentrale Verwaltung der Benutzerrechte durch Systemadministratoren

Weitergabekontrolle

- Alle Mitarbeiter wurden auf das Datengeheimnis verpflichtet
- Datenschutzgerechte Löschung der Daten erfolgt nach Auftragsbeendigung
- Einrichtung VPN-Tunnel
- E-Mailverschlüsselung und -signierung

Eingabekontrolle

- Protokollierung der Eingabe, Änderungen und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung von Daten durch individuelle Benutzernamen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes

Auftragskontrolle

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Schriftliche Weisung an Auftragnehmer i.S.v. Art 28 DSGVO
- Die AMNAU GmbH beschäftigt einen zertifizierten Datenschutzbeauftragten und sorgt durch ein Datenschutzmanagementkonzept für dessen angemessene und effektive Einbindung in relevante Geschäftsprozesse
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis