Vertrag über die Bereitstellung der Plattform „ehyp home"

zwischen der

Prohyp GmbH
August-Everding-Straße 24
81671 München

- im Folgenden: „**PROHYP**" oder „**ANBIETERIN**" genannt,

und

der „**KUNDIN**" oder dem „**Untervermittler**"

- beide gemeinschaftlich im Folgenden „**Vertragspartner**" genannt

Vorbemerkungen / Präambel
Die Vertragspartner sind einander auf Basis eines Rahmenvertrages sowie etwaiger Nachträge und Ergänzungsvereinbarungen hierzu (im Folgenden insgesamt „Hauptvertrag" genannt) vertraglich verbunden. Auf den Hauptvertrag wird ausdrücklich Bezug genommen. Der Hauptvertrag bildet die wesentliche Grundlage der Kooperation der Vertragspartner. Der vorliegende Plattformnutzungsvertrag ergänzt den Hauptvertrag in Bezug auf die Nutzung der neuen und funktionserweiterten Baufinanzierungsplattform „ehyp home".

Alle im vorliegenden Vertrag und dem **Anhang 1** enthaltenen Informationen zur technischen und fachlichen Spezifikation der ANWENDUNG sind eine Beschreibung des IST-Zustands zum Stichtag 01.10.2025. Der KUNDIN ist bewusst, dass die ANBIETERIN die ANWENDUNG stetig weiterentwickelt und sich dadurch insbesondere die in **Anhang 1** genannten technischen und fachlichen Spezifikationen ändern werden. Die KUNDIN stimmt dem ausdrücklich zu.

§ 1 Vertragsgegenstand
Gegenstand dieses Leistungsscheins ist die Bereitstellung der in **Anhang 1** vereinbarten Softwareanwendung (im Folgenden: ANWENDUNG) zur Nutzung ihrer Funktionalitäten, die technische Ermöglichung der Nutzung der ANWENDUNG und die Einräumung von Nutzungsrechten an der ANWENDUNG sowie die Bereitstellung von Speicherplatz für die von der KUNDIN durch Nutzung der ANWENDUNG erzeugten und/oder die zur Nutzung der ANWENDUNG erforderlichen Daten (im Folgenden: ANWENDUNGSDATEN) in im **Anhang 1** vereinbarten Umfang durch die ANBIETERIN gegenüber der KUNDIN.

Die ANWENDUNG selbst dient dabei lediglich der technischen Umsetzung der Beratung und Untervermittlung der ANBIETERIN an die KUNDIN.

§ 2 Bereitstellung der ANWENDUNG und Speicherplatz für ANWENDUNGSDATEN

(1) Die ANBIETERIN hält ab sofort auf einer zentralen Datenverarbeitungsanlage oder mehreren Datenverarbeitungsanlagen (im Folgenden, auch bei Mehrzahl: SERVER) die in **Anhang 1** vereinbarte ANWENDUNG in der jeweils aktuellen Version zur Nutzung nach Maßgabe der nachfolgenden Regelungen bereit.

(2) Die ANBIETERIN gewährleistet, dass die bereitgestellte ANWENDUNG:
   a. für die sich aus der Leistungsbeschreibung in **Anhang 1** ergebenden Zwecke grundsätzlich geeignet ist,
   b. während der gesamten Vertragslaufzeit frei von erheblichen Mängeln ist.

(3) Die ANBIETERIN betreibt die ANWENDUNG hybrid. Die ANWENDUNG wird demnach parallel auf eigenen Servern der ANBIETERIN und auch auf dem Cloud-Dienst Microsoft Azure betrieben bzw. gehostet. Dies beinhaltet auch den damit verbundenen Transfer der ANWENDUNGSDATEN in ein Drittland. Die KUNDIN stimmt dem ausdrücklich zu. Der ANBIETERIN steht es nach eigenem Ermessen frei, dieses hybride Betriebsprofil jederzeit zu ändern.

(4) Die Verantwortung für die Erstellung und Verwaltung der individuellen Benutzerkennungen innerhalb der ANWENDUNG (Accounts) obliegt grundsätzlich der KUNDIN. Die KUNDIN ist für die Pflege der Nutzerdaten allein verantwortlich. Den Nutzern werden von der ANBIETERIN keine Zugangsdaten zur Verfügung gestellt, sofern die Anmeldung der Nutzer über das SSO (Single Sign On) - Verfahren erfolgt. Für die Zuweisung von Rechten und Rollen bzw. Kompetenzen eines Accounts innerhalb der ANWENDUNG ist die KUNDIN allein verantwortlich. Dies gilt insbesondere für gewerberechtliche Anforderungen an Tätigkeiten eines Accounts im Sinne des § 34i GewO.

(5) Die KUNDIN ist Fall der Teilnahme am SSO-Verfahren verpflichtet sicherzustellen, dass alle von ihr erstellten Benutzerkennungen als authentifizierte Nutzer der ANWENDUNG autorisiert sind.

(6) Die ANBIETERIN verfügt über interne Benutzerkennungen mit Zugriff auf die ANWENDUNG und die ANWENDUNGSDATEN. Dieser Zugang ist für die Quality Assurance, sowie für Maßnahmen zur Fehlerbehebung erforderlich.

(7) Die ANBIETERIN wird die ANWENDUNG konstant weiterentwickeln. Mit der Bereitstellung einer neuen Version oder einer Änderung der ANWENDUNG können Änderung von Funktionalitäten der ANWENDUNG, Änderung von Workflows der KUNDIN innerhalb der ANWENDUNG und/oder auch Beschränkungen in der Verwendbarkeit bisher erzeugter ANWENDUNGSDATEN einhergehen. Die KUNDIN ist durch die Nutzung der ANWENDUNG damit ausdrücklich einverstanden.

(8) Die ANWENDUNG umfasst Funktionalitäten, welche gegebenenfalls über API (Application Programming Interface) durch die KUNDIN an- und eingebunden werden können. Die KUNDIN ist für die An- und Einbindung dieser Schnittstellen selbst verantwortlich. Für API gelten gegebenenfalls zusätzlich gesonderte Nutzungsbedingungen.

(9) Die ANBIETERIN hält auf dem SERVER ab dem Zeitpunkt der betriebsfähigen Bereitstellung für die ANWENDUNGSDATEN Speicherplatz im für die Ausführung der ANWENDUNG benötigten Umfang bereit.

(10) Die ANWENDUNG und die ANWENDUNGSDATEN werden auf dem SERVER regelmäßig, mindestens kalendertäglich, gesichert. Für die Einhaltung handels- und steuerrechtlicher Aufbewahrungsfristen ist die KUNDIN allein verantwortlich.

(11) Leistungsübergabepunkt (LÜP) für den Betrieb der ANWENDUNG ist das Ausgangsinterface der Firewall der ANBIETERIN in Richtung Internet

(12) Für die Schaffung der erforderlichen Systemvoraussetzungen auf Seiten der KUNDIN für die Nutzung der ANWENDUNG ist die KUNDIN allein verantwortlich. Für die Beschaffenheit der erforderlichen Hard- und Software auf Seiten der KUNDIN sowie für die erforderliche Telekommunikationsverbindung zwischen der KUNDIN und der ANBIETERIN bis zum Übergabepunkt ist die ANBIETERIN nicht verantwortlich.

§ 3 Technische Verfügbarkeit der ANWENDUNG und des Zugriffs auf die ANWENDUNGSDATEN, Reaktions- und Wiederherstellungszeiten

(1) Die ANBIETERIN schuldet die in **Anhang 1** vereinbarte Verfügbarkeit der ANWENDUNG und der ANWENDUNGSDATEN am Service-Endpunkt. Unter Verfügbarkeit verstehen die Vertragspartner die technische Nutzbarkeit der ANWENDUNG und der ANWENDUNGSDATEN am Service-Endpunkt zum Gebrauch durch die KUNDIN.

(2) Störungen oder Fehler der ANWENDUNG, welche nicht im Macht- und Einflussbereich der ANBIETERIN liegen (wie z.B. Störung der bereitgestellten Schnittstellen auf Seiten der KUNDIN oder durch unsachgemäße Nutzung der ANWENDUNG durch die KUNDIN) entstehen, sind nicht von der ANBIETERIN zu vertreten.

(3) Für Nutzung der ANWENDUNG wird ein Desktop Internet Browser benötigt. Die ANBIETERIN stellt die Nutzbarkeit der ANWENDUNG für alle Desktop Browser mit einem Marktanteil innerhalb Deutschlands von mehr als 20% sicher.

§ 4 Gewährleistung

(1) Es gelten die im **Anhang 1** festgelegten Verfügbarkeiten der ANBIETERIN.

(2) Die Anwendung des § 536a Abs. 2 BGB ist jedoch ausgeschlossen. Ausgeschlossen ist auch die Anwendung von § 536a Abs. 1 BGB, soweit die Norm eine verschuldensunabhängige Haftung vorsieht.

(3) Die ANBIETERIN stellt die ANWENDUNG im Rahmen eines „Software-as-a-Service"-Modells bereit. Sie wird dabei in der jeweils aktuellen Version „wie sie ist" („as is") und „wie verfügbar" („as available") zur Nutzung über das Internet bereitgestellt.

(4) Die ANBIETERIN übernimmt keine Gewähr dafür, dass die ANWENDUNG jederzeit ohne Unterbrechung, fehlerfrei oder sicher verfügbar ist. Insbesondere wird keine Gewähr für bestimmte Funktionen, die Kompatibilität mit bestimmten Systemen oder die Eignung für einen bestimmten Zweck übernommen, sofern nicht ausdrücklich etwas anderes bestimmt ist.

(5) Soweit gesetzlich zulässig, sind sämtliche Gewährleistungsansprüche ausgeschlossen. Dies gilt insbesondere für Sach- und Rechtsmängel, soweit diese nicht auf Vorsatz oder grober Fahrlässigkeit der ANBIETERIN beruhen.

(6) Die ANBIETERIN übernimmt keine Verantwortung für Datenverluste, Systemausfälle oder sonstige Schäden, die durch die Nutzung der ANWENDUNG entstehen, es sei denn, diese beruhen auf vorsätzlichem oder grob fahrlässigem Verhalten.

(7) Zwingende gesetzliche Rechte der KUNDIN bleiben von diesem Ausschluss unberührt.

§ 5 Nutzungsrechte, Rechte der ANBIETERIN bei Überschreitung der Nutzungsbefugnisse

(1) Nutzungsrechte an der ANWENDUNG

a. Die KUNDIN erhält an der ANWENDUNG das einfache, nicht ohne ausdrückliche Zustimmung der ANBIETERIN unterlizenzierbare und nicht übertragbare, auf die Laufzeit des Hauptvertrages beschränkte Nutzungsrecht nach Maßgabe der nachstehenden Regelungen.
b. Eine physische Überlassung der ANWENDUNG an die KUNDIN erfolgt nicht. Die KUNDIN darf die ANWENDUNG nur für ihre eigenen geschäftlichen Tätigkeiten nutzen.
c. Die KUNDIN ist nicht berechtigt, Änderungen an der ANWENDUNG vorzunehmen.
d. Sofern die ANBIETERIN während der Vertragslaufzeit neue Versionen, Updates, Upgrades oder andere Entwicklungen im Hinblick auf die ANWENDUNG vornimmt, gelten die vorstehenden Rechte auch für diese.
e. Rechte, die der KUNDIN vorstehend nicht ausdrücklich eingeräumt werden, stehen der KUNDIN nicht zu. Die KUNDIN ist insbesondere nicht berechtigt, die ANWENDUNG über die vereinbarte Nutzung hinaus zu nutzen oder von Dritten nutzen zu lassen oder die ANWENDUNG Dritten zugänglich zu machen. Insbesondere ist es nicht gestattet, die ANWENDUNG zu vervielfältigen, zu veräußern oder zeitlich begrenzt zu überlassen, insbesondere nicht zu vermieten oder zu verleihen.

(2) Verpflichtungen der KUNDIN zur sicheren Nutzung

a. Die KUNDIN trifft alle notwendigen bzw. erforderlichen Vorkehrungen, die Nutzung der ANWENDUNG durch Unbefugte zu verhindern.
b. Die KUNDIN ist allein verantwortlich dafür, dass die ANWENDUNG nicht zu rassistischen, diskriminierenden, pornographischen, den Jugendschutz gefährdenden, politisch extremen oder sonst gesetzeswidrigen oder gegen behördliche Vorschriften oder Auflagen verstoßenden Zwecken verwendet oder entsprechende Daten, insbesondere ANWENDUNGSDATEN, erstellt und/oder auf dem SERVER gespeichert werden.

(3) Verletzung der Bestimmungen nach Abs. 1 und 2 durch die KUNDIN

a. Verletzt die KUNDIN die Regelungen in Abs. 1 oder 2 aus von ihr zu vertretenden Gründen auch nach vorheriger Abmahnung weiterhin, kann die ANBIETERIN nach vorheriger schriftlicher Benachrichtigung den Zugriff der KUNDIN auf die ANWENDUNG oder die ANWENDUNGSDATEN ganz oder teilweise sperren, wenn die Verletzung hierdurch nachweislich abgestellt werden kann.

b. Verstößt die KUNDIN rechtswidrig gegen § 5 Abs. 2 lit. b dieses Vertrages, ist die ANBIETERIN berechtigt, die dadurch betroffenen Daten bzw. ANWENDUNGSDATEN zu löschen. Im Fall eines rechtswidrigen Verstoßes durch Nutzer hat die KUNDIN der ANBIETERIN auf Verlangen unverzüglich sämtliche Angaben zur Geltendmachung der Ansprüche gegen den Nutzer zu machen, insbesondere dessen Namen und Anschrift mitzuteilen.
c. Verletzt die KUNDIN trotz entsprechender schriftlicher Abmahnung der ANBIETERIN weiterhin oder wiederholt die Regelungen in Abs. 1 oder 2, und hat die KUNDIN dies zu vertreten, so kann die ANBIETERIN den vorliegen Vertrag ohne Einhaltung einer Kündigungsfrist außerordentlich kündigen.

(4) Rechte der KUNDIN an etwa entstehenden Datenbanken/Datenbankwerken
Sofern und soweit während der Laufzeit dieses Vertrags, insbesondere durch Zusammenstellung von ANWENDUNGSDATEN, durch nach diesem Vertrag erlaubte Tätigkeiten der KUNDIN auf dem SERVER der ANBIETERIN eine Datenbank, Datenbanken, ein Datenbankwerk oder Datenbankwerke entstehen, stehen alle Rechte hieran der KUNDIN zu. DIE KUNDIN bleibt auch nach Vertragsende Eigentümerin der Datenbanken bzw. Datenbankwerke.

§ 6 Haftung für Rechte Dritter

(1) Die ANBIETERIN wird die KUNDIN von Rechten Dritter bzw. von deren Geltendmachung und von einer daraus resultierenden Beeinträchtigung der Erbringung vereinbarter Leistungen unverzüglich unterrichten und die KUNDIN in geeigneter Weise den vollen Zugriff auf die ANWENDUNGSDATEN ermöglichen.

(2) Die ANBIETERIN haftet nicht für eine Verletzung der Rechte Dritter durch die KUNDIN, sofern und soweit sich diese Verletzung aus einer Überschreitung der nach diesem Vertrag eingeräumten Nutzungsrechte ergibt. In diesem Fall stellt die KUNDIN die ANBIETERIN von sämtlichen Ansprüchen Dritter auf erstes Anfordern frei.

§ 7 Vergütung

(1) Die ANBIETERIN ermöglicht der KUNDIN die Nutzung der ANWENDUNG in seinem elementaren Funktionsumfang mehrkostenfrei. Die Vergütungs- bzw. Provisionsbestimmungen für die Vermittlungstätigkeit richten sich ausschließlich nach den jeweiligen Bestimmungen des Hauptvertrages.

(2) Die ANBIETERIN weist die KUNDIN ausdrücklich darauf hin, dass bestimmte Funktionen innerhalb der ANWENDUNG, welche zur Vermittlung von Baufinanzierung nicht zwingend elementar sind, zukünftig kostenpflichtig werden können. Das gilt für bestehende Funktionen und für zusätzliche Funktionen der ANWENDUNG gleichermaßen. Im Falle einer eintretenden Kostenpflichtigkeit für bereits bestehende Funktionen wird die ANBIETERIN dies rechtzeitig im Voraus ankündigen. Schließt die KUNDIN keinen entsprechenden Nutzungsvertrag ab, wird die ANBIETERIN die Funktion nach Ablauf der Ankündigungsfrist für die KUNDIN abschalten.

(3) Die ANWENDUNG ermöglicht es der KUNDIN, Leistungen und Services Dritter zu nutzen. Diese Fremd- bzw. Drittanbieterleistungen (z.B. SCHUFA Abrufe oder

Objektbewertungen durch Sprengnetter, VDP, o.ä.) werden mit der KUNDIN gesondert abgerechnet.

§ 8 Pflichten und Obliegenheit der KUNDIN

Die KUNDIN wird alle Pflichten und Obliegenheiten erfüllen, die zur Abwicklung des Vertrags erforderlich sind. Die KUNDIN wird insbesondere

- die der KUNDIN bzw. den Nutzern zugeordneten Nutzungs- und Zugangsberechtigungen sowie vereinbarte Identifikations- und Authentifikations-Sicherungen geheim halten, vor dem Zugriff durch Dritte schützen und nicht an unberechtigte Nutzer weitergeben. Diese Daten sind durch geeignete und übliche Maßnahmen zu schützen. Die KUNDIN wird die ANBIETERIN unverzüglich unterrichten, wenn der Verdacht besteht, dass die Zugangsdaten und/oder Kennwörter nicht berechtigten Personen bekannt geworden sein könnten;
- die gemäß § 2 erforderlichen technischen Zugangs- und Nutzungsvoraussetzungen schaffen;
- die Beschränkungen/ Verpflichtungen im Hinblick auf die Nutzungsrechte nach § 5 einhalten, insbesondere
    - alle von der KUNDIN für die Nutzung der ANWENDUNG vorgesehenen Nutzer als „*named User*" nachvollziehbar kenntlich zu machen;
    - keine Informationen oder Daten unbefugt abrufen oder abrufen lassen oder in Programme, die von der ANBIETERIN betrieben werden eingreifen oder eingreifen lassen oder in Datennetze der ANBIETERIN unbefugt eindringen oder ein solches Eindringen fördern;
    - den im Rahmen der Vertragsbeziehung und/oder unter Nutzung der ANWENDUNG möglichen Austausch von elektronischen Nachrichten nicht missbräuchlich für den unaufgeforderten Versand von Nachrichten und Informationen an Dritte zu Werbezwecken nutzen;
    - die ANBIETERIN von Ansprüchen Dritter freistellen, die auf einer rechtswidrigen Verwendung der ANWENDUNG durch die KUNDIN beruhen oder die sich aus von der KUNDIN verursachten datenschutzrechtlichen, urheberrechtlichen oder sonstigen rechtlichen Streitigkeiten ergeben, die mit der Nutzung der ANWENDUNG verbunden sind;
    - die berechtigten Nutzer verpflichten, ihrerseits die für sie geltenden Bestimmungen dieses Vertrags einzuhalten;
- dafür Sorge tragen, dass sie (z.B. bei der Übermittlung von Texten/ Daten Dritter auf den SERVER der ANBIETERIN) alle Rechte Dritter an von ihr verwendetem Material beachtet;
- soweit sie bei Nutzung der ANWENDUNG personenbezogene Daten erhebt, verarbeitet oder nutzt, sämtliche datenschutzrechtliche Pflichten einhalten;
- vor der Übermittlung von Daten und Informationen an die ANBIETERIN bzw. vor der Verarbeitung von Daten in der ANWENDUNG, diese Daten auf Schadsoftware prüfen und dem Stand der Technik entsprechende Schutzmaßnahmen ergreifen, welche die Integrität der zu verarbeitenden Daten gewährleisten;
- wenn die KUNDIN zur Erzeugung von ANWENDUNGSDATEN mit Hilfe der ANWENDUNG der ANBIETERIN Daten übermittelt, diese regelmäßig und der Bedeutung der Daten entsprechend sichern und eigene Sicherungskopien erstellen, um bei Verlust der Daten und Informationen die Rekonstruktion derselben zu ermöglichen;
- sofern und soweit der ANBIETERIN die technische Möglichkeit dazu eröffnet wird, regelmäßig die auf dem SERVER gespeicherten ANWENDUNGSDATEN durch Download sichern.

§ 9 Datensicherheit, Datenschutz

(1) Die Vertragspartner werden die jeweils anwendbaren, datenschutzrechtlichen Bestimmungen beachten und ihre im Zusammenhang mit dem Vertrag und dessen Durchführung eingesetzten Beschäftigten auf das Datengeheimnis nach § 53 BDSG verpflichten, soweit diese nicht bereits allgemein entsprechend verpflichtet sind.

(2) Erhebt, verarbeitet oder nutzt die KUNDIN personenbezogene Daten, so steht sie dafür ein, dass sie dazu nach den anwendbaren, insbesondere datenschutzrechtlichen, Bestimmungen berechtigt ist und stellt im Fall eines Verstoßes die ANBIETERIN von allen Ansprüchen Dritter auf erstes Anfordern hin frei.

(3) Die Verpflichtungen nach Abs. 1 bis 2 bestehen, solange die ANWENDUNGSDATEN im Einflussbereich der ANBIETERIN liegen, auch über das Vertragsende hinaus.

(4) Die ANBIETERIN setzt zum Zwecke der Weiterentwicklung und Verbesserung der ANWENDUNG Technologien zur anonymen Erfassung und Analyse des Nutzungsverhaltens der Nutzer ein. Die KUNDIN stimmt dem Einsatz solcher Technologien grundsätzlich zu.
Zusätzlich setzt die ANBIETERIN Technologien zur Durchführung individualisierter Umfragen und zur Abgabe von Feedbacks ein.
Der Einsatz all dieser Technologien erfolgt erst nach Zustimmung durch den Nutzer.

(5) Die Vertragspartner werden die jeweils notwendigen Zusatzverträge abschließen, wenn die datenschutzrechtliche Konstellation dies erfordert. Für die Nutzung der Plattform schließen beide Vertragspartner einen Vertrag über die Verarbeitung personenbezogener Daten im Auftrag gem. Artikel 28 DSGVO ab (**Anhang 2**).

Die KUNDIN erklärt sich mit dem Lösch- und Sperrkonzept der ANBIETERIN für die Plattform einverstanden.

§ 10 Geheimhaltung

(1) Vertraulich zu behandelnde Informationen sind die von dem informationsgebenden Vertragspartner ausdrücklich als vertraulich bezeichneten Informationen und solche Informationen, deren Vertraulichkeit sich aus den Umständen der Überlassung eindeutig ergibt. Durch die ANBIETERIN vertraulich zu behandeln sind insbesondere die ANWENDUNGSDATEN, sollte sie von ihnen Kenntnis erlangen.
Keine vertraulich zu behandelnde Information liegt vor, soweit der die Information empfangende Vertragspartner nachweist, dass sie:

- ihm vor dem Empfangsdatum bekannt oder allgemein zugänglich waren;
- der Öffentlichkeit vor dem Empfangsdatum bekannt oder allgemein zugänglich waren;
- der Öffentlichkeit nach dem Empfangsdatum bekannt oder allgemein zugänglich wurden, ohne dass der informationsempfangende Vertragspartner hierfür verantwortlich ist.

(2) Die Vertragspartner werden über alle vertraulichen Informationen, die ihnen im Rahmen dieses Vertragsverhältnisses zur Kenntnis gelangt sind, Stillschweigen bewahren bzw. diese nur im vorher schriftlich hergestellten Einvernehmen des jeweils anderen Vertragspartners Dritten gegenüber – gleich zu welchem Zweck – verwenden.

(3) Öffentliche Erklärungen der Vertragspartner über eine Zusammenarbeit werden nur im vorherigen gegenseitigen Einvernehmen abgegeben.

(4) Die Verpflichtungen nach Abs. 2 bestehen auch über das Vertragsende hinaus auf unbestimmte Zeit, und zwar so lange, wie ein Ausnahmetatbestand nach Abs. 1 nicht nachgewiesen ist.

§ 11 Haftung, Haftungsgrenzen und Vertragsstrafe

(1) Die Vertragspartner haften einander bei Vorsatz oder grober Fahrlässigkeit für alle von ihnen sowie ihren gesetzlichen Vertretern oder Erfüllungsgehilfen verursachten Schäden unbeschränkt.

(2) Bei leichter Fahrlässigkeit haften die Vertragspartner im Fall der Verletzung des Lebens, des Körpers oder der Gesundheit unbeschränkt.

(3) Im Übrigen haftet ein Vertragspartner nur, soweit er eine wesentliche Vertragspflicht verletzt hat. Wesentliche Vertragspflichten sind solche Pflichten, die für die Erreichung des Vertragsziels von besonderer Bedeutung sind, ebenso alle diejenigen Pflichten, die im Fall einer schuldhaften Verletzung dazu führen können, dass die Erreichung des Vertragszwecks gefährdet wird. In diesen Fällen ist die Haftung auf den Ersatz des vorhersehbaren, typischerweise eintretenden Schadens beschränkt. Die verschuldensunabhängige Haftung der ANBIETERIN auf Schadensersatz (§ 536a BGB) für bei Vertragsschluss vorhandene Mängel wird ausgeschlossen; Abs. 1 und 2 bleiben unberührt.

(4) Ein Vertragspartner ist zur Zahlung einer Vertragsstrafe nur verpflichtet, wenn dies dieser Vertrag ausdrücklich vorsieht. Die Aufrechnung mit und gegen die Vertragsstrafe ist zulässig.

(5) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

§ 12 Laufzeit, Kündigung

(1) Das Vertragsverhältnis über die Nutzung der ANWENDUNG beginnt mit Zustimmung des Bevollmächtigten der KUNDIN zu diesem Vertrag und wird auf unbestimmte Zeit geschlossen.

(2) Der vorliegende Vertrag über die Bereitstellung der ANWENDUNG durch die ANBIETERIN endet mit Beendigung des Hauptvertrages automatisch mit, ohne dass es einer gesonderten Kündigung bedarf.

(3) Im Übrigen gelten hinsichtlich ordentlicher und außerordentlicher Kündigung dieses Vertrages die Bestimmungen des „Hauptvertrages" entsprechend.

§ 13 Pflichten bei und nach Beendigung des Vertrags

(1) Mit Beendigung des Vertragsverhältnisses ist die ANBIETERIN auf Anfrage der KUNDIN verpflichtet, die von der KUNDIN gespeicherten ANWENDUNGSDATEN dieser auf einem dauerhaft lesbaren mobilen und revisionssicheren Datenträger in einem maschinenlesbaren Datenformat zur Verfügung zu stellen.

(2) Die KUNDIN ist verpflichtet, der ANBIETERIN die entstandenen notwendigen und nachgewiesenen Kosten zu ersetzen.

(3) Die ANBIETERIN ist auf Verlangen der KUNDIN verpflichtet, nach rechtlicher Beendigung dieses Vertrags zur Abwicklung dieses Vertragsverhältnisses mit einem durch die KUNDIN zu benennenden Dritten nach Weisung der KUNDIN in zumutbarem Umfang zusammenzuarbeiten. Diese Zusammenarbeit ist gesondert nach Aufwand zu vergüten. Die Vergütung erfolgt zu den im Zeitpunkt der Beendigung des Vertrages geltenden allgemeinen Stunden- bzw. Tagessätzen der ANBIETERIN. Zusätzlich hat die KUNDIN der ANBIETERIN sämtliche angefallenen erforderlichen und nachgewiesenen Aufwendungen zu ersetzen. Diese Zusammenarbeit ist beschränkt auf
   a. die Übermittlung der von der KUNDIN gespeicherten ANWENDUNGSDATEN,
   b. die Übermittlung sonstiger die KUNDIN betreffenden Daten, soweit es sich nicht um Geschäftsgeheimnisse handelt.

§ 14 Höhere Gewalt

Keiner der Vertragspartner ist zur Erfüllung der vertraglichen Verpflichtungen im Fall und für die Dauer höherer Gewalt verpflichtet. Insbesondere folgende Umstände sind als höhere Gewalt in diesem Sinne anzusehen:
Von dem Vertragspartner nicht zu vertretende(s)

- Feuer, Explosion, Überschwemmung,
- Krieg, Meuterei, Blockade, Embargo,
- über 6 Wochen andauernder und von dem Vertragspartner nicht schuldhaft herbeigeführter Arbeitskampf,
- nicht von einem Vertragspartner beeinflussbare technische Probleme des Internets; dies gilt nicht, sofern und soweit die ANBIETERIN die Telekommunikationsleistung mit anbietet,
- Endemien und Pandemien.

Jeder Vertragspartner hat den anderen über den Eintritt eines Falls höherer Gewalt unverzüglich in Textform in Kenntnis zu setzen.

§ 15 Risikomanagement

Die ANBIETERIN betreibt aktives Risikomanagement. Dabei werden regulatorische Anforderungen eingehalten, die aufgrund der Zugehörigkeit zu einem Bankenkonzern Anwendung auf die ANBIETERIN finden. Dabei liegt besonderer Fokus auf den branchenüblichen Anforderungen an das operationelle - und IT-Risikomanagement. Teil der Maßnahmen, um diesen Anforderungen gerecht zu werden, sind die folgenden.

a. Schulung des Personals zur Identifikation, Meldung und Umgang mit Risiken
b. Risk Assessments
c. Audits- Implementierung von Kontrollmechanismen- Unabhängige Überwachung aller implementierten Maßnahmen
d. Jährliche Erstellung eines Risikoberichts

§ 16 IT-Security und Update Konzept

(1) Für den IT-Betrieb hat die ANBIETERIN eine ausgearbeitete und gültige IT-Strategie. Diese wurde abgeleitet aus der allgemeinen Geschäftsstrategie und werden sowohl regelmäßig sowie nach Bedarf anhand eines definierten Prozesses aktualisiert, abgestimmt und kommuniziert.

(2) Ein Informationssicherheitsbeauftragter wurde benannt, der über security@interhyp.de kontaktiert werden kann.

(3) Mitarbeitende der ANBIETERIN werden initial beim Onboarding sowie regelmäßig (mindestens einmal jährlich) bzgl. allgemeiner IT-Themen, vorwiegend bzgl. IT-Sicherheit sowie Datenschutz, geschult. Die Teilnahme ist für alle Mitarbeitenden verpflichtend.

(4) Der Betrieb der IT-Services wurde vom TÜV SÜD nach den Normen ISO/IEC 20000-1 (Zertifikat-Registrier-Nr.: 12 410 35042 TMS) und ISO/IEC 27001 (Zertifikat-Registrier-Nr.: 12 310 49897 TMS) zertifiziert.

(5) Die folgenden Maßnahmen und Prozesse sind Teil des Katalogs, mit dem die ANBIETERIN die IT-Security sicherstellt:
   a. Die ANBIETERIN pflegt sämtliche relevante Systeme in einer zentralen Configuration Management Database (CMDB), die als Dreh- und Angelpunkt für die effiziente Verwaltung und Aktualisierung dieser Systeme dient. Die CMDB ermöglicht eine umfassende Dokumentation der Systemkonfigurationen und deren Veränderungen im Laufe der Zeit, was eine transparente und konsistente Systemverwaltung gewährleistet. Auf diese Weise wird eine zuverlässige Nachverfolgung von Systemänderungen und eine schnellere Fehlerbehebung ermöglicht.
   b. Um die Sicherheit der Systeme zu gewährleisten, führt die ANBIETERIN regelmäßig Schutzbedarfsanalysen für alle relevanten Systeme durch. Diese Analysen berücksichtigen die sich ständig ändernden Anforderungen an den Schutz der Informationen und gewährleisten eine angemessene Anpassung der Sicherheitsmaßnahmen. Die Ergebnisse dieser Analysen bilden die Grundlage für die Implementierung zielgerichteter Sicherheitsmaßnahmen, um potenzielle Risiken zu minimieren.
   c. Die ANBIETERIN hat umfassende Security Prozesse definiert und implementiert, die sicherstellen, dass Sicherheitsaspekte in sämtlichen Aspekten des IT-Betriebs berücksichtigt werden. Dies umfasst die Identifizierung und Bewertung von Bedrohungen, die Umsetzung von Sicherheitsrichtlinien und -verfahren, die Schulung des Personals in Sicherheitsbewusstsein und die Bereitstellung eines klaren Rahmens für die Reaktion auf Sicherheitsvorfälle. Die Implementierung solcher Prozesse fördert die Integration von Sicherheit in den gesamten IT-Betrieb und trägt dazu bei, potenzielle Schwachstellen frühzeitig zu identifizieren und zu beheben.
   d. Die ANBIETERIN gewährleistet die regelmäßige Durchführung von Schwachstellenscans und das entsprechende Patchen aller relevanten Systeme. Diese Maßnahme dient dazu, potenzielle Schwachstellen in der IT-Infrastruktur zu identifizieren und schnell zu beheben, um die Sicherheit und Stabilität der Systeme zu gewährleisten. Durch diese proaktive Vorgehensweise wird das Risiko von Sicherheitsverletzungen minimiert.
   e. Vor jedem Deployment in die Produktionsumgebung wird der Softwarecode auf Schwachstellen gescannt. Diese Überprüfung stellt sicher, dass keine Sicherheitslücken in der bereitgestellten Software vorhanden sind, und trägt zur Vermeidung von Sicherheitsverletzungen bei, die durch fehlerhaften Code verursacht werden könnten.

f. Container werden regelmäßig auf Schwachstellen gescannt, um sicherzustellen, dass auch in diesen isolierten Umgebungen keine Sicherheitsrisiken bestehen. Durch diese Maßnahme wird das Risiko von Angriffen auf Container-basierte Anwendungen minimiert.
g. Relevante Systeme werden anlassbezogen auf Malware überprüft, um sicherzustellen, dass sie frei von schädlicher Software sind. Diese Prüfungen sind wichtig, um unautorisierte Aktivitäten zu erkennen und zu unterbinden.
h. Systeme werden anhand definierter Security Baselines gehärtet und regelmäßig auf die Einhaltung der Sollkonfiguration überprüft. Dies gewährleistet, dass die Systeme in einem sicheren Zustand bleiben und nicht durch unerwünschte Konfigurationsänderungen gefährdet werden.
i. Die ANBIETERIN hat Security Monitoring für alle relevanten Systeme eingerichtet, um verdächtige Aktivitäten in Echtzeit zu erkennen. Dies ermöglicht eine schnelle Reaktion auf potenzielle Sicherheitsvorfälle und trägt zur Früherkennung von Bedrohungen bei.
j. Abhängig von ihrem Schutzbedarf werden Systeme regelmäßig Penetrationstests ausgesetzt. Diese Tests simulieren Angriffsversuche und helfen dabei, Schwachstellen aufzudecken und zu beseitigen, um die Sicherheit der Systeme zu erhöhen.
k. Die ANBIETERIN hat einen umfassenden Security Incident Prozess definiert und implementiert, der sicherstellt, dass bei Sicherheitsvorfällen effektiv und koordiniert gehandelt wird. Die unterstützenden Runbooks bieten klare Handlungsanleitungen für das Incident-Management-Team.
l. Ein zentrales Identity and Access Management-System wurde eingerichtet, um die Verwaltung von Benutzeridentitäten und Zugriffsrechten zu zentralisieren. Dies trägt zur effizienten und sicheren Verwaltung von Zugriffen bei.
m. Für alle relevanten Systeme sind detaillierte Berechtigungskonzepte definiert, die die Steuerung des Zugriffs auf sensible Daten und Ressourcen ermöglichen.
n. Rechte werden gemäß den Prinzipien Need to Know und Least Privilege vergeben, um sicherzustellen, dass Benutzer nur die Berechtigungen erhalten, die sie für ihre Aufgaben benötigen, und keine überflüssigen Zugriffsrechte haben.
o. Die Führungskräfte überprüfen zweimal jährlich die vergebenen Rechte, um sicherzustellen, dass sie immer noch den aktuellen Anforderungen und der Sicherheitsrichtlinie entsprechen.
p. Aktuelle Virenscanner sind im Einsatz, um sicherzustellen, dass schädliche Software frühzeitig erkannt und blockiert wird. Dies ist ein wichtiger Bestandteil des Schutzes vor Viren und Malware.

§ 17 Schlussbestimmungen

(1) Auf das vorliegende Vertragsverhältnis findet deutsches Recht unter Ausschluss des UN-Kaufrechts Anwendung.

(2) Die Anhänge sind Bestandteil dieses Vertrags. Im Übrigen gelten die Bestimmungen des Hauptvertrages.

(3) Änderungen oder Ergänzungen dieses Vertrags und der Anhänge bedürfen der zu ihrer Wirksamkeit der elektronischen Form. Dies gilt auch für die Abbedingung des Formerfordernisses.

(4) Die etwaige Unwirksamkeit einzelner Bestimmungen dieses Vertrags beeinträchtigt nicht die Gültigkeit des übrigen Vertragsinhalts.

(5) Ergeben sich in der praktischen Anwendung dieses Vertrags Lücken, die die Vertragspartner nicht vorgesehen haben, oder wird die Unwirksamkeit einer Regelung rechtskräftig oder von beiden Vertragspartnern übereinstimmend festgestellt, so verpflichten sie sich, diese Lücke oder unwirksame Regelung in sachlicher, am wirtschaftlichen Zweck des Vertrages orientierter angemessener Weise auszufüllen bzw. zu ersetzen.

(6) Ausschließlicher Gerichtsstand für Streitigkeiten aus oder über den vorliegenden Vertrag ist, sofern nicht eine Norm zwingend einen anderen Gerichtsstand anordnet, entsprechend § 17 ZPO am Sitz des Klägers.

Anhang 1

Leistungsbeschreibung ehyp home

Inhalt

1 Leistungsumfang

1.1 Präambel

Die ANBIETERIN stellt der KUNDIN die ANWENDUNG (=technische Plattform) zur Verfügung, die die Erfassung, Prüfung und Verarbeitung von Daten im Rahmen der Baufinanzierung unterstützt. Die Nutzung erfolgt über eine browserbasierte Benutzeroberfläche sowie gegebenenfalls über Programmschnittstellen (APIs).

1.2 Enthaltene Feature Sets

Die ANWENDUNG stellt alle zwingend elementar zur Erfüllung der vertragsgemäßen Funktion und Nutzung erforderlichen Grundfunktionen zur Verfügung.

Hiermit kann die KUNDIN unter anderem folgende Dinge abbilden:

- **Beratung & Produktabwicklung**
  Die ANWENDUNG stellt Funktionen für Antrags-Initiierung, Produktberatung und Produktabwicklung zur Verfügung, durch die es dem Nutzer ermöglicht wird, seine Kundenvorhaben zu erfassen, passende Finanzierungsvarianten abzubilden und diese zu vergleichen. Für das Kundenvorhaben in Frage kommende Produktanbieter werden mit vorhabens- und anbieterspezifischen Machbarkeitshinweisen und beratungsunterstützenden Produktdetails

dargestellt. Darüber hinaus unterstützt die ANWENDUNG bei der Anbahnung und Prozessierung der notwendigen Schritte bis zur Kreditentscheidung.

- **Vertriebsmanagement**
  Die ANWENDUNG stellt Funktionen zur Vertriebsproduktivität & -steuerung und Kommunikation & Dokumentation zur Verfügung, durch die eine strukturierte Aufgabenorganisation für jeden Nutzer und die Kollaboration zwischen allen Beteiligten ermöglicht wird.

- **Organisationsverwaltung**
  Die ANWENDUNG stellt Funktionen zur Abbildung der Organisations-Hierarchie und den damit verbundenen Einstellungen & Berechtigungen zur Steuerung des Verhaltens der ANWENDUNG, sowie der Administration der anbindbaren technischen Schnittstellen (APIs) zur Verfügung.

2 Incident Management

Im Rahmen des Incident Management beseitigt die ANBIETERIN die von der KUNDIN gemeldeten Störungen beim Betrieb der ANWENDUNG, die während der Laufzeit dieses Anhangs auftreten, nach Maßgabe der folgenden Regelungen.

Eine Störung liegt vor, wenn Einschränkungen bei der Verfügbarkeit der ANWENDUNG bestehen, sie geschuldete Funktionen nicht erfüllt, von der Definition abweichende Ergebnisse liefert, den Lauf unkontrolliert abbricht oder in anderer Weise nicht funktionsgerecht arbeitet, so dass die Nutzung der ANWENDUNG unmöglich oder eingeschränkt ist.

Alle Störungen aus dem laufenden Produktionsbetrieb werden von der KUNDIN an die von der ANBIETERIN benannten, zentralen Ansprechpartner der ANBIETERIN gemeldet.

Die ANBIETERIN verpflichtet sich, vorliegende Störungen zu beheben und alle erforderlichen Maßnahmen zur Wiederherstellung eines ordnungsgemäßen Betriebs zu ergreifen.

3 Service Level Agreement (SLA)

3.1 Übergreifende Regelungen

1) Die ANBIETERIN ist verantwortlich für die vertragsgemäße Erbringung des Leistungsgegenstandes mit der in diesem Service Level Agreement (SLA) vereinbarten Service-Qualität.

2) Die KUNDIN ist zur Prüfung der erbrachten Dienstleistung verpflichtet. Dazu gehören die zeitnahe Überprüfung und gegebenenfalls Reklamation der erbrachten Leistungen, ohne dass die Verpflichtungen der ANBIETERIN zur Erbringung mangelfreier Leistungen

und zur Behebung von Störungen dadurch eingeschränkt werden würde.

3) Die KUNDIN wird die ANBIETERIN, soweit im Rahmen der Mitwirkung geboten, in jeder Hinsicht bei der Erfüllung der vertraglichen Leistungspflichten unterstützen.

4) Bei den definierten Mitwirkungspflichten handelt es sich um wesentliche Vertragspflichten. Hängt eine Leistung der ANBIETERIN von einer Mitwirkungshandlung der KUNDIN ab, ist die ANBIETERIN für Verzögerungen, die aus fehlender oder nicht ordnungsgemäßer Mitwirkung der KUNDIN resultieren, nicht verantwortlich.

3.2 Dienstleistungsgüte

3.2.1 Definitionen

3.2.1.1 Service-Endpunkt

Ein Service-Endpunkt ist ein spezifischer Zugangspunkt zu unserem Dienst, der über eine URL erreichbar ist. Für die Zwecke dieses Vertrages bezieht sich der Service Endpunkt auf die Login-Seite der Anwendung.

3.2.1.2 Verfügbarkeit

Die Verfügbarkeit ist der Prozentsatz der Zeit, in der der Service-Endpunkt gemäß den unten definierten Verfügbarkeitskriterien erreichbar ist.

3.2.1.3 Nutzungszeiten und Wartungsfenster

System-Nutzungszeit	7 Tage x 24 Stunden
Kern-Nutzungszeit	Mo.-Fr. 08:00 – 18:00 Uhr Ausnahme: bundeseinheitliche Feiertage
Wartungsfenster	Mo.-Fr. 18:00 – 08:00 Uhr Sa. 00:00 – 24:00 Uhr Sonntag und bundeseinheitliche Feiertage: 00:00 – 24:00 Uhr

3.2.2 Service Level – Verfügbarkeit

3.2.2.1 Service Level

Die Interhyp Gruppe gewährleistet, dass der Service-Endpunkt eine Verfügbarkeit von mindestens 97,00%/Monat in der Kernnutzungszeit aufweist.

3.2.2.2 Messung der Verfügbarkeit

Die Verfügbarkeit wird durch regelmäßige http-Checks am Service-Endpunkt gemessen. Diese Checks werden von einem Monitoring-System durchgeführt und protokolliert.

3.2.3 Berechnung der Verfügbarkeit

3.2.3.1 Zeitbasis

Die Verfügbarkeit wird auf einer monatlichen Basis berechnet und berichtet.

3.2.3.2 Berechnung

Die Verfügbarkeit wird wie folgt berechnet:

Verfügbarkeit (%)=(1-(Gesamtzeit des Ausfalls während der Kernnutzungszeit/Kernnutzungszeit))x100

Anhang 2

Vertrag

zur

Auftragsverarbeitung

Zwischen

der „KUNDIN“ oder dem „Untervermittler“
Verantwortlicher

– im Folgenden „Auftraggeber“ genannt –

und

Prohyp GmbH
Domagkstraße 34
80807 München

Auftragsverarbeiter

– im Folgenden „Auftragnehmer“ genannt –

– zusammen „Vertragspartner“ genannt –

Präambel
Die Vertragspartner haben einen Vertrag über die Bereitstellung der Plattform ehyp home (im Folgenden „Plattformnutzungsvertrag“) abgeschlossen, auf dessen Basis der Auftragnehmer Daten für den Auftraggeber bearbeitet. In dessen Rahmen erhält der Auftragnehmer von dem Auftraggeber personenbezogene Daten. Um die Bedingungen der Datenverarbeitung zu regeln, schließen die Vertragspartner folgende Vereinbarung:

§ 1 Gegenstand des Auftrages

1.1 Der Auftragnehmer erhebt, verarbeitet oder nutzt personenbezogene Daten im Auftrag des Auftraggebers.

1.2 Der Gegenstand des Auftrages ist die Nutzung der Plattform der Interhyp („eHyp Home“) zur Vermittlung von Immobilienfinanzierungen.

Die Einzelheiten zum genauen Leistungsgegenstand, insbesondere im Hinblick auf Umfang, Art, Zweck und Dauer des Auftrages, ergeben sich aus dem Plattformnutzungsvertrag. Der Plattformnutzungsvertrag, dessen Anlagen und dieser Vertrag werden im Folgenden zusammen „Vereinbarung“ genannt.

1.3 Die Art der Daten ergibt sich aus **Anlage 1**. Der Kreis der Betroffenen umfasst Kunden, Interessenten und Mitarbeiter.

1.4 Eine Datenübermittlung an Stellen in Staaten außerhalb der Europäischen Union (sogenannte Drittstaaten) findet lediglich statt, wenn die besonderen Voraussetzungen der Artikel 44 ff. DSGVO erfüllt sind. Ein angemessenes Schutzniveau wird sichergestellt durch jeweils aktuelle Standardvertragsklauseln nach Artikel 46 Abs. 2 litt. c und d DSGVO sowie durch Berücksichtigung von Angemessenheitsbeschlüssen der Europäischen Kommission nach Artikel 45 Abs. 3 DSGVO.

§ 2 Rechte und Pflichten des Auftraggebers

2.1 Für die Zulässigkeit der Datenerhebung, Datenverarbeitung und Datennutzung im Rahmen der Vereinbarung sowie für die Wahrung der Rechte der Betroffenen ist der Auftraggeber alleinverantwortlich. Es obliegt dem Auftraggeber eigenverantwortlich, die Betroffenen darauf hinzuweisen, dass ihre Daten erhoben, verarbeitet und genutzt werden und zu welchem Zweck dies erfolgt. Der Auftraggeber wird dafür Sorge tragen, dass die Betroffenen auf etwaige Widerrufsmöglichkeiten hingewiesen werden.

2.2 Der Auftraggeber hat das Recht, schriftlich oder in Textform Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen.

2.3 Der Auftraggeber teilt dem Auftragnehmer unter Angabe von Name, Organisationseinheit, Funktion und Telefonnummer die Personen mit, die gegenüber dem Auftragnehmer weisungsberechtigt sind oder als Ansprechpartner fungieren. Änderungen werden dem Auftragnehmer unverzüglich in Textform mitgeteilt.

§ 3 Kontrollrechte des Auftraggebers

Der Auftragnehmer räumt dem Auftraggeber bzw. deren Datenschutzbeauftragten oder Prüfern, die bei dem Auftraggeber aufgrund gesetzlicher Vorschriften tätig werden, nach rechtzeitiger

Anmeldung, mindestens jedoch 30 Werktage, ein Auskunfts-, Einsichts- und Prüfungsrecht bezüglich der für den Auftraggeber erbrachten Leistungen ein. Auf Verlangen des Auftraggebers wird der Auftragnehmer den Auftraggeber im Rahmen von vorgenannten Prüfungen in angemessenen Umfang unterstützen, wenn und soweit die vertragsgegenständliche Verarbeitung von Daten des Auftraggebers Gegenstand des Aufsichtsverfahrens ist. Bei dem Zugang und der Prüfung hat der Auftraggeber angemessene Rücksicht auf die Betriebsabläufe und berechtigte Geheimhaltungsinteressen des Auftragnehmers zu nehmen. Als Nachweis für die Einhaltung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 DS-GVO kann der Auftragnehmer, auch aktuelle, aussagekräftige Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren),

§ 4 Rechte und Pflichten des Auftragnehmers

4.1 Der Auftragnehmer und das von ihm zur Leistungserbringung eingesetzte Personal verarbeitet personenbezogene Daten ausschließlich im Rahmen der Vereinbarung.

4.2 Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke als die vertraglich vereinbarten, sofern er nicht durch das Recht der EU oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist.

4.3 Der Auftragnehmer wird dem Auftraggeber unverzüglich in Textform (z.B. per Email) informieren, wenn eine von dem Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis der Auftraggeber die rechtliche Zulässigkeit bestätigt hat.

4.4 Der Auftragnehmer ist verpflichtet, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte nachzukommen.

4.5

4.6 Der Auftragnehmer wird den Auftraggeber informieren, wenn der Auftragnehmer der Meinung ist, es liegt ein datenschutzrechtlicher Verstoß vor.

4.7 Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zu unterstützen.

4.8 Der Auftragnehmer ist verpflichtet, auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung seiner und der Aufgaben des Auftraggebers zusammenzuarbeiten.

§ 5 Berichtigung, Einschränkung und Löschung von Daten

5.1 Der Auftragnehmer legt dem Auftraggeber das Lösch- und Sperrkonzept in der **Anlage 2** für die Plattform „eHyp Home“ vor.

Der Auftraggeber erklärt sich mit dem Lösch- und Sperrkonzept des Auftragnehmers einverstanden.

5.2 Nach Abschluss der jeweiligen vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber, hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellten Verarbeitungs- oder Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, gemäß dem in Anlage 3 aufgeführten Lösch- und

Sperrkonzeptzu sperren oder zu löschen, sofern keine gesetzlichen Aufbewahrungsfristen des Auftragnehmers entgegenstehen.

5.3 Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten oder sonstiger datenschutzrechtlicher Belange wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber zur Bearbeitung weiterleiten

§ 6 Beauftragung von Subunternehmen

6.1 Subunternehmer, deren Einsatz zur Durchführung des vereinbarten Auftrages als Unterauftragnehmer bei Abschluss der Vereinbarung bereits durch den Auftraggeber genehmigt sind, werden in der **Anlage 3** benannt.

6.2 Nicht als Subunternehmern im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Softwareentwicklungs- und Beratungsleistungen, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene Vereinbarungen zu treffen.

§ 7 Datenschutzbeauftragter des Auftragnehmers

Der Auftragnehmer hat

Data Protection Office
Interhyp AG
Telefon: 089 20307-1400
E-Mail: datenschutz@interhyp.de

als zentrale Anlaufstelle für den Datenschutz und den/die Datenschutzbeauftrage/n eingerichtet.

§ 8 Datengeheimnis

8.1 Der Auftragnehmer verpflichtet sich, vor der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die zur Verarbeitung der personenbezogenen Daten befugten Personen auf die Wahrung der Vertraulichkeit verpflichtet zu haben.

8.2 Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht.. und diese überwacht.

8.3

§ 9 Sicherheit der Verarbeitung nach Artikel 32 DS-GVO

9.1 Der Auftragnehmer ist verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

In diesem Sinne ist der Auftragnehmer verpflichtet, die in **Anlage 4** dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung und während der gesamten Vertragslaufzeit einzuhalten.

9.2 Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

9.3 Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung durch den Auftragnehmer angepasst werden.

§ 10 Vertragsdauer

10.1 Dieser Vertrag tritt mit seiner Unterzeichnung in Kraft. Die Dauer dieses Auftrages (Laufzeit) entspricht der Laufzeit des zwischen den Vertragspartnern geschlossenen Plattformnutzungsvertrages. Wird der Plattformnutzungsvertrag gekündigt, endet auch dieser Vertrag zur Auftragsverarbeitung automatisch, ohne dass es einer gesonderten Kündigung bedarf. Das Datengeheimnis besteht auch nach Beendigung dieses Vertrages, gleich aus welchem Rechtsgrund, fort.

10.2 Der Auftraggeber kann diesen Vertrag zur Auftragsverarbeitung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieses Vertrages vorliegt In diesem Fall liegt gleichzeitig ein außerordentlicher Kündigungsgrund für den Plattformnutzungsvertrag vor.

10.3 Im Übrigen bleiben die Regelungen zur außerordentlichen Kündigung des Plattformnutzungsvertrages unberührt.

§ 11 Haftung

Es gelten bezüglich der Haftung die Haftungsregelungen aus dem Plattformnutzungsvertrag. Sollten keine Haftungsregelungen im Plattformnutzungsvertrag vereinbart worden sein, so gelten im Übrigen die gesetzlichen Bestimmungen zur Haftung.

§ 12 Sonstiges

12.1 Im Falle von Widersprüchen zwischen dem Plattformnutzungsvertrag und diesem Vertrag gehen die Bestimmungen dieses Vertrages vor. Dieser Vertrag ersetzt mit Unterzeichnung alle

gegebenenfalls bestehenden früheren Vereinbarungen oder entsprechende Anlagen zu früheren Vereinbarungen.

Die Vertragspartner sind sich einig, dass das vorliegende Vertragsverhältnis zur Auftragsverarbeitung lediglich die Leistungen aus dem Plattformnutzungsvertrag erfasst. Andere Bereiche der Zusammenarbeit der Vertragspartner, insbesondere die Vermittlung von Immobiliar- und/oder Allgemeinverbraucherdarlehen und/oder Bausparverträge sind nach einhelliger Auffassung der Vertragspartner kein Bestandteil dieses Vertrages zur Auftragsverarbeitung.

12.2 Änderungen und Ergänzungen dieses Vertrages bedürfen zu ihrer Wirksamkeit der Schriftform. Das Schriftformerfordernis gilt auch für die Aufhebung des Schriftformerfordernisses selbst.

12.3 Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag, insbesondere über seinen Bestand und seine Erfüllung, ist München.

12.4 Sollten einzelne Bestimmungen dieses Vertrages nichtig oder unwirksam sein oder werden, so bleiben der Vertrag als Ganzes und die übrigen Bestimmungen davon unberührt. An die Stelle nichtiger oder unwirksamer Bestimmungen treten die gesetzlichen. Dies gilt ebenso im Falle von Regelungslücken. Im Falle von Gesetzeslücken tritt an ihre Stelle die Regelung, die die Vertragspartner bei sachgerechter Abwägung der beiderseitigen Interessen gewählt hätten, wenn ihnen das Fehlen der Regelung bewusst gewesen wäre.

Anlagen:

Anlage 1 - Art der Daten
Anlage 2 – Sperr- und Löschkonzept
Anlage 3 – Genehmigte Subunternehmerliste
Anlage 4 - Technische und organisatorische Maßnahmen

Anlage 1:

Sperr- und Löschkonzept (PDF beigefügt)

Konzept zur automatischen Regellöschung

Allgemeine Informationen

Zeitpunkt der Löschung	• Die automatische Regellöschung erfolgt immer zum **Stichtag 31. Dezember** eines Jahres.
Details zur Umsetzung	• Die Aufbewahrungsfrist wird für **jeden Antrag separat** betrachtet und bei Kunden mit ggf. mehreren Anträgen wird jeder Antrag entsprechend des jeweiligen Auslösungszeitpunktes einzeln gelöscht. • Die **personenbezogenen Datenfelder** werden entsprechend einer Feldliste **anonymisiert** und unwiderruflich überschrieben. • Zum weiteren **Schutz der Kundendaten** (während der Aufbewahrungsfrist) werden die Anträge nach 2 Jahren zum Monatsende (Abschlussdatum, Abbruchdatum oder Erstellungsdatum bei aktiven Anträgen) für Prohyp gesperrt. Der Vermittler hat die Möglichkeit einen gesperrten Antrag für die Prohyp-Mitarbeiter zu entsperren. Nach Entsperrung wird der Antrag nach 2 Monaten erneut gesperrt. Die Entsperrung wird im Logbuch dokumentiert. • Vor der bevorstehenden Löschung hat der Partner die Möglichkeit einen **Datenexport** (Report Antragsdaten in den eHyp-Reports) durchzuführen. Dokumente müssen ggf. separat über den Unterlagenmanager exportiert werden. Der Master-Vermittler erhält dazu eine Vorankündigung per E-Mail.
Aufbewahrungsfristen	• Aufbewahrungsfrist von 6 Jahren für Kommunikationsdaten als Handelsbriefe (§ 257 I Nr. 2, 3 HGB und § 147 I Nr. 2, 3 AO) • Aufbewahrungsfrist von bis zu 10 Jahren für Antragsdaten zur Geltendmachung, Ausübung oder Verteidigung von/gegen Rechtsansprüchen (§ 257 Abs. 4 i.V.m. Abs. 1 Nr. 2, 3 HGB und § 147 Abs. 3 S. 1 i.V.m. Abs. 1 Nr. 2, 3 AO)

Konzept zur automatischen Regellöschung

Löschfristen für eHyp Kundendaten

Antragsstatus	Auslösungs-zeitpunkt	Löschzeitpunkt	Begründung der Aufbewahrungsfrist
Abgebrochene Anträge *('technischer Status=Abbruch)*	Abbruchdatum	6 Jahre nach Auslösungszeitpunkt	• **Ein Großteil aller Beschwerdefällen** erreichen Prohyp und Prohyp-Partner nach 3 Jahren. • Kommunikationsdaten aus dem Logbuch qualifizieren wir als **Handelsbriefe**, so dass diese bereits einer **gesetzlichen Aufbewahrungsfrist von 6 Jahren** unterliegen (§ 257 I Nr. 2, 3 HGB und § 147 I Nr. 2, 3 AO). Aufgrund der Komplexität der Haftungsfälle erstrecken wir die **6 jährige Aufbewahrungsfrist auf alle Daten** (einschl. personenbezogenen Antragsdaten und Dokumente).
Abgeschlossene Anträge *('technischer Status=E-Fax)*	Abschlussdatum (E-Fax)	10 Jahre nach Auslösungszeitpunkt	• **Beschwerden**, die die Prohyp und Prohyp-Partner nach 6 Jahren erreichen, betreffen nur **abgeschlossene** Anträge. • Auswertungen der Beschwerdefälle haben eine **steigenden Tendenz von Haftungsfällen**, sowohl in der Anzahl als auch im Haftungsvolumen, ergeben. • Wir erfüllen gleichzeitig das **Interesse unserer Partner** sich auch nach 6-Jahren gegen Haftungsansprüche von Kunden verteidigen zu können. • Alle abgeschlossenen (und abgebrochenen) Anträge werden nach **2 Jahren für Prohyp-Mitarbeiter gesperrt.** Partner haben weiterhin Zugriff auf diese Anträge und können im Einzelfall die Sperrung aufheben. • Die Entwicklung des Haftungsrisikos und ggf. Anpassung der Fristen unterliegen einem regelmäßigen **Review**.
Aktive Anträge *(alle Anträge, die angelegt wurden und weder abgebrochen noch abgeschlossen sind)*	Antragserstellung	6 Jahre nach Auslösungszeitpunkt	• Aktive Anträge stehen im Zusammenhang mit einer **aktiven Beratung des Kunden**. Prinzipiell greift für aktive Anträge somit eigentlich noch keine Aufbewahrungsfrist, da der Vermittlungszweck noch besteht. • Sofern die aktiven Anträge nach 6 Jahren noch nicht abgebrochen oder abgeschlossen werden, wird der Antrag trotz des „aktiven Status" der Regellöschung zugeführt. Diese Maßnahme dient der **Vermeidung einer dauerhaften Speicherung von Kundendaten.**

Anlage 2:
Art der Daten

Stammdaten

- **Personendaten**
- Anrede
- Titel
- Vorname(n)
- Nachname(n)
- Geburtsdatum
- Geburtsort
- Geschlecht
- Staatsangehörigkeit(en)
- Familienstand
- Anzahl Kinder
- **Einkommensdaten**
- Arbeitgeber (Name und Adresse)
- Berufliche Stellung/Funktion im Unternehmen/Abteilung/Bereich
- Branche des Arbeitgebers/Unternehmensbereichs/Berufsfeldes/Tätigkeitsfeldes

Anlage 3:
Genehmigte Subunternehmerliste

Microsoft Azure

Anlage 4:
Technische und organisatorische Maßnahmen

(1) Schutzmaßnahmen der **Zutrittskontrolle:**

Der Auftragnehmer hat die räumliche Annäherung an eine Datenverarbeitungsanlage (DVA) mit Serverfunktion (Server) geregelt. Hierbei wurde festgelegt, welche Personengruppen Zutritt zu der DVA haben. Die Zuordnung der Befugnisse nach Personen wird aufgezeichnet und aufbewahrt.

Zum Schutz von unzulässigen Eingriffen auf den Server durch unberechtigte Personen sind folgende Maßnahmen umgesetzt:

OnPrem Rechenzentren

1. Die Interhyp IT gewährt nur einem speziell geschulten Personenkreis Zutritt in die Rechenzentren nach dem „need to know“ Prinzip. Das Wachpersonal der Rechenzentren erhält jeweils eine Zutrittsliste mit berechtigten Personen der Interhyp IT. Das Wachpersonal führt jeweils eine Identitätsfeststellung anhand eines Lichtbildausweises durch. Erst nach erfolgreicher Ausweisung, wird den zutrittsberechtigten Mitarbeitenden eine Karte für den Zutritt zu den Serverräumen übergeben. Ein Textprotokoll über den Zutritt wird vom Wachpersonal geführt.

2. Für den Zugriff auf die jeweiligen Serverschränke ist die Eingabe eines Usernamens und Passwortes notwendig. Die Serverschränke werden daraufhin elektronisch entriegelt. Nur berechtigte Mitarbeitende haben Zugriff auf die jeweiligen Schränke nach dem „need to know“ Prinzip. Eine Protokollierung der Schranköffnung findet im System statt.

3. Der Zugang zum Rechenzentrum ist durch Durchfahrtssperren und Wachpersonal (24 Stunden/ Tag) besonders gesichert.

4. Eine visuelle Zutrittsüberwachung erfolgt sowohl durch den bemannten Empfangsbereich wie auch durch Kameras in den sensiblen Teilen der Rechenzentren.

Cloud Rechenzentren

Die Cloud Rechenzentren werden von Microsoft Azure gehostet. Unsere Daten werden ausschließlich in Europa verwaltet. Vertraglich wurden ausreichende Zutrittsschutzmaßnahmen vereinbart, um ebenfalls in diesen Rechenzentren den Schutz vor unzulässigen Eingriffen auf unsere Daten zu gewährleisten.

Hauptgebäude München

1. Am Hauptgebäude in München ist der Zutritt für berechtigte Mitarbeitende nur mit Magnetkarten möglich. Diese werden den Mitarbeitenden nach Identitätsfeststellung am ersten Arbeitstag ausgehändigt. Am Ende des Beschäftigungsverhältnisses werden diese wieder zurückgegeben. Die Eingänge sind mittels Videoüberwachung abgesichert und mit Speedgates ausgestattet, das nur nach erfolgreicher Authentifizierung mit der Magnetkarte passiert werden kann.

2. Ein Wachdienst überprüft das Gebäude auch außerhalb der Geschäftszeiten auf unberechtigte Personen. Berechtigte Personen - wie IT-Bereitschaftsdienst – werden dem Wachdienst von der Interhyp Abteilung Facility Management gemeldet.

3. Eine Alarmanlage sichert die Büro Etagen. Bei einer Einbruchserkennung wird automatisch der Wachdienst alarmiert. Der Freischaltcode der Alarmanlage ist nach dem

„need to know“ Prinzip nur berechtigen Mitarbeitenden bekannt (z.B. Bereitschaftsdienst).

Niederlassungen

IT-Räume in den Niederlassungen der Interhyp sind von den Büroräumen der Mitarbeitenden separiert und mit einem Sicherheitsschloss versehen. Die Serverschränke in den IT-Räumen sind mit einem Rack Schließsystem gesichert.

(2) Schutzmaßnahmen der **Zugangskontrolle:**

Der Auftragnehmer hat sichergestellt, dass nur befugte Personen die Möglichkeit haben, sich an der DVA (OnPrem & Cloud) anzumelden und damit Zugang zu den Daten zu erlangen. Die Anmeldung erfolgt über ein individuelles Benutzerkonto mittels Benutzernamen und Passwort. Alle Kontoänderungsaktivitäten werden protokolliert. Bei der Vergabe von Zugangsberechtigungen wird Folgendes eingehalten:

1. Keine Wiederverwendung der letzten 20 Passwörter.
2. Änderung nach spätestens 180 Tagen.
3. Insgesamt mindestens 10 Zeichen.
4. Drei der folgenden Kriterien müssen erfüllt sein:
   - Mindestens 1 Sonderzeichen
   - Mindestens 1 Großbuchstabe
   - Mindestens 1 Kleinbuchstabe
   - Mindestens 1 Ziffer
5. Bei initialen vom First Level Support bzw. vom Hersteller ausgegebenen Passwörtern ist eine Änderung beim ersten Login nötig.
6. Keine bloße Verwendung von Wörterbuchwörtern oder sich wiederholenden Zeichen- oder Wortfolgen.
7. Keine Wiederholung des Benutzernamens.
8. Fehlerhafte Eingabe eines Kennwortes führt nach drei Fehlversuchen zur Sperrung des bezogenen Benutzerkontos.
9. Benutzerkonten, die unbegründet länger als 180 Tage nicht in Benutzung sind, werden gelöscht.
10. Bei eventuellem ungewolltem Bekanntwerden eines Passwortes wird dieses umgehend geändert.
11. Nutzerkennungen, d. h. Nutzername und Passwort, sind an den individuellen Nutzer gebunden und dürfen nicht an Dritte weitergegeben werden.
12. Kennwörter werden niemals unverschlüsselt dargestellt oder gespeichert, ein ausgedrucktes Initialkennwort für neue Mitarbeitende wird umgehend geändert.
13. Der Auftragnehmer belehrt seine Mitarbeitende über den Umgang mit Kennwörtern entsprechend.
14. Alle Endgeräte, welche für die Verarbeitung von personenbezogenen Daten genutzt werden, sind mit einer Full-Disk-Encryption ausgestattet.

In **Cloud Rechenzentren** haben Mitarbeitende von Microsoft grundsätzlich keinen Zugang auf den Interhyp Azure Tenant.
Zugangsberechtigungen werden nur im Supportfall und nach ausdrücklicher Initiierung der Interhyp genehmigt. Um dies sicherzustellen, haben wir hier ein Non Disclosure Agreement (NDA) mit Microsoft abgeschlossen.

(3) Schutzmaßnahmen der **Zugriffskontrolle:**

Der Auftragnehmer hat sichergestellt, dass die Verarbeitung und Nutzung personenbezogener Daten auf die vertraglich festgelegten Aufgaben beschränkt ist. Hierzu hat der Auftragnehmer ein Rollen- und Rechtekonzept implementiert. Personenbezogene Daten werden in allen Phasen von Erhebung über Verarbeitung bis hin zur Nutzung sowie Speicherung so geschützt, dass Unbefugte sie weder lesen, kopieren, verändern noch entfernen können.

Die Vergabe von Zugriffsberechtigungen über das Rollen- und Rechtekonzept wird protokolliert.

Zugriffsberechtigungen werden von den jeweiligen Führungskräften halbjährlich auf deren Aktualität geprüft und ggf. angepasst oder entfernt.

(4) Schutzmaßnahmen der **Weitergabekontrolle:**

Personenbezogene Daten werden bei der elektronischen Übertragung oder während ihres Transports so gesichert, dass sie nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Insbesondere bei der Übertragung wird die Vertraulichkeit und Integrität der personenbezogenen Daten durch eine adäquate Verschlüsselung sichergestellt; die angewandten Verschlüsselungsalgorithmen entsprechen dem aktuellen technischen Stand.

Zu Geschäftspartnern unterhält die Interhyp ein eigenes VPN-Netzwerk, das per IPSEC Verschlüsselung eine zusätzliche Vertraulichkeit sicherstellt.
Die Authentizität der externen Anwendungsserver wird durch offiziell ausgestellte Zertifikate sichergestellt.

(5) Schutzmaßnahmen der **Eingabekontrolle:**

Sämtliche zu protokollierende Benutzer- und Systemaktivitäten werden so aufgezeichnet, dass nachträglich überprüft und festgestellt werden kann, ob, von wem und zu welcher Zeit personenbezogene Daten eingegeben, verändert oder entfernt wurden. Dies wird durch Historisierung der personenbezogenen Daten durch die genaue Angabe der Zeit und ausführenden Person sichergestellt.

(6) Schutzmaßnahmen der **Verfügbarkeitskontrolle:**

Der Auftragnehmer gewährleistet die Verfügbarkeit personenbezogener Daten. Hierzu werden die Daten wie folgt geschützt:

Alle Daten des Auftraggebers sind an zwei physikalisch unterschiedlichen Standorten vorhanden. Dies gewährleistet der Auftragnehmer durch die Auslagerung der Backupmedien an einen anderen Standort als im Hause des Auftragnehmers.
Dieses Datensicherungskonzept sieht entweder ein tägliches inkrementelles Backup sowie einmal pro Monat ein vollständiges Backup oder ein kontinuierliches Backup vor (jeweils auf Festplatten) (online/onsite).
Dadurch ist eine rasche Wiederherstellbarkeit der personenbezogenen Daten gewährleistet.
Das Backup wird nachgelagert auf ein verschlüsseltes, separates Medium übertragen (auf Band). Der Aufbewahrungsort befindet sich an einem anderen Standort als in den Rechenzentren des Auftragnehmers. Die Backupmedien sind dort in einem feuerfesten Tresor oder Schrank gelagert (offline/offsite).

Die Systeme des Auftragnehmers, welche personenbezogene Daten verarbeiten, sind mittels eines mehrstufigen Firewallkonzepts sowie einer vollumfänglichen Virenschutzlösung gegen Datenverlust abgesichert.

Die DVA (OnPrem & Cloud) sind über redundante Stromversorgung abgesichert und stellen im Falle eines vollständigen Verlustes der Einspeisung durch das Stromnetz den Betrieb über Notstromaggregate sicher.

Für potentiell auftretende technische Ausfälle wird die Verfügbarkeit der Systeme, welche personenbezogene Daten verarbeiten, durchgehend überwacht und nachgelagert mittels Notfallplänen/Wiederanlaufplänen abgesichert.

In der Cloud wird eine Three Lines of Defense Backup Strategie angewendet.

In der First Line werden Azure native Funktionen verwendet, wie bspw. regionsübergreifende Replikation, Soft-Deletion, Versionierung, Snapshots und Management Locks.
In der Second Line werden zusätzlich Backups und Replikationen auf separaten standby Instanzen gespeichert.
In der Third Line werden bei Bedarf verschlüsselte Backups bei externen (non Azure) Einrichtungen gesichert.

Im Fall eines Austritts aus der Azure Cloud ist eine Exitstrategie ausgearbeitet und anwendbar.

(7) Schutzmaßnahmen der **Trennungskontrolle:**

Der Auftragnehmer hat sichergestellt, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden. Hierzu ist die DVA (OnPrem & Cloud), auf der die Daten des Auftraggebers verarbeitet werden, von anderen Systemen abgeschottet.
Darüber hinaus hat der Auftragnehmer Virenschutzmaßnahmen, ein Firewallkonzept, Patch-Management, Netzwerkmanagement sowie eine Notfallplanung implementiert.

Folgende Systeme sind eingerichtet:

1. Application Layer Firewall

2. Intrusion Detection System

3. Virenschutzsystem, das alle Datenzugriffe überwacht und in regelmäßigen Abständen, nicht jedoch weniger als 1-mal pro Woche, einen vollen Scan der DVA (OnPrem & Cloud) durchführt. Die Signaturen des Virenschutzsystems werden mindestens einmal täglich aktualisiert.

Funktionstrennung

1. Entwicklungs-, Test- und Produktivsysteme werden strikt voneinander getrennt. Die Trennung erfolgt mindestens auf logischer Ebene bzw. Virtualisierungsebene, sofern nichts anderes im Vertrag vereinbart wurde.
2. Daten zu Entwicklungszwecken werden mit geeigneten Werkzeugen/ Methoden anonymisiert
3. Die Daten der einzelnen Mandanten werden immer logisch voneinander getrennt.

(8) Schutzmaßnahmen der **Incident Response:**
Datenschutz Vorfälle können von extern über die E-Mail-Adresse datenschutz@interhyp.de gemeldet werden. Eine entsprechende Information ist auf der Website der Interhyp veröffentlicht. Das Incident Management erfolgt nach dem ISO27001 Incident Management Prozess der Interhyp: Der Vorfall wird analysiert und bei Bestätigung die entsprechenden Fachabteilungen einbezogen, um den Vorfall auszuwerten, forensisch zu untersuchen und Maßnahmen abzuleiten. Sind personenbezogene Daten bei einem Vorfall beteiligt, wird die Rechtsabteilung hinzugezogen, um ggf. weitere Schritte einzuleiten, z.B. Information der Betroffenen etc.