Version 1.0 vom 08.06.2021

Vertrag zur Auftragsverarbeitung im Rahmen der Nutzung der hellohousing.de WebApp

zwischen

Hello Housing GmbH
Wattstraße 11
13355 Berlin

und

[Vertragspartner]

Präambel

Diese Anlage konkretisiert die Datenschutzverpflichtungen der Hello Housing GmbH (nachfolgend „Auftragnehmer“) gegenüber dem Nutzer der hellohousing.de WebApp (nachfolgend „Auftraggeber“), die sich aus der in dem Vertrag (Bestellung und AGB) 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. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten	**Art und Zweck der Datenverarbeitung**	**Kategorien betroffener Personen**
Mietvertragsdaten	Verarbeitung zur Erstellung von Nebenkostenabrechnungen Verwaltung von Mietdokumenten und Mietverhältnissen	Mieter
Verbrauchsdaten	Verarbeitung zur Erstellung von Nebenkostenabrechnungen	Mieter
Daten aus Betriebskostenabrechnungen	Verarbeitung zur Erstellung von Nebenkostenabrechnungen	Mieter
Zahlungseingänge	Finanzverwaltung, Buchhaltung, Forderungsmanagement	Mieter
Kontaktdaten, Nachrichtenverlauf zwischen Mieter und Vermieter	Gegenseitige Information und Kommunikation bzgl. Mietangelegenheiten	Mieter

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

§ 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 DS-GVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach 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.

§ 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) DS-GVO 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 so lange 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 Datenschutz-Grundverordnung (Art. 32 DS-GVO) 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 (siehe Anhang über technische und organisatorische Maßnahmen nach Art. 32 DS-GVO) und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(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 DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

(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) DS-GVO 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 Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger 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.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, 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 DS-GVO, gilt §3 Abs. 10 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer auf Nachfrage den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

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.

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.

Eine aktuelle Liste der Subunternehmer ist im Anhang zu dieser Vereinbarung aufgeführt.

Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.

§ 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 Datenschutz-Grundverordnung 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 Formerfordernis.

(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.

§9 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

Annex 1: Liste der von uns beauftragten Unterauftragsverarbeiter

Subunternehmer	**Dienstleistung**
Microsoft Ireland Limited South County Business Park, One Microsoft Court, Carmanhall and Leopardstown, Dublin, D18 DH6K, Irland	Cloud-Server Dienste
Cloud Primero Posthoornstraat 17 3011WD Rotterdam Netherlands	Softwareentwicklung & -betrieb
neoverv GmbH Wattstr. 11, 13355 Berlin, Deutschland	Softwareentwicklung & -betrieb

Annex 2: Technische und organisatorische Maßnahmen (TOM) der Hello Housing GmbH zur Gewährleistung des Datenschutzes und der Datensicherheit

1 Einleitung

Die hier beschrieben technischen und organisatorische Maßnahmen (TOM) umfassen die in der Praxis getroffenen Vorkehrungen der Hello Housing GmbH zur Gewährleistung der Sicherheit von personenbezogenen Daten. Die Maßnahmen werden fortlaufend aktualisiert und erweitert.

Personenbezogene Daten der Hello Housing GmbH insbesondere der hellohousing WebApp werden durch uns und durch von uns beauftragte externe Dienstleister verarbeitet. Mit allen externen Anbietern haben wir Vereinbarungen über Auftragsdatenverarbeitung abgeschlossen, welche die Anbieter zur Einhaltung der rechtlichen Vorschriften zum Datenschutz und der Datensicherheit verpflichten. So stellen wir sicher, dass die Daten nur an Standorten gespeichert werden, die der europäischen Datenschutzverordnung unterliegen. Alle externen Dienstleister haben zertifizierte Datenschutz- und Informationssicherheitskonzepte implementiert, die den gesetzlichen Anforderungen entsprechen. Die Namen der von uns beauftragten Dienstleister mit Zugriff auf personenbezogene Daten sind in Annex 1 dargestellt.

2 Allgemeine organisatorische Maßnahmen

- Als Ansprechpartner und Koordinator für den Datenschutz ist Hr. Jörg Radeke verantwortlich, der unter der E-Mail Adresse info@hellohousing.de kontaktiert werden kann.
- Alle Mitarbeiter sind über die Datenschutzvorkehrungen informiert und zur Vertraulichkeit der Kundendaten verpflichtet worden.
- Ein Datenschutzkonzept mit den hier dargestellten technischen und organisatorischen Maßnahmen ist erarbeitet worden.
- Soweit externe Dienstleister Zugang zu personenbezogenen Daten bekommen, müssen diese sich im Rahmen einer Vereinbarung für die Auftragsdatenverarbeitung zur Einhaltung der rechtlichen Vorgaben des Datenschutzes und der Datensicherheit verpflichten.

3 Vertraulichkeit

3.1 Zutrittskontrolle

Dieser Abschnitt beschreibt Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Die Zutrittskontrolle erfolgt über die folgenden Maßnahmen:

Technische Maßnahmen	Organisatorische Maßnahmen
▪ Personenbezogene Daten werden ausschließlich elektronisch gespeichert ▪ Chipkarten-basiertes Zugangssystem reguliert den Zutritt zum Flur ▪ Büroräume verfügen über Sicherheitsschlösser ▪ Zugänge sind videoüberwacht	▪ Schlüsselausgabe ist dokumentiert und erfolgt nur an Berechtigte ▪ Mitarbeiter sind angewiesen Büroräume bei Abwesenheit zu verschließen ▪ Computer nach Büroschluss unter Verschluss

	▪ Das Bürogebäude wird außerhalb der Bürozeiten von einem Sicherheitsdienst überwacht

3.2 Zugangskontrolle

Hello Housing führt die folgenden Maßnahmen durch, die geeignet sind zu verhindern, dass Computer und mobile Endgeräte von Unbefugten genutzt werden können.

Technische Maßnahmen	**Organisatorische Maßnahmen**
▪ Login mit Benutzername und sicherem Passwort ▪ Anti-Viren Software installiert und aktuell ▪ Firewall installiert und aktuell ▪ Verschlüsselte Datenübertragung zwischen Endgeräten und Servern	▪ Zentrale Verwaltung von Benutzerberechtigungen und Anlegen von Benutzerprofilen ▪ Richtlinien für sichere Passwörter ▪ Allgemeine Richtlinien zum Datenschutz und Datensicherheit ▪ Mitarbeiter müssen Anti-Viren Software aktuell halten

3.3 Zugriffskontrolle

Desweiten veranlasst Hello Housing Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen	**Organisatorische Maßnahmen**
▪ Differenziertes Rechtemanagement des Zugriffs auf alle elektronischen Dateien ▪ Computer und mobile Endgeräte werden jeweils nur durch einen Mitarbeiter genutzt	▪ Zentrale Administration von Benutzerrechten / Erstellen von Benutzerprofilen ▪ Individuelle Nutzerprofile, keine geteilten Nutzerprofile ▪ Differenzierte Steuerung der Benutzerrechte mit individuellen Profilen nach betrieblicher Notwendigkeit (mit absolut notwendigen Zugriffsrechten) ▪ Regelmäßige Überprüfung der Notwendigkeit von Zugriffsberechtigungen

3.4 Trennungskontrolle

Hello Housing hat außerdem Maßnahmen veranlasst, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden. Dies geschieht beispielsweise durch logische aber auch physikalische Trennung der Daten.

Technische Maßnahmen	Organisatorische Maßnahmen
▪ Trennung von Produktiv- und Testumgebung ▪ Trennung zwischen Zahlungsdienstdaten und anderen Nutzerdaten ▪ Mandantenfähigkeit der hellohousing WebApp ▪ Trennung der Daten von verschiedenen Auftraggebern ▪ Nutzung standardisierter Zugriffsverfahren / -abläufen ▪ Separate Speicherung der Daten nach Nutzungsszenarien	▪ In der Entwicklungs- und Testumgebung werden nur anonymisierte Daten verwendet ▪ Differenzierte Steuerung der Berechtigungen (siehe 3.3.)

3.5 Pseudonymisierung und Anonymisierung

Insbesondere bei der Entwicklung und beim Testen der WebApp anonymisiert bzw. verändert Hello Housing personenbezogene Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Diese zusätzlichen Informationen werden gesondert aufbewahrt.

Technische Maßnahmen	Organisatorische Maßnahmen
▪ Getrennte Aufbewahrung der Nutzerdaten und Nutzeridentitäten	▪ Für Entwicklungs- und Testzwecke werden nur anonymisierte bzw. pseudonymisierte Daten verwendet

3.6 Verschlüsselung

Sowohl die auf den externen Datenträgern gespeicherten Daten als auch die gesendeten Daten sind standardmäßig verschlüsselt. Eine unverschlüsselte Übertragung von personenbezogenen Daten findet nicht statt.

4 Integrität

4.1 Weitergabekontrolle

Hello Housing veranlasst im Rahmen zur Weitergabekontrolle Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Diese Maßnahmen sollen es uns außerdem ermöglichen zu überprüfen und feststellen, an welche Stellen eine elektronische Übermittlung personenbezogener Daten vorgesehen ist. Im Einzelnen umfasst das:

Technische Maßnahmen	Organisatorische Maßnahmen
▪ E-Mail-Verschlüsselung ▪ Nutzung von Ende-zu-Ende Verschlüsselung bei der Datenübertragung	▪ Interne Richtlinie personenbezogene Daten nur auf den dafür vorgesehen Servern zu speichern und eine Übermittlung nur über sichere

	unternehmensinterne Kanäle (E-Mail Server, verschlüsselte Netzwerke) vorzunehmen, Speicherung auf privaten Speichermedien und Versand Übertragung über unsichere Kanäle ist nicht gestattet ▪ Interne Richtlinie zur ausschließlichen Aufbewahrung von personenbezogenen Daten in elektronischen Format, eine Ablage oder Übermittlung von Daten in physischer Form erfolgt nicht

4.2 Eingabe- und Verarbeitungskontrolle

Die Eingabe- und Verarbeitungskontrolle betrifft Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass / Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	**Organisatorische Maßnahmen**
▪ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten ▪ Technische Protokollierung der An- und Abmeldungen am System	▪ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht aber Benutzergruppen) ▪ Differenzierte Steuerung der Berechtigungen (siehe 3.3.) ▪ Klare Zuständigkeiten für Löschungen

5 Verfügbarkeit und Belastbarkeit

5.1 Verfügbarkeitskontrolle

In diesem Abschnitt beschreiben wir die Maßnahmen, die Hello Housing GmbH gewährleistet, damit personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Hello Housing betreibt keine eigene Datenserverinfrastruktur sondern nutzt für die Speicherung aller Daten externe, cloud-basierte Datencenter von führenden Anbietern mit zertifizierten Datensicherheitskonzepten.

Die Betreiber der Datencenter können aufgrund der getroffenen technischen und organisatorischen Vorkehrungen eine Beschädigung der Datenspeicher mit sehr hoher Wahrscheinlichkeit ausschließen. Durch technische Sicherungsanlagen ist eine extrem hohe Datenverfügbarkeit gewährleistet. Redundante Datenspeicherung garantiert die Wiederherstellbarkeit der Daten sollte eines der Datencenter durch Beschädigung ausfallen.

6 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

6.1 Datenschutzmanagement

Technische Maßnahmen	Organisatorische Maßnahmen
▪ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf ▪ Dokumentiertes Datensicherheitskonzept	▪ Eine Überprüfung und Anpassung der Maßnahmen wird mindestens einmal pro Jahr durchgeführt ▪ Mitarbeiter über Datenschutz unterrichtet und verpflichtet und regelmäßige Sensibilisierung ▪ Zentrale Ansprechperson für den Datenschutz und Datensicherheit benannt

6.2 Incident-Response-Management

Technische Maßnahmen	Organisatorische Maßnahmen
▪ Einsatz und Aktualisierung von Firewalls, Spamfilter, Virenscanner auf eigenen Endgeräten um Vorfälle zu erkennen	▪ Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde) ▪ Dokumentation von Sicherheitsvorfällen und Datenpannen

6.3 Datenschutzfreundliche Voreinstellungen

Hello Housing erhebt nur so viele personenbezogene Daten, wie für die Bereitstellung der Dienstleistungen unbedingt erforderlich. Nutzerdaten werden automatisch spätestens drei Monate nach Ende der Geschäftsbeziehung gelöscht.

6.4 Auftragskontrolle (Outsourcing an Dritte)

Hello Housing verpflichtet externe Subunternehmer mit Zugriff auf personenbezogene Daten (Auftragsverarbeitung) zum Datenschutz und Datensicherheit. Dazu veranlassen wir die folgenden Maßnahmen, um ein hohes Maß an Datenschutz zu gewährleisten:

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung
- Schriftliche Weisungen an den Auftragnehmer
- Regelungen zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Rücknahme von etwaigen Berechtigungen / Zugangsdaten
- Regelmäßige Überprüfung und ggf. Anpassungen der Maßnahmen