

Vereinbarung zur Auftragsdatenverarbeitung (gemäß Art. 28 DSGVO)

- zwischen -

proba##AGName2##

##AGStreet##

##AGZIP## ##AGCITY##

##AGCountry##

vertreten durch

##AGCONTACT##

- im Folgenden: **Auftraggeber (AG)** genannt -

- und der-

hope-Software GmbH

Waldstr. 26

74867 Neunkirchen

Deutschland

vertreten durch

Steffen Diemer

- im Folgenden: **Auftragnehmer (AN)** genannt -

1 Präambel

Der AN führt im Auftrag des AG Tätigkeiten aus, welche weisungsgebundene Verarbeitungen von personenbezogenen Daten beinhalten. Dies stellt eine Auftragsverarbeitung im Sinne des Art. 28 EU Datenschutz-Grundverordnung (DSGVO) dar. Dieser liegen die Regelungen der DSGVO und des Bundesdatenschutzgesetzes (BDSG) zugrunde. Der vorliegende Vertrag zur Auftragsverarbeitung stellt die vertragliche Regelung der ordnungsgemäßen Verarbeitung personenbezogener Daten durch den AN im Auftrag des AG dar. Der Verantwortliche für die Verarbeitung im Sinne des Art. 4 Nr. 7 sowie Art. 28 DSGVO ist der AG. Die Anlage 1 "Technische und organisatorische Maßnahmen" und Anlage 2 "Weitere Auftragsverarbeiter" sind Bestandteil dieses Vertrags zur Auftragsverarbeitung.

2 Grundlage, Gegenstand und Dauer der Verarbeitung

2.1 Grundlage und Gegenstand

1. Die Grundlage dieses Auftrages ist die Nutzung der Softwareprodukte des AN sowie den Schnittstellen und der Onlinebuchungsplattform hopeWeb in Verbindung mit den AGB des AN.
2. Der AN übernimmt folgende Verarbeitungen:
 - Supportdienstleistungen per Telefon und Fernwartung, Zugriff auf die Systeme des AG
 - Bereitstellung der Softwareprodukte in externen Cloudservern
 - Verarbeitung von Buchungen und Gastdaten über die hoteleigenen Webseiten des AG
 - Verschlüsseltes Backup vom AG festgelegter Daten und Dateien auf externe Server
 - Senden von Gastdaten an vom AG freigegebenen Dritte wie z.B. Bewertungsportale, ChannelManager, Meldescheinsysteme, Türschließenanlagen, Telefonsysteme, etc.

2.2 Dauer

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 30 Tagen zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

3 Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

3.1 Art und Zweck der Verarbeitung

1. Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten
2. Zu dem genannten Zweck dürfen die Daten auf den Systemen des AG und des AN verarbeitet werden
3. Die Verarbeitung dient folgendem Zweck:
 - Durchführen von Supportdienstleistungen
 - Bereitstellung der Softwareprodukte des AN auf externen Cloudservern
 - Erfassen und Verarbeiten von Onlinebuchungen für den AG
 - Durchführung eines verschlüsselten Onlinebackups aller seitens des AG gewünschten Daten
 - Übermittlung der Daten an externe Dienstleister des AG

3.2 Art der Daten

Es werden folgende Daten verarbeitet:

- Name
- Adresse
- Telefon
- Email
- Zusätzliche in den Softwareprodukten erfassten Informationen

3.2.1 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Gäste
- Interessenten
- Geschäftspartner
- Gäste von Onlinebuchungen

4 Pflichten des AN

1. Der AN verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom AG angewiesen, es sei denn, der AN ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der AN diese dem AG vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der AN verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
2. Der AN bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
3. Der AN verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
4. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
5. Der AN sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der AN trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzerfordernisse laufend angemessen angeleitet und überwacht werden.
6. Im Zusammenhang mit der beauftragten Verarbeitung hat der AN den AG bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem AG auf Anforderung unverzüglich zuzuleiten.
7. Wird der AG durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der AN den AG im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
8. Auskünfte an Dritte oder den Betroffenen darf der AN nur nach vorheriger Zustimmung durch den AG erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den AG weiterleiten.

9. Der AN gewährleistet, dass er einen Datenschutzbeauftragten benannt hat, insofern dieser gemäß § 38 Abs. 1 BDSG oder Art. 37 Abs. 1 DSGVO dazu verpflichtet ist, und dass der Datenschutzbeauftragte seine Tätigkeit gemäß § 38 Abs. 2 BDSG und Art. 38 und 39 DSGVO ausüben kann. Dessen Kontaktdaten werden dem AG oder dessen Datenschutzbeauftragten zum Zweck der direkten Kontaktaufnahme auf Anfrage unverzüglich mitgeteilt. Ein Wechsel des Datenschutzbeauftragten bzw. dessen Abberufung ist dem AG unverzüglich mitzuteilen.
10. Jede Verlagerung der vereinbarten Datenverarbeitung in ein Drittland bedarf der vorherigen Genehmigung des AG. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet bis dahin ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, es sei denn, der AG gestattet die Datenverarbeitung in einem Drittland vorab und der AN hat sich davon überzeugt, dass bei der datenverarbeitenden Stelle im Drittland ein erforderliches Schutzniveau für die Datenverarbeitung im Sinne des Art. 44 Satz 2 DSGVO vorliegt oder hergestellt wurde. Als vorab genehmigt gelten insbesondere die in Anlage 2 aufgeführten Subunternehmen aus Drittstaaten. Der AN garantiert für Verlagerungen der vereinbarten Datenverarbeitung in ein Drittland oder Hinzuziehung dort befindlicher Auftragsverarbeiter, dass die Einhaltung der besonderen Voraussetzungen der Art. 44 - 50 DSGVO erfüllt sind. Für die Zulässigkeit der Verlagerung in ein Drittland oder die Einbeziehung von Auftragsverarbeitern in einem Drittland trägt der AN die Verantwortung. Er hat die Zulässigkeit und die Einhaltung der DSGVO auf Verlangen des AG nachzuweisen.

5 Technische und organisatorische Maßnahmen

1. Der AN gewährleistet die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 und Art. 5 Abs. 1 und 2 DSGVO. Diese hat der AN in der Anlage 1 zu diesem Vertrag zur Auftragsverarbeitung ausführlich darzulegen. Bei Akzeptanz durch den AG werden die dokumentierten Maßnahmen Grundlage des Auftrags.
2. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um solche der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der involvierten Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen gemäß Art. 32 Abs. 1 DSGVO zu berücksichtigen. Hierzu hat der AN insbesondere die Räume, in denen sich die Daten des AG befinden, so zu sichern, dass Unbefugten der Zutritt verwehrt wird, und sicherzustellen, dass der Zugriff auf die personenbezogenen Daten Unbefugten verwehrt wird. Er muss auch verhindern, dass die Unterlagen des AG von Unbefugten gelesen, verändert, kopiert oder entfernt werden können, und seine innerbetriebliche Organisation so gestalten, dass diese den besonderen Ansprüchen des Datenschutzes gerecht wird und die Daten nur im Rahmen der Weisungen des AG verarbeitet werden und während einer Übertragung ausreichend geschützt sind. Den für die Auftragsverarbeitung zuständigen Mitarbeitern des AN müssen diese Weisungen bekannt gemacht werden.
3. Der AN kontrolliert regelmäßig seine 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 Personen gewährleistet wird.

4. Der AN gewährleistet die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem AG im Rahmen seiner Kontrollbefugnisse dieses Vertrags und wird dem AG diese, bei längerer Beauftragung, nach jährlicher Aufforderung erneut darlegen bzw. zusichern, dass sich keine Änderungen ergeben haben.
5. Soweit die Prüfung oder ein Audit des AG oder dessen Datenschutzbeauftragter oder ein Kontrollverfahren der zuständigen Aufsichtsbehörde einen Anpassungsbedarf der getroffenen Maßnahmen aufzeigt, ist dieser einvernehmlich umzusetzen.
6. Die getroffenen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem AN gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das vorherige Sicherheitsniveau nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.
7. Die Verarbeitung von Daten in Privatwohnungen ist nur mit vorheriger schriftlicher Zustimmung des AG im Einzelfall gestattet. Soweit eine solche Verarbeitung erfolgt, ist vom AN sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des AG uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können. Ausdrücklich ausgenommen hiervon ist die temporäre Verarbeitung von Daten des AG zum Zwecke von Supportdienstleistungen und Fehlersuche/-behebungen von Mitarbeitern im Home-Office.

6 Rückgabe und Löschung der Daten

1. Kopien der Daten dürfen ohne Genehmigung des AG nicht erstellt werden. Hiervon ausgenommen sind Sicherheitskopien, soweit diese zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Der AN erwirbt keinerlei Rechte an den ihm zur Verfügung gestellten Daten, verwendet die Daten für keine anderen Zwecke als die ordnungsgemäße Durchführung des Vertrags und dieser Vereinbarung und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben.
2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den AG - spätestens nach Kündigung oder Erfüllung des Auftrags - hat der AN sämtliche in seinen Besitz gelangten digitalen Daten und Informationen sowie selbige in Papierform, die erstellten Verarbeitungs- und Nutzungsergebnisse sowie Daten und Informationen, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem AG auszuhändigen oder nach vorheriger Genehmigung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist dem AG anschließend vorzulegen oder alternativ die Löschung in Textform zu bestätigen.
3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den AN entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem AG übergeben.

7 Einbeziehung weiterer Auftragsverarbeiter

1. Der AN setzt den AG darüber in Kenntnis, sofern er beabsichtigt, weitere als die in Anlage 1 ausgewiesenen Auftragsverarbeiter hinzuzuziehen, welche direkt mit der Verarbeitung von personenbezogenen Daten des AG beauftragt sind. Erfolgt innerhalb von 4 Wochen kein Widerspruch des AG, gilt die Beauftragung der weiteren Auftragsverarbeiter als genehmigt.
2. Als hinzugezogene Auftragsverarbeiter im Sinne dieser Regelung sind solche Dienstleister zu verstehen, die sich unmittelbar ganz oder teilweise auf die Erbringung der beauftragten Datenverarbeitung beziehen. Nicht hierzu gehören Nebenleistungen, die der AN z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder zur Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der AN ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des AG auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
3. Zieht es der Auftragsverarbeiter in Erwägung, die Dienste eines weiteren Auftragsverarbeiters hinzuzuziehen, um bestimmte Verarbeitungstätigkeiten im Namen des AG auszuführen, so wird der AN diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Recht der Europäischen Union oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegen, die in diesem vorliegendem Vertrag zwischen AG und dem AN vereinbart sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so umgesetzt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Sämtliche Änderungen dieses Vertrags zur Auftragsverarbeitung hat der AN auch hinzugezogenen Auftragsverarbeitern fortwährend aufzuerlegen. Kommt der hinzugezogene Auftragsverarbeiter seinen Pflichten nicht nach oder verstößt dieser gegen die DSGVO, so haftet der AN gegenüber dem AG oder den betroffenen Personen für die Schäden, die dadurch entstanden sind.
4. Die Weitergabe von personenbezogenen Daten des AG an durch den AN hinzugezogene Auftragsverarbeiter ist erst mit Vorliegen der Genehmigung des AG über die Hinzuziehung und die Erfüllung aller Voraussetzungen aus § 9 des vorliegenden Vertrags erlaubt. Der AG erhält vom AN auf Aufforderung Einblick in die relevanten Vertragsunterlagen mit dem hinzugezogenen Auftragsverarbeiter, wobei der AN berechtigt ist, Preise und Vergütungen o. Ä. unkenntlich zu machen.
5. Soll der hinzugezogene Auftragsverarbeiter außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums tätig werden, stellt der AN die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Diese weist der AN dem AG unaufgefordert nach.
6. Der AN hat die Auftragsverarbeiter, welche er hinzuzuziehen gedenkt, in Anlage 2 aufzulisten und die dort abgefragten Angaben zu beantworten. Durch Unterschrift dieses Vertrags zur Auftragsverarbeitung durch den AG wird deren Hinzuziehung genehmigt.

8 Rechte und Pflichten des AG

1. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der AG verantwortlich.
2. Der AG informiert den AN unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
3. Der AG ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim AN in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom AN soweit erforderlich Zutritt und Einblick zu ermöglichen. Der AN ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.
4. Kontrollen beim AN haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom AG zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des AN, sowie nicht häufiger als alle 12 Monate statt. Soweit der AN den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9 Mitteilungspflichten

1. Der AN teilt dem AG Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des AN vom relevanten Ereignis an eine vom AG benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
 - a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
 - c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - d. eine Beschreibung der vom AN ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
2. Ebenfalls unverzüglich mitzuteilen sind Verstöße des AN oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
3. Der AN informiert den AG unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
4. Der AN sichert zu, den AG bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10 Vergütung

Die Vergütung des AN ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

11 Verschwiegenheit und Wahrung von Betriebs- und Geschäftsgeheimnissen

1. Der AN hat sich mit der Geheimhaltung von Betriebs- und Geschäftsgeheimnissen im Sinne des § 17 des Gesetzes gegen den unlauteren Wettbewerb (UWG) vertraut gemacht und sichert deren Einhaltung für sich und das durch ihn eingesetzte Personal sowie hinzugezogene Auftragsverarbeiter zu. Dies gilt auch für die sich aus dem vorliegenden Vertragsverhältnis ergebenden Folgeaufträge oder Auftragserweiterungen sowie andere künftige Geschäftsbeziehungen und bezieht sich auf alle Leistungen des AN gegenüber dem AG und ggf. dessen verbundene Unternehmen wie Mutter-, Tochter- und Schwestergesellschaften unabhängig davon, an welchem Ort diese erbracht werden. Sie erstrecken sich auf sämtliche personenbezogene Daten, Unternehmensdaten und -informationen, gleich in welcher Form diese vorliegen und gleich ob sie ausdrücklich als vertraulich bezeichnet sind oder nicht.
2. Der AN sichert zu, dass das von ihm eingesetzte Personal sämtliche während der Erfüllung des Auftrags auch zufällig zugänglich gewordenen Daten geheim hält, sich weder Aufzeichnungen darüber macht noch Kopien anfertigt, entsprechende Daten nicht an Dritte weitergibt oder für eigene Zwecke nutzt.
3. Sollte der AN bzw. dessen zur Vertragserfüllung eingesetztes Personal das E-Mail-System, das Internet/Intranet bzw. die IT-Systeme des AG nutzen wollen, so wird sich der AN bzw. das entsprechende Personal vorab die ausdrückliche Erlaubnis einholen und vor deren Nutzung beim AG über die internen Regelungen des AG zum Umgang mit diesen Systemen und Medien informieren und diesen entsprechen. Der AG behält sich vor, auf alle zur Verfügung gestellten Systeme sowie Daten und Informationen ohne Vorankündigung zuzugreifen. Der AN ist dann seinerseits verpflichtet, das von ihm eingesetzte Personal über die Einhaltung der genannten internen Regelungen des AG regelmäßig zu informieren und deren Einhaltung sicherzustellen.
4. Für eine Unterrichtung, Verpflichtung und Schulung des durch den AN eingesetzten Personals ist der AN verantwortlich. Der AN sichert zu, dass dieser nur Personal einsetzt, das mit den Anforderungen der DSGVO und allen nationalen sowie anderen einschlägigen Datenschutzbestimmungen, der Wahrung von Betriebs- und Geschäftsgeheimnissen im Sinne des § 17 UWG, den Pflichten aus dieser Verpflichtungserklärung und zur Vertraulichkeit im Sinne des Art. 28 Abs. 3 Satz 2 lit. b) DSGVO vertraut ist.

12 Schlussbestimmungen

1. Der AN ist sich bewusst, dass die Verletzung dieses Vertrags zur Auftragsverarbeitung einen Verstoß gegen die DSGVO, das BDSG, das UWG oder eine sonstige datenschutzrechtliche Vorschrift darstellen kann und dies eine Ordnungswidrigkeit oder Straftat darstellen kann und dass er für diese Verletzungen selbst verantwortlich sowie haftbar ist.
2. Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt. An die Stelle der unwirksamen Bestimmungen wird eine andere treten, die wirksam ist und die nach Inhalt und Zweck der unwirksamen Bestimmung am nächsten kommt.

Neunkirchen, ##DayDate##

Ort, Datum



Auftragnehmer

##City##, ##DayDate##

Ort, Datum

Unterschrift digital gesetzt
durch
Passworteingabe
und
aktive Bestätigung
des Kunden

Auftraggeber

Anlage 1 – technische und organisatorische Maßnahmen

1. Maßnahmen zur Vertraulichkeit:

1.1 Beschreibung der Zutrittskontrolle:

- Elektrisches Schließsystem mit Schließzylinder
- Schließsystem mit Protokollfunktion
- Sicherheitsschlösser
- Sorgfältige Auswahl von Reinigungspersonal

1.2 Beschreibung der Zugangskontrolle:

- Login mit Benutzername und Passwort
- Einsatz von Firewalls zum Schutz des Netzwerkes
- Richtlinie "Sicheres Passwort"
- Richtlinie "Sicheres Löschen/Vernichten"
- Allgemeine Richtlinie Datenschutz und/oder Sicherheit

1.3 Beschreibung der Zugriffskontrolle:

- Erstellen und Einsatz eines Berechtigungskonzepts
- Sichere Löschung von Datenträgern vor deren Wiederverwendung (z.B. durch mehrfaches Überschreiben)
- Einsatz von Aktenvernichtern
- Protokollierung von Zugriffen auf Anwendungen, konkret bei Eingabe, Änderung und Löschung von Daten

1.4 Beschreibung der Weitergabekontrolle:

- Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet
- Bereitstellung über verschlüsselte Verbindungen wie z.B. https, sftp

1.5 Beschreibung des Trennungsgebots:

- Trennung von Produktiv- und Testsystem
- Logische Mandantentrennung (softwareseitig)
- Festlegung von Datenbankrechten

1.6 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

2. Maßnahmen zur Integrität:

2.1 Beschreibung der Eingabekontrolle:

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe.
- Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können

3. Maßnahmen zur Verfügbarkeit und Belastbarkeit:

3.1 Verfügbarkeitskontrolle:

- Einsatz von Antivirensoftware zum Schutz vor Malware
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Verschlüsseltes Backup auf externe Serversysteme
- Feuer- und Rauchmeldeanlagen
- Redundante Datenhaltung (z.B. gespiegelte Festplatten, RAID 1 oder höher)

3.2 Beschreibung der Wiederherstellbarkeit:

- Kontrolle des Sicherungsvorgangs
- Regelmäßige Tests zur Datenwiederherstellung

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

4.1 Datenschutz-Management

- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
- Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

4.2 Incident-Response-Management

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virens Scanner und regelmäßige Aktualisierung
- Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
- Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen


4.3 Auftragskontrolle:

- Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO.
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen.
- Verpflichtung auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO

4.4 Beschreibung des Managementsystems:

- Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DS-GVO)
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

Neunkirchen, ##DayDate##



hope - Software GmbH
Waldstrasse 26
74867 Neunkirchen
Tel.: +49.6262.8809999
info@hope-Software.com
www.hope-Software.com

Steffen Diemer
Tina Forstmann
Friedrich Diemer

NEUNKIRCHEN • BERLIN • OFFENBURG • LINGEN • SWAKOPMUND



Ort, Datum

Auftragnehmer

Anlage 2 – Zugelassene Subdienstleister

Weiterer Auftragsverarbeiter Nr. 1:

Name:

webgo GmbH

Anschrift inklusive Land:

Wandsbeker Zollstr. 95, 22041 Hamburg, Deutschland

Umfang, Art und Zweck der Tätigkeit:

Data-Center, Server-Hosting, web-Hosting, Wordpress-Hosting, Email-Provider

Weiterer Auftragsverarbeiter Nr. 2:

Name:

myLoc managed IT AG

Anschrift inklusive Land:

Am Gatherhof 44, 40472 Düsseldorf, Deutschland

Umfang, Art und Zweck der Tätigkeit:

Data-Center, Server-Hosting, Cloud-Hosting, Email-Provider, Hosting CRM-system, Email-Provider

Weiterer Auftragsverarbeiter Nr. 3:

Name:

United Internet AG

Anschrift inklusive Land:

Elgendorfer Straße 57, 56410 Montabaur, Deutschland

Umfang, Art und Zweck der Tätigkeit:

Data-Center, Server-Hosting, web-Hosting, Email-Provider, Domain-Verwaltung

Weiterer Auftragsverarbeiter Nr. 4:

Name:

Hetzner Online GmbH

Anschrift inklusive Land:

Industriestr. 25, 91710 Gunzenhausen, Deutschland

Umfang, Art und Zweck der Tätigkeit:

Data-Center, Server-Hosting, Hosting hopeWeb, Email-Provider

Weiterer Auftragsverarbeiter Nr. 5:

Name:

Contabo GmbH

Anschrift inklusive Land:

Aschauer Straße 32a, 81549 München, Deutschland

Umfang, Art und Zweck der Tätigkeit:

Server-Hosting, web.Hosting, Email-Provider

