Vereinbarung zur Auftragsverarbeitung

Die Vertragsparteien

_____
Unternehmensbezeichnung, Firma

_____
Straße, Hausnummer

_____

PLZ, Stadt

im Folgenden: Auftraggeber

und

HiBit Computer GmbH
Roseggerstr. 35
21079 Hamburg

im Folgenden: Auftragsverarbeiter – schließen folgenden Vertrag:

1. Allgemeine Bestimmungen und Auftragsgegenstand

1.1 Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragsverarbeiter (Art. 28 DSGVO). Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Vereinbarung sind Anlage 1 zu entnehmen.
1.2 Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er allein ist für Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge nach Art. 6 DSGVO und die Wahrung der Betroffenenrechte verantwortlich.
1.3 Die Verarbeitung der Daten durch den Auftragsverarbeiter findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung des Auftraggebers.
1.4 Die Vergütung wird außerhalb dieses Vertrags vereinbart.

2. Vertragslaufzeit und Kündigung

Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3.1 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragsverarbeiter zu. In dieser Rolle kann er insbesondere die unverzügliche

Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragsverarbeiter ist verpflichtet, den Weisungen des Auftraggebers Folge leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.
3.2 Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragsverarbeiter substantiiert anzweifelt, ist der Auftragsverarbeiter berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.
3.3 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisung sind auf Verlangen des Auftragsverarbeiters schriftlich oder in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragsverarbeiter hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.
3.4 Der Auftraggeber benennt auf Verlangen des Auftragsverarbeiters eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragsverarbeiter unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren oder durch Dritte kontrollieren zu lassen. Der Auftragsverarbeiter wird diese Kontrollen dulden und sie im erforderlichen Maße unterstützen. Er wird dem Auftraggeber insbesondere die für die Kontrollen relevanten Auskünfte vollständig und wahrheitsgemäß erteilen, ihm die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme/ -systeme gewähren sowie Vorort-Kontrollen ermöglichen. Sofern der Auftraggeber der Verarbeitung der Daten außerhalb der Geschäftsräume (z.B. Privatwohnung) zugestimmt hat, hat der
Auftragsverarbeiter dafür zu sorgen, dass der Auftraggeber auch diese Räume zu Kontrollzwecken begehen darf.
4.2 Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragsverarbeiters nicht mehr als erforderlich beeinträchtigen. Insbesondere sollen Vorortkontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Vorlauffrist erfolgen, sofern der Kontrollzweck einer vorherigen Ankündigung nicht widerspricht.
4.3 Die Ergebnisse der Kontrollen und Weisungen sind von beiden Vertragsparteien in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragsverarbeiters

5.1 Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragsverarbeiter erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig
(z.B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragsverarbeiter dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
5.2 Der Auftragsverarbeiter hat bei der Auftragsdurchführung sämtliche gesetzlichen Vorschriften einzuhalten. Er hat insbesondere die nach Art. 32 DSGVO notwendigen technischen und organisatorischen Maßnahmen implementieren und das nach Art. 30 Abs. 2 DSGVO erforderliche Verzeichnis von Verarbeitungstätigkeiten zu führen, soweit dies gesetzlich vorgeschrieben ist.
5.3 Sofern der Auftragsverarbeiter nach der DSGVO oder sonstigen gesetzlichen Vorschriften zur Benennung eines Datenschutzbeauftragten verpflichtet ist, bestätigt er, dass er einen solchen in Einklang mit den gesetzlichen Vorschriften bestellt hat.

Datenschutzbeauftragter des Auftragsverarbeiters:

Deutsche Datenschutz Consult GmbH
Stresemannstraße 29
22769 Hamburg

Telefon: +49 40 2286070-0
E-Mail: beratung@ddsc.de

Änderungen hinsichtlich Person oder Kontaktdaten des Datenschutzbeauftragten werden dem Auftraggeber unverzüglich mitgeteilt.
5.4 Die Verarbeitung personenbezogener Daten außerhalb der Betriebsstätten des Auftragsverarbeiters oder seiner Unterauftragsverarbeiter, insbesondere im Rahmen von Fernwartung, Bereitschaftsdiensten, mobilen Arbeitsplätzen oder Homeoffice, ist zulässig, sofern die gleichen technischen und organisatorischen Maßnahmen eingehalten werden wie innerhalb der Betriebsstätten. Zugriffe auf Kundensysteme erfolgen ausschließlich über verschlüsselte Verbindungen und durch hierzu autorisierte Mitarbeiter des Auftragsverarbeiters.
5.5 Der Auftragsverarbeiter hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden
Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.
5.6 Der Auftragsverarbeiter wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

6. Technische und organisatorische Maßnahmen

6.1 Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 2 dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt und mit dem Auftraggeber abgestimmt.
6.2 Der Auftragsverarbeiter wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen. Erforderliche Anpassungen werden vom Auftragsverarbeiter dokumentiert und dem Auftraggeber auf Nachfrage zur Verfügung gestellt. Wesentliche Änderungen, durch die das Schutzniveau verringert werden könnte, sind vorab mit dem Auftraggeber abzustimmen.

7. Unterstützungspflichten des Auftragsverarbeiters

7.1 Der Auftragsverarbeiter wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Reichweite der Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung.
7.2 Der Auftragsverarbeiter wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

8.1 Der Auftragsverarbeiter ist berechtigt, Unterauftragsverarbeiter einzusetzen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter ergeben sich aus Anlage 3. Der Auftraggeber erteilt mit Unterzeichnung dieses Vertrages seine Zustimmung zu den dort aufgeführten Unterauftragsverarbeitern. Der Auftragsverarbeiter informiert den Auftraggeber über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern in Textform. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Tagen nach Zugang der Information widersprechen.
8.2 Subunternehmer werden vom Auftragsverarbeiter unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Nebenleistungen, die der Auftragsverarbeiter zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragsverarbeiter
wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen
Datenschutzstandards sicherstellen.
8.3 Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Die

Subunternehmerverträge haben darüber hinaus sicherzustellen, dass die im vorliegenden Vertrag vereinbarten Kontroll- und Weisungsbefugnisse durch den Auftraggeber in gleicher Weise und in vollem Umfang auch gegenüber dem Unterauftragsverarbeiter ausgeübt werden können. Der Auftragsverarbeiter ist im Falle einer entsprechenden Aufforderung des Auftraggebers verpflichtet, Auskunft über die datenschutzrechtlich relevanten Verpflichtungen des Subunternehmers zu erteilen und erforderlichenfalls die entsprechenden Vertragsunterlagen oder Kontroll- und Aufsichtsergebnisse sowie entsprechende Dokumentationen, Protokolle und Verzeichnisse des Auftragsverarbeiters einzusehen oder die Übermittlung dieser Unterlagen in Kopie zu verlangen.
8.4 Im Vertrag mit dem Subunternehmer ist festzuschreiben, welche Verantwortlichkeiten der Subunternehmer hat, damit der Auftraggeber diese entsprechend überprüfen kann. Ferner muss der Vertrag mit dem Subunternehmer sicherstellen, dass der Auftraggeber ggü. Dem Subunternehmer zur Ausübung der gleichen Kontrollrechte, wie ggü. Dem Auftragsverarbeiter berechtigt ist. Der Auftragsverarbeiter hat sicherzustellen, dass die vom Auftraggeber erteilten Weisungen auch von den Subunternehmern befolgt und protokolliert werden. Die Einhaltung dieser Pflichten wird vom Auftragsverarbeiter vor Vertragsschluss mit dem Subunternehmer und sodann regelmäßig kontrolliert und dokumentiert.
8.5 Die Weiterleitung von Daten an den Unterauftragsverarbeiter ist erst zulässig, wenn der Subunternehmer seine Pflichten nach Art. 32 Abs. 4 und 29 DSGVO ggü. den ihm unterstellten Personen erfüllt hat.
8.6 Der Auftragsverarbeiter ist für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Unterauftragsverarbeiter verantwortlich. Er haftet ggü. dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.
8.7 Der Auftragsverarbeiter hat sich von seinen Unterauftragsverarbeitern bestätigen zu lassen, dass diese – soweit gesetzlich vorgeschrieben – einen Datenschutzbeauftragten benannt haben.
8.8 Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilungspflichten des Auftragsverarbeiters

9.1 Verstöße gegen diesen Vertrag, gegen die Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragsverarbeiter selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.
9.2 Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten nach Art. 33 und 34 DSGVO zu unterstützen. Eigenständige Meldungen an Behörden oder Betroffene nach Art. 33 und 34 DSGVO darf der Auftragsverarbeiter erst nach vorheriger Weisung des Auftraggebers durchführen.
9.3 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragsverarbeiter um Auskunft, Berichtigung, Sperrung oder Löschung, wird der Auftragsverarbeiter die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragsverarbeiter dem Ersuchen des Betroffenen ohne Zustimmung des Auftraggebers nachkommen.
9.4 Der Auftragsverarbeiter wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragsverarbeiter den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen). Der Auftraggeber ist berechtigt, die Maßnahmen des Auftragsverarbeiters in geeigneter Weise zu überprüfen. Hierzu ist er insbesondere berechtigt, die einschlägigen Löschprotokolle und die betroffenen Datenverarbeitungsanlagen vor Ort in Augenschein zu nehmen.

11. Datengeheimnis und Vertraulichkeit

11.1 Der Auftragsverarbeiter ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln und einschlägige Geheimnisschutzregeln, denen der Auftraggeber unterliegt (z.B. § 203 StGB), zu beachten. Der

Auftraggeber ist verpflichtet, den Auftragsverarbeiter bei Auftragserteilung auf ggf. bestehende besondere Geheimnisschutzregeln hinzuweisen.
11.2 Der Auftragsverarbeiter verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragsverarbeiter aufnehmen.
11.3 Der Auftragsverarbeiter wird die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise dokumentieren. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

12. Schlussbestimmungen

12.1 Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.
12.2 Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.
12.3 Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.
12.4 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

_____, den _____	Hamburg, den _____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift (Auftraggeber)	Unterschrift (Auftragsverarbeiter)

ANLAGE 1 – Hosting-, Cloud-, Kommunikations- und Archivierungsdienste

Gegenstand der Verarbeitung
Der Auftragsverarbeiter erbringt für den Auftraggeber Hosting-, Kommunikations-, Archivierungs- und Datensicherungsleistungen.
Die Verarbeitung personenbezogener Daten erfolgt ausschließlich zur Bereitstellung, Administration, Wartung, Sicherung und Wiederherstellung der vereinbarten Dienste. Art und Umfang der Verarbeitung richten sich nach den vom Auftraggeber beauftragten Leistungen.
Die Verarbeitung kann insbesondere im Zusammenhang mit der Bereitstellung von Hosting-, E-Mail-, Kommunikations-, Archivierungs- und Backupdiensten erfolgen.

Hosting- und Cloud-Dienste
Im Rahmen der Hosting- und Cloud-Dienstleistungen stellt der Auftragsverarbeiter technische Infrastrukturen zur Speicherung, Verarbeitung und Übertragung von Daten bereit. Die Verarbeitung personenbezogener Daten erfolgt ausschließlich im Auftrag des Auftraggebers und nur im erforderlichen Umfang zur Erbringung der vereinbarten Leistungen.

Hierzu gehören insbesondere:

[X] Webhosting
[X] E-Mail-Hosting
[X] Domainservices
[X] Virtuelle Server (VPS)
[X] Dedizierte Server
[X] Managed Hosting
[X] Backup Hosting
[X] MailStore MSP

Kommunikationsdienste
Der Auftragsverarbeiter kann Kommunikations- und Telefoniedienste bereitstellen und administrieren. Im Rahmen dieser Leistungen können technische Kommunikationsdaten, Benutzerinformationen, Verbindungsdaten und sonstige zur Leistungserbringung erforderliche Informationen verarbeitet werden.

Hierzu gehören insbesondere:

[X] 3CX Hosting
[X] SIP-/VoIP-Kommunikationsdienste
[X] Notfalltelefonanlage
[X] Videokonferenz- und Chatdienste
[X] Datensicherungs- und Wiederherstellungsdienste

Backup- und Wiederherstellungsdienste
Zur Sicherstellung der Verfügbarkeit und Wiederherstellbarkeit von Daten können Datensicherungs- und Recovery-Dienste bereitgestellt werden. Die Verarbeitung erfolgt ausschließlich zur Durchführung von Datensicherungen, Wiederherstellungen und Integritätsprüfungen.

[X] Archivierungsdienste
[X] Datensicherungs- und Wiederherstellungsdienste

Verarbeitete Datenarten

Im Rahmen der vereinbarten Hosting-, Kommunikations-, Archivierungs- und Datensicherungsleistungen können abhängig von den konkret beauftragten Leistungen unterschiedliche Kategorien personenbezogener Daten verarbeitet werden.

Art und Umfang der Verarbeitung werden durch den Auftraggeber bestimmt. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der technischen Leistungserbringung, Administration, Wartung, Sicherung und Wiederherstellung der bereitgestellten Systeme.

Insbesondere können folgende Datenarten betroffen sein:

[X] Personalstammdaten
[X] Kommunikationsdaten
[X] Vertragsdaten
[X] Kundenhistorie
[X] Zahlungsdaten
[X] Benutzerkonten
[X] E-Mail-Inhalte
[X] E-Mail-Anhänge
[X] Archivierungsdaten
[X] Rufnummern
[X] Verbindungsdaten
[X] Gesprächsprotokolle (CDR)
[X] Voicemail-Daten
[X] Chat- und Konferenzdaten
[X] Log- und Diagnosedaten
[X] Backupdaten

Betroffene Personen

Die Verarbeitung kann sich auf personenbezogene Daten unterschiedlicher Personengruppen beziehen, deren Daten durch den Auftraggeber im Rahmen seiner Geschäftstätigkeit verarbeitet werden.

Die konkreten Kategorien betroffener Personen ergeben sich aus den vom Auftraggeber genutzten Diensten und den darin gespeicherten Datenbeständen.

Insbesondere können folgende Personengruppen betroffen sein:

[X] Kunden
[X] Interessenten
[X] Beschäftigte
[X] Lieferanten
[X] Ansprechpartner
[X] Geschäftspartner
[X] Webseitenbesucher
[X] Sonstige Betroffene

Besondere Leistungsbestandteile

3CX Hosting

Der Auftragsverarbeiter betreibt und administriert auf Wunsch gehostete 3CX-Kommunikationssysteme. Hierbei können technische Konfigurationsdaten, Benutzerkonten, Verbindungsdaten, Voicemaildaten und Systemprotokolle verarbeitet werden.

MailStore MSP

Der Auftragsverarbeiter betreibt Systeme zur revisionssicheren E-Mail-Archivierung. Hierbei können E-Mail-Inhalte, Anhänge, Archivierungsinformationen und Protokolldaten verarbeitet werden.

ANLAGE 2 – Technische und Organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen treffen Auftraggeber und Auftragnehmer die nachfolgenden technischen und organisatorischen Maßnahmen (TOM).

Diese Maßnahmen gelten für die in Anlage 1 zur Vereinbarung zur Auftragsverarbeitung beschriebenen Hosting-, Kommunikations-, Archivierungs- und Datensicherungsleistungen, die durch den Auftragnehmer erbracht werden.

Bei der Auswahl der Maßnahmen wurden die Schutzziele des Art. 32 Abs. 1 DSGVO, insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste, berücksichtigt. Die Wiederherstellbarkeit der Verfügbarkeit und des Zugangs zu personenbezogenen Daten nach einem physischen oder technischen Zwischenfall ist sichergestellt. Die technischen und organisatorischen Maßnahmen werden regelmäßig auf ihre Wirksamkeit überprüft, bewertet und bei Bedarf angepasst.

Generell gilt Folgendes:

Die HiBit Computer GmbH stellt dem Auftraggeber Hosting-, Kommunikations-, Archivierungs- und Datensicherungsleistungen zur Verfügung. Dies umfasst insbesondere die Bereitstellung und den Betrieb von Hard- und Software, Speicher- und Kommunikationsdiensten, Hosting-Plattformen, Datensicherungs- und Archivierungssystemen, Internetanbindungen sowie weiterer vertraglich vereinbarter Leistungen.

Der Auftraggeber bleibt Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO und entscheidet allein über Zweck und Mittel der Verarbeitung personenbezogener Daten.

Die HiBit Computer GmbH verarbeitet personenbezogene Daten ausschließlich im Rahmen der technischen Bereitstellung, Administration, Wartung, Überwachung, Datensicherung, Archivierung und Wiederherstellung der vereinbarten Systeme und Dienstleistungen.

Soweit dies zur Erbringung der vertraglich vereinbarten Leistungen erforderlich ist, kann die HiBit Computer GmbH Zugriff auf Systeme, Anwendungen und personenbezogene Daten des Auftraggebers erhalten. Eine Verarbeitung erfolgt ausschließlich im Rahmen der vertraglichen Vereinbarungen, der Weisungen des Auftraggebers sowie der geltenden datenschutzrechtlichen Bestimmungen.

Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

Der Auftragsverarbeiter setzt die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden unter Berücksichtigung der gesetzlichen Anforderungen des Art. 32 DSGVO festgelegt.

Es wurden insbesondere folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern:

Es wurden folgende Maßnahmen getroffen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, Serverräumen, Netzwerkkomponenten und sonstigen Einrichtungen, in denen personenbezogene Daten verarbeitet oder gespeichert werden, zu verwehren:

Zutrittskontrolle

[X] Alarmanlage
[X] Automatisches Zugangskontrollsystem
[X] Chipkarten-/Transponder-Schließsystem
[X] Schließsystem mit Codesperre
[X] Biometrische Zugangssperren
[X] Videoüberwachung der Zugänge
[X] Sicherheitsschlösser

Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern:

Zugangskontrolle

[X] Zuordnung von Benutzerrechten
[X] Erstellen von Benutzerprofilen
[X] Passwortvergabe
[X] Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
[X] Authentifikation mit OTP Verfahren (OneTimePassword)
[X] Authentifikation mit Benutzername / Passwort
[X] Zuordnung von Benutzerprofilen zu IT-Systemen
[X] Einsatz von VPN-Technologie bei der Übertragung von Daten
[X] Verschlüsselung mobiler IT-Systeme
[X] Verschlüsselung mobiler Datenträger
[X] Verschlüsselung der Datensicherungssysteme
[X] Sperren externer Schnittstellen (USB etc.)
[X] Einsatz von Intrusion-Detection-Systemen
[X] Einsatz von Anti-Viren-Software
[X] Verschlüsselung von Datenträgern in Laptops / Notebooks
[X] Einsatz einer Hardware-Firewall
[X] Einsatz einer Software-Firewall
[X] MFA für VPN-Zugänge
[X] MFA für administrative Cloud-Dienste
[X] Rollenbasierte Berechtigungskonzepte
[X] Trennung von Benutzer- und Administratorkonten

Es wurden folgende Maßnahmen getroffen, 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

Zugriffskontrolle

[X] Berechtigungskonzept
[X] Verwaltung der Rechte durch Systemadministrator
[X] regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. Bei Ausscheiden von Mitarbeitern o.Ä.)
[X] Anzahl der Administratoren ist das „Notwendigste“ reduziert
[X] Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
[X] Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
[X] Sichere Aufbewahrung von Datenträgern
[X] physische Löschung von Datenträgern vor Wiederverwendung
[X] ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
[X] Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
[X] Regelmäßige Überprüfung von Berechtigungen
[X] Protokollierung administrativer Tätigkeiten
[X] Verwendung persönlicher Administratorkonten
[X] Dokumentierte Vergabe privilegierter Rechte

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

Auftragskontrolle

[X] Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
[X] vorherige Prüfung der und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag)
[X] Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis
[X] Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der
Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur
Kenntnis genommen werden können

Transport- bzw. Weitergabekontrolle

[X] Einsatz von VPN-Tunneln
[X] Verschlüsselung der Kommunikationswege (z.B. Verschlüsselung des EMail-Verkehrs)
[X] Verschlüsselung physischer Datenträger bei Transport
[X] VPN-gesicherte Fernwartungszugriffe

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Datensicherungen können auf lokalen Backupsystemen innerhalb der Rechenzentrumsinfrastruktur sowie auf räumlich getrennten Speichersystemen oder Cloudspeichern gespeichert werden. Soweit technisch und vertraglich vorgesehen, erfolgt eine zusätzliche Aufbewahrung von Datensicherungen an einem räumlich getrennten Standort zur Verbesserung der Ausfallsicherheit und Wiederherstellbarkeit.

Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

[X] Unterbrechungsfreie Stromversorgung (USV)
[X] Klimatisierung der Serverräume
[X] Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
[X] Schutzsteckdosenleisten in Serverräumen
[X] Feuer- und Rauchmeldeanlagen in Serverräumen
[X] Feuerlöschgeräte in oder vor Serverräumen
[X] Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
[X] Erstellen eines Backup- & Recoverykonzepts
[X] Testen von Datenwiederherstellung
[X] Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
[X] In Hochwassergebieten: Serverräume über der Wassergrenze
[X] Veeam Backup & Replication
[X] Nakivo Backup & Replication
[X] Proxmox Backup Server
[X] Regelmäßige Wiederherstellungstests
[X] Speicherung von Datensicherungen auf lokalen Backup- und/oder S3-kompatiblen Speichersystemen
[X] Verschlüsselte Übertragung von Datensicherungen

Folgende Maßnahmen gewährleisten die Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Incident-Response-Management

[X] Einsatz von WatchGuard Firewalls mit Total Security Services und regelmäßige Aktualisierung
[X] Intrusion Prevention System (IPS)
[X] Einsatz von Spamfilter und regelmäßige Aktualisierung
[X] Einsatz von Virenscanner und regelmäßige Aktualisierung
[X] DNS Security
[X] Application Control
[X] WebBlocker
[X] Server-Eye Monitoring und Alarmierung

Folgende Maßnahmen 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.

Eingabekontrolle

[X] Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
[X] Manuelle oder automatisierte Kontrolle der Protokolle

E-Mail-Sicherheit

Zum Schutz elektronischer Kommunikation werden technische und organisatorische Maßnahmen eingesetzt, um die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von E-Mail-Nachrichten sicherzustellen. Hierzu werden mehrstufige Verfahren zur Erkennung und Abwehr von Schadsoftware, Spam-Nachrichten, Phishing-Angriffen und sonstigen unerwünschten Kommunikationsinhalten eingesetzt.

Die eingesetzten Maßnahmen dienen insbesondere dem Schutz personenbezogener Daten vor unbefugtem Zugriff, Manipulation, Verlust oder unbefugter Offenlegung während der Übertragung und Speicherung.

Hierzu gehören insbesondere:

[X] Einsatz von Tobit David Mailservern
[X] Einsatz von ASSP Spamfilter
[X] Graylisting-Verfahren
[X] Virenschutz
[X] Spamfilterung
[X] TLS-Verschlüsselung
[X] SPF-, DKIM- und DMARC-Unterstützung (soweit implementiert)

Fernwartung und Remote Administration

Zur Erbringung von Support-, Wartungs-, Administrations- und Entstörungsleistungen kann der Auftragsverarbeiter auf Systeme des Auftraggebers mittels Fernzugriff zugreifen. Fernzugriffe erfolgen ausschließlich durch autorisierte Mitarbeiter und nur soweit dies zur Erfüllung der vertraglich vereinbarten Leistungen erforderlich ist.

Die eingesetzten Fernwartungs- und Administrationsverfahren gewährleisten eine sichere Authentifizierung der zugreifenden Personen sowie die verschlüsselte Übertragung sämtlicher Kommunikationsdaten. Administrative Tätigkeiten werden soweit technisch möglich nachvollziehbar dokumentiert.

Hierzu gehören insbesondere:

[X] Fernwartung ausschließlich über verschlüsselte Verbindungen
[X] VPN-Zugänge mit MFA
[X] Protokollierung administrativer Tätigkeiten
[X] Zugriff nur durch autorisierte Mitarbeiter
[X] Dokumentierte Berechtigungskonzepte

Überprüfung, Evaluierung und Anpassung der technischen und organisatorischen Maßnahmen

Die Wirksamkeit, der durch den Auftragsverarbeiter verantworteten, technischen und organisatorischen Maßnahmen, wird regelmäßig, mindestens einmal jährlich sowie anlassbezogen überprüft und bewertet.

Soweit Leistungen oder Infrastrukturen durch Unterauftragsverarbeiter oder Rechenzentrumsbetreiber bereitgestellt werden, erfolgt die Überprüfung auf Grundlage geeigneter Nachweise, vertraglicher Vereinbarungen, Zertifizierungen, Dokumentationen oder sonstiger vom jeweiligen Anbieter bereitgestellter Informationen.

Erforderliche Anpassungen der technischen und organisatorischen Maßnahmen werden unter Berücksichtigung des Stands der Technik, organisatorischer Änderungen sowie gesetzlicher Anforderungen vorgenommen.

ANLAGE 3 – Unterauftragsverarbeiter

Zur Erbringung der vertraglich vereinbarten Leistungen kann der Auftragsverarbeiter weitere Dienstleister als Unterauftragsverarbeiter im Sinne des Art. 28 DSGVO einsetzen.

Die nachfolgend aufgeführten Unternehmen werden vom Auftragsverarbeiter regelmäßig im Rahmen der Leistungserbringung eingesetzt und können dabei – abhängig von der konkret beauftragten Leistung – Zugriff auf personenbezogene Daten erhalten oder personenbezogene Daten im Auftrag verarbeiten.

Der Auftragsverarbeiter stellt sicher, dass mit allen eingesetzten Unterauftragsverarbeitern die nach Art. 28 DSGVO erforderlichen Vereinbarungen abgeschlossen wurden und die datenschutzrechtlichen Anforderungen eingehalten werden.

Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind nachfolgend aufgeführt:

(Unternehmens-) Name	Beschreibung der Leistung	Ort der Leistungserbringung
n@work Internet Informationssysteme GmbH	Bereitstellung - Rechenzentrum - Housing - Internetanbindung	Wendenstraße 379 & Grevenweg 120, 20537 Hamburg 20537 Hamburg
Microsoft Ireland Operations Ltd.	- Microsoft 365 - Exchange Online - Microsoft Teams - Azure-Dienste (soweit genutzt)	EU-Rechenzentren gemäß Microsoft DPA
Server-Eye GmbH	- Monitoring - Alarmierung - Remote Management	Vom Anbieter betriebene Rechenzentren innerhalb der Europäischen Union
TeamViewer Germany GmbH	- Fernwartung und Remote Support	Deutschland / EU entsprechend den Herstellerangaben
Wasabi Technologies LLC	- Cloud Object Storage - S3-kompatibler Speicher - Datensicherungen - Backup-Archivierung	EU-Rechenzentren gemäß der vom Auftragnehmer genutzten Speicherregionen (derzeit Frankfurt am Main, Deutschland, soweit verwendet)

Kundenspezifische Unterauftragsverarbeiter

Abhängig von den durch den Auftraggeber beauftragten Leistungen oder den technischen Anforderungen der jeweiligen Kundenumgebung können weitere Unterauftragsverarbeiter eingesetzt werden.

Solche Unterauftragsverarbeiter können sowohl durch den Auftragnehmer vorgeschlagen oder beauftragt als auch durch den Auftraggeber vorgegeben oder benannt werden.

Soweit zusätzliche Unterauftragsverarbeiter im Rahmen der Leistungserbringung eingesetzt werden, informieren sich Auftraggeber und Auftragnehmer gegenseitig hierüber in angemessener Form. Der Auftragnehmer stellt sicher, dass die datenschutzrechtlichen Anforderungen gemäß Art. 28 DSGVO eingehalten werden und – soweit erforderlich – entsprechende Vereinbarungen mit den eingesetzten Unterauftragsverarbeitern bestehen.

Der Auftraggeber wird über die Hinzuziehung weiterer Unterauftragsverarbeiter informiert. Sofern gesetzlich oder vertraglich erforderlich, erfolgt die Einholung einer Zustimmung oder die Einräumung eines Widerspruchsrechts gemäß den Bestimmungen dieser Vereinbarung. Weitere Unterauftragsverarbeiter können insbesondere im Bereich Cloud-Dienste, Hosting, Datensicherung, Archivierung, Kommunikationsdienste, Monitoring, Fernwartung oder sonstiger IT-Dienstleistungen eingesetzt werden.