vyble® Auftragsdatenverarbeitungsvereinbarung (AVV)

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus § 14 der Allgemeinen Geschäftsbedingungen der vyble GmbH (nachfolgend „AGB“) ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit der Nutzung der vyble® HR-Plattform in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (nachfolgend auch „Daten“) des Auftraggebers bzw. von Beschäftigten des Auftraggebers für Zwecke des Beschäftigungsverhältnisses verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1. Aus den Vertragsgrundlagen ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

   a) Art der Daten:
   - Name, Geburtsname, Geburtsdatum, Geburtsort, Wohnanschrift, Personalnummer, Versicherungsnummer gemäß Sozialversicherungsausweis, Berufsbezeichnung, Steuerklasse, Konfessionszugehörigkeit, Konfessionszugehörigkeit Ehepartner, Anzahl der Kinder, Name der Kinder, Geburtsdatum der Kinder, Arbeitnehmernummer, Staatsangehörigkeit, Kontoverbindung, Ausbildungsinformationen, Steuernummer, Krankenkasse, Gehalt, Stundenlohn, Arbeits- und Fehlzeiten, Steueridentifikationsnummer, Vermögenswirksame Leistungen, betriebliche Altersvorsorge, Firmenfahrzeug, Schwerbehinderung, Pfändung, Aufenthaltserlaubnis, Benefits, Anstellungsverträge, Geburtsurkunden, Nachweise für Erstattungen im Rahmen der Lohn- und Gehaltsabrechnung, Lohnsteuerbescheinigungen, Krankenscheine Arbeitnehmer, Krankenscheine Kinder des Arbeitnehmers

   b) Art und Zweck der Datenverarbeitung:
   - das Erheben der Daten, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderungen, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

   c) Kategorien der betroffenen Personen:
   - Arbeitgeber, Arbeitnehmer, Ehepartner der Arbeitnehmer, Kinder der Arbeitnehmer

   d) Laufzeit
   - Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit der Vertragsgrundlage, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Pflichten ergeben.

2. Der Auftraggeber kann die Vertragsgrundlage jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

§ 2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Angebot konkretisiert sind. Der Auftraggeber ist im Rahmen der Vertragsgrundlage für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 EU-DSGVO bzw. § 26 BDSG und die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 EU-DSGVO bzw. §§ 32 bis 37 BDSG allein verantwortlich (Verantwortlicher im Sinne des Art. 4 Nr. 7 EU-DSGVO).
2. Die Weisungen werden anfänglich durch die Vertragsgrundlage festgelegt und können vom Auftraggeber danach in schriftlicher oder elektronischer Form (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die in der Vertragsgrundlage nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne von Artikel 28 Abs. 3 lit. a) EU-DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
2. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.
3. 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 EU-DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.
   Das im Anhang A beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.
   Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
4. Der Auftragnehmer unterstützt den Auftraggeber, soweit in den AGB vereinbart, im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gemäß Kapitel III der EU-DSGVO bzw. Teil 2 Kapitel 2 BDSG sowie bei der Einhaltung der in Art. 33 bis 36 EU-DSGVO genannten Pflichten.
5. Der Auftragnehmer gewährleistet, dass er die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter sowie andere für den Auftragnehmer tätige Personen vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und es diesen 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 Auftragsverhältnisses fort.
6. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
7. 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.
8. Der Auftragnehmer gewährleistet seinen Pflichten nach Art. 32 Abs. 1 lit. d) EU- DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
9. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist oder wenn dies in der Vertragsgrundlage vereinbart 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.
10. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe; Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren.
11. Daten, Datenträger sowie sämtliche sonstige Materialien, die im Zusammenhang mit dem Auftragsverhältnis stehen, sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder datenschutzgerecht zu löschen bzw. zu vernichten/ vernichten zu lassen. Gleiches gilt für Test- und Ausschussmaterial. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung/ Vernichtung der Daten, trägt diese der Auftraggeber.
12. Nach Auftragsende gewährt der Auftragnehmer einen Zeitraum von 4 Wochen, in dem der Auftraggeber sämtliche Daten selbstständig herunterladen/ exportieren kann. Spätestens 6 Monate nach Auftragsende werden die Daten vom

Auftragnehmer unwiderruflich gelöscht. Abweichende Vereinbarungen zwischen Auftragnehmer und Auftraggeber bedürfen der Schriftform

13. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 EU-DSGVO verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 4 Pflichten des Auftraggebers

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

§ 5 Weisungsberechtigte, Weisungsempfänger

1. Der Auftraggeber benennt dem Auftragnehmer die weisungsberechtigten Personen des Auftraggebers (Vorname, Name, Organisationseinheit, Telefon).
2. Der Auftragnehmer benennt dem Auftraggeber die weisungsempfangsberechtigten Personen beim Auftragnehmer (Vorname, Name, Organisationseinheit, Telefon).
3. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind der anderen Partei unverzüglich schriftlich oder in Textform die Nachfolger bzw. die Vertreter mitzuteilen.

§ 6 Anfragen betroffener Personen

Der Auftraggeber hat den Auftragnehmer unverzüglich und 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.

§ 7 Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach.
   Zum Nachweis der Einhaltung der vereinbarten Pflichten kann der Auftragnehmer dem Auftraggeber folgende Informationen zur Verfügung stellen (alternativ):
   - mindestens jährlich Durchführung eines Selbstaudits zur Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen unter Mitteilung des Ergebnisses samt vollständigem Auditbericht,
   - unternehmensinterne Verhaltensregeln einschließlich eines externen Nachweises über deren Einhaltung (z.B. von Datenschutzbeauftragten, IT- Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren),
   - Zertifikat zu Datenschutz und/oder Informationssicherheit (z.B. ISO 27001),
   - genehmigte Verhaltensregeln nach Art. 40 EU-DSGVO, oder
   - Zertifikate nach Art. 42 EU-DSGVO.
4. 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 in der Vertragsgrundlage vereinbart ist. Der Aufwand einer Inspektion ist für den Auftragnehmer auf den angemessenen und erforderlichen Umfang sowie grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

5. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Ziff. 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.

§ 8 Subunternehmer (weitere Auftragsverarbeiter)

1. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der in der Vertragsgrundlage vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.
2. Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Über die Hinzuziehung oder Ersetzung von Subunternehmern informiert der Auftragnehmer den Auftraggeber.
3. Der Auftraggeber kann gegen derartige Änderungen innerhalb einer angemessenen Frist aus wichtigem Grund gegenüber dem Auftraggeber Einspruch erheben (Art. 28 Abs. 2 Satz 2 EU-DSGVO). Erfolgt kein Einspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor und ist eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich, hat der Auftraggeber das Recht zur außerordentlichen Kündigung der Vertragsgrundlage.
4. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. EU-DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
5. Zurzeit sind für den Auftragnehmer die in Anhang B mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.
6. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden.

§ 9 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 EU-DSGVO liegen.
7. Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in elektronischer Form (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.
8. Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen der AGB vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
9. Es gilt deutsches Recht.

§ 10 Haftung und Schadensersatz

Eine zwischen den Parteien im Vertragswerk vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, sofern und soweit in dieser Vereinbarung nicht ausdrücklich anderes vereinbart ist.

§ 11 Sonstiges

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind vom Auftragnehmer entsprechend der jeweiligen gesetzlichen oder vertraglich vereinbarten Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Anlage A – Technisch organisatorische Maßnahmen nach Art. 32 EU-DSGVO

Zutrittskontrolle

Da die Daten der Auftraggeber, wie angegeben, auf dem Frankfurter Server von Amazon Web Services gespeichert werden, erfüllen wir ausschließlich die Standarderfordernisse bzgl. der Zutrittskontrolle.

Unbefugten ist der Zutritt zu unseren Geschäftsräumen nicht möglich. Die Räume sind durch ein Sicherheitsschlosssystem gesichert. Die Mitarbeiter erhalten codierte Sicherheitsschlüssel, deren Erhalt sie unterzeichnen und welche sie nach Beendigung des Arbeitsverhältnisses wieder abgeben müssen. Unsere Geschäftsräume sind stets verschlossen. Dritte werden nach Anmeldung am Eingang abgeholt und nach dem Termin wieder zum Ausgang geleitet.

Weiter werden unsere Geschäftsräume durch ein Kamerasystem überwacht, welches bei Aktivierung zu ungewöhnlichen Zeiten direkt Alarm an den Sicherheitsbeauftragten gibt.

Wir verpflichten ebenso unsere Subunternehmer, die im Rahmen dieses Auftrags tätig werden, zu angemessenen Maßnahmen zur Zutrittskontrolle. Dazu gehört insbesondere, dass in Sicherheitsbereiche wie Serverräumen oder Rechenzentren nur autorisierte Mitarbeiter Zutritt erhalten.

Zugangskontrolle

Es wird bei uns verhindert, dass Unberechtigte unsere Datenverarbeitungssysteme nutzen können. Hierbei unterscheiden wir zwischen dem Zugang zu unseren lokalen Datenverarbeitungssystemen, dem Datenzugang über unsere Software sowie dem Zugang zu den externen Datenverarbeitungssystemen.

lokale Datenverarbeitungssysteme:
Zu unseren lokalen Datenverarbeitungssystemen haben nur die jeweiligen Mitarbeiter einen passwortgesicherten Zugang. In der Abwesenheit der Nutzer meldet sich das System automatisch ab. Es wurden Standardsicherheitsmaßnahmen gegen Fremdzugriffe getroffen. Ebenso sind kabellose Internetverbindungen WPA2-passwortgesichert.

Zugang zu den Daten innerhalb der Software:
Der Auftraggeber sowie bestimmte Mitarbeiter erhalten Zugänge zu unserer Software, in welcher Daten abrufbar sind. Es ist hierfür ein entsprechender Benutzerstammsatz eingerichtet. Der Zugang zu dem System erfolgt mittels einer authentifizierten E-Mail-Adresse des Nutzers, eines selbstgewählten
Passwortes (technisch erzwungen: 8 Zeichen, Zahlen, Buchstaben und Sonderzeichen; Speicherung via PBKD5-Hash (SHA256)). Administratormitarbeiter müssen in einem regelmäßigen Turnus ihre Passwörter ändern. Die Passwörter können via E-Mail-Reset-Link oder die Passwörter der Mitarbeiter des Auftraggebers durch den

Auftraggeber selbst zurückgesetzt werden. Zudem kann der Auftraggeber alternativ zu dem Login-Verfahren das Single-Sign-On via Google aktivieren. Die Logins im Admin- und Kundensystem werden stets protokolliert und sind jederzeit nachvollziehbar. Das System bietet einen automatischen Schutz vor DDOS-Angriffen. Dazu wird der Account nach einer bestimmten Anzahl von vergeblichen Login-Versuchen gesperrt. Zudem besteht für die Applikationsserver eine virtuelle Firewall.

Zugang zum externen Datenverarbeitungssystemen (Server):
Der Zugang zum externen Datenverarbeitungssystem beim Auftragnehmer ist auf eine konkludente Anmeldung von zwei bestimmten Personen begrenzt (4-Augen-Prinzip). Für den Zugang ist eine verschlüsselte Verbindung (SSH) notwendig sowie die Nutzung zweie passwortgeschützte versteckte personell getrennte Tokens. Ebenso werden diese Logins protokolliert.

Zugriffskontrolle

Die unerlaubte Tätigkeit in den Datenverarbeitungssystemen außerhalb der eingeräumten Berechtigungen wird verhindert. Die Kundendaten sind auf Datenbankebene (Multi-Tenant-System) getrennt. Zudem wurde ein konfigurierbares Berechtigungskonzept zur Verwaltung verschiedener Zugriffsrechte der einzelnen Nutzer erstellt. Jegliche Zugriffe der Nutzer werden umfänglich protokolliert. Änderungen an Daten können auf Weisung des Auftraggebers zurückgesetzt werden. Zudem erfolgt im System keine Löschung von Daten, sondern lediglich eine Datensperrung – die Löschung erfolgt nur, wie im Vertrag bezeichnet, auf besondere Weisung des Auftraggebers.

Weitergabekontrolle

Die elektronische Übertragung von Daten erfolgt ausschließlich über eine verschlüsselte SSL-Verbindung, welche ebenso umfassend protokolliert wird. Es erfolgt kein physikalischer Datentransport.

Eingabekontrolle

Jegliche Benutzerzugriffe sowie Änderungen an Daten werden mit Datum und Uhrzeit protokolliert. Hierbei kann genau zugeordnet werden, welcher Nutzer welche Änderungen vorgenommen hat. Zudem sind die Eingabemöglichkeiten der einzelnen Nutzer durch das konfigurierbare Rollensystem einschränkbar.

Auftragskontrolle

Alle Mitarbeiter wurden bezüglich des Datenschutzes, der IT-Sicherheit und der rollenspezifischen Verhaltensregeln umfassend geschult und zum Datengeheimnis gemäß § 5 BDSG verpflichtet. Weiter wird die weisungsgemäße Auftragsdatenverarbeitung wie im Vertrag spezifiziert gewährleistet. Zudem werden Dritte, die mit Durchführung einzelner Auftragsdatenverarbeitungen beauftragt werden dementsprechend verpflichtet.

Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle erfolgt entsprechend der Durchführung unseres Partners Amazon Web Services, welcher mehrfach zertifiziert und überprüft wurde. Mehr Informationen zum Datenschutz bei AWS erhalten Sie hier: https://aws.amazon.com/de/data-protection/

Trennungskontrolle

Wir nehmen die Datentrennung sehr ernst. Der Betrieb von Produktiv- und Testsystemen erfolgt bei uns auf getrennten Servern. Zudem sind alle Kundendaten auf getrennten Datenbankebenen (Multi-Tenant-System) gespeichert.

vyble® Auftragsdatenverarbeitungsvereinbarung (AVV)

Anlage B – über Subunternehmer des Auftragsverarbeiters

Subunternehmer	Auftragsinhalt	Beschreibung
Amazon Web Services EMEA SARL, Niederlassung Deutschland Marcel-Breuer-Str. 12, 80807 München, Deutschland, eingetragen im Handelsregister des Amtsgerichts München unter HRB 242240, USt-ID: DE317013094 Zweigniederlassung der **Amazon Web Services EMEA SARL** 38 Avenue John F. Kennedy, L-1855 Luxembourg, eingetragen im Luxemburgischen Handelsregister unter R.C.S. B186284	**Cloud-Computing-Provider** Bereitstellung von Rechenleistung und Storage-Kapazitäten	Die Speicherung sowie die Verarbeitung der Daten erfolgt ausschließlich auf Servern in Frankfurt am Main, Deutschland. Weitere Details sind dem Whitepaper AWS bei vyble® zu entnehmen.