VEREINBARUNG AUFTRAGSVERARBEITUNG HINWEISGEBERSYSTEM

Die Compliance.One GmbH (nachfolgend „Auftragnehmer“ oder „Compliance.One“) stellt dem Auftraggeber ihr digitales Hinweisgebersystem (nachfolgend „Hinweisgebersystem“) als SaaS zur Verfügung. Der Auftraggeber nutzt das Hinweisgebersystem, um Beschäftigten und evtl. sonstigen Dritten die anonyme oder vertrauliche Meldung von potenziellen Compliance-Verstößen im Unternehmen zu ermöglichen. Das Hinweisgebersystem verarbeitet die im Rahmen der Abgabe von Meldungen erhobene Daten dabei im Auftrag des Auftraggebers. Diese Vereinbarung Auftragsverarbeitung konkretisiert, als Teil des Hauptvertrages zwischen den Parteien, die Verpflichtungen beider Parteien zur Einhaltung des anwendbaren Datenschutzrechts, insbesondere der Anforderungen der Datenschutzgrundverordnung („DSGVO“).

1. Hinweisgebersystem

Bei einer **anonymen Meldung** geben die hinweisgebenden Personen weder Namen noch Kontaktdaten an.

Bei einer **pseudonymen Meldung** liegen nur Compliance.One die Kontaktdaten der hinweisgebenden Personen vor, diese werden dem Auftraggeber gegenüber jedoch nicht offengelegt. Der Auftraggeber weist Compliance.One unwiderruflich an, bei einer pseudonymen Meldung personenbezogen Daten, die eine Identifikation der hinweisgebenden Person ermöglichen, weder ihm gegenüber noch einem Dritten gegenüber offenzulegen.

Bei einer **transparenten Meldung** erhält die beim Auftraggeber für die Bearbeitung von Meldungen zuständige interne Meldestelle Zugriff auf die Daten zur Identität der hinweisgebenden Person und kann unmittelbar mit der hinweisgebenden Person kommunizieren. Der Auftraggeber ist dabei gesetzlich verpflichtet, die Vertraulichkeit der Identität der hinweisgebenden Person zu wahren, dementsprechend dürfen grundsätzlich nur die Beschäftigten der internen Meldestelle beim Auftraggeber, die die jeweilige Meldung bearbeiten, die Identität der hinweisgebenden Person kennen.

Für die Zurverfügungstellung der Hinweisgeberseite ist es zudem erforderlich, dass für die Dauer des Aufrufs der Hinweisgeberseite **personenbezogene Daten technischer Natur** (IP-Adresse und Geräteinformationen) verarbeitet werden. Diese personenbezogenen Daten werden nur für die Dauer des Aufrufs der Hinweisgeberseite verarbeitet. Die IP-Adresse wird in den Logfiles anonymisiert (Ersetzung des letzten Oktetts der IP-Adresse durch „xxxx.xxxx“), die Geräteinformationen werden nicht gespeichert.

2. Anwendungsbereich

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in der Leistungsvereinbarung und in **Anlage 1** zu dieser Vereinbarung Auftragsverarbeitung festgelegt.

3. Weisungsgebundenheit

3.1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in Textform geändert, ergänzt oder ersetzt werden, sofern sie nicht unwiderruflich erteilt wurden. Mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen.

3.2 Falls der Auftragnehmer verpflichtet ist, personenbezogene Daten nach dem Recht der Union oder des Mitgliedstaates, dem der Auftragnehmer unterliegt, zu verarbeiten, wird der Auftragnehmer den Auftraggeber hierüber vor der jeweiligen Verarbeitung schriftlich informieren, es sei denn, das Gesetz verbietet solche Informationen aus wichtigen Gründen des öffentlichen Interesses. Im letztgenannten Fall wird der Auftragnehmer den Auftraggeber unverzüglich informieren, sobald ihm dies rechtlich möglich ist.

3.3 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.

4. Technische und organisatorische Maßnahmen

4.1 Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

4.2 Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist in **Anlage 2** zu dieser Vereinbarung Auftragsverarbeitung und ergänzend in der technischen Übersicht der Applikation in **Anlage 3** dokumentiert. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftraggeber kann jederzeit eine aktuelle Übersicht, der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

5. Betroffenenrechte

5.1 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO (insb. Auskunft, Berichtigung, Sperrung oder Löschung). Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

5.2 Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird der Auftragnehmer unverzüglich an den Auftraggeber weiterleiten.

5.3 Bei pseudonymen Meldungen erteilt der Auftraggeber dem Auftragnehmer die Weisung, der hinweisgebenden Person gegenüber die Betroffenenrechte unmittelbar direkt zu erfüllen.

6. Sonstige Pflichten des Auftragnehmers

6.1 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, spätestens innerhalb von 24 Stunden, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

6.2 Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie erforderlichenfalls bei Durchführung einer Datenschutzfolgenabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind dem Auftraggeber auf Anforderung unverzüglich zur Verfügung zu stellen.

6.3 Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer, den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

6.4 Die beim Auftragnehmer zur Verarbeitung eingesetzten Personen haben sich schriftlich zur Vertraulichkeit verpflichtet, wurden mit den relevanten Bestimmungen des Datenschutzes vertraut gemacht und werden hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht.

6.5 Der Auftragnehmer wird den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unterstützen.

6.6 Der Auftraggeber kann sich bei Fragen zum Datenschutz beim Auftragnehmer jederzeit an den Datenschutzbeauftragten des Auftragnehmers wenden. Datenschutzbeauftragter des Auftragnehmers ist Rechtsanwalt Conrad Graf, E-Mail privacy@compliance.one.

7. Rechte und Pflichten des Auftraggebers

7.1 Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

7.2 Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer, soweit erforderlich und möglich, Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen des Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers sowie nicht häufiger als alle 12 Monate statt.

8. Unterauftragsverarbeiter

8.1 Die Beauftragung von Unterauftragsverarbeitern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers zulässig.

8.2 Der Auftraggeber stimmt der Beauftragung von Unterauftragsverarbeitern gemäß der Übersicht Unterauftragsverarbeiter, anbei als **Anlage 4**, zu. In der Übersicht Unterauftragsverarbeiter ist auch der Prozess für zukünftige Änderungen der Unterauftragsverarbeiter definiert.

8.3 Der Auftragnehmer hat die Unterauftragsverarbeiter sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass diese die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten können. Der Auftragnehmer hat insbesondere zu kontrollieren, dass sämtliche Unterauftragsverarbeiter die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen haben.

8.4 Nicht als Unterauftragsverhältnisse im Sinne dieser Vereinbarung Auftragsverarbeitung sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen und Bewachungsdienste.

8.5 Die Beauftragung von Unterauftragsverarbeitern lässt die vertraglichen und datenschutzrechtlichen Verpflichtungen des Auftragnehmers gegenüber dem Auftraggeber unberührt. Der Auftragnehmer haftet für eventuelle Schlechtleistungen eines Unterauftragsverarbeiters wie für eigenes Verschulden.

9. Datenübermittlung in Drittländer

Die Auftragsverarbeitung erfolgt ausschließlich innerhalb der Europäischen Union bzw. des EWR und/oder in Drittländern, für die ein Angemessenheitsbeschluss der EU-Kommission vorliegt. Eine Verlagerung der Auftragsverarbeitung in ein „unsicheres“ Drittland bedarf der ausdrücklichen Genehmigung des Auftraggebers.

10. Löschung und Rückgabe von personenbezogenen Daten

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2 Nach Beendigung der Leistungsvereinbarung oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer die im Auftrag verarbeiteten personenbezogenen Daten dem Auftraggeber auszuhändigen oder datenschutzgerecht zu löschen.

10.3 Von der Aushändigung ausgenommen sind pseudonyme Meldungen. Diese werden dem Auftraggeber anonymisiert zur Verfügung gestellt oder gelöscht.

10.4 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

ANLAGE 1: BESCHREIBUNG DER AUFTRAGSVERARBEITUNG

Verantwortlicher und Auftragsverarbeiter

Der Auftraggeber ist Verantwortlicher im Sinne der DSGVO und nutzt das Hinweisgebersystem des Auftragnehmers, um seinen Beschäftigten und sonstigen Dritten die Meldung von potenziellen Compliance-Verstößen im Unternehmen zu ermöglichen.

Der Auftragnehmer stellt als Auftragsverarbeiter dem Auftraggeber das Hinweisgebersystem als Software-as-a-Service (SaaS) zur Verfügung.

Betroffene

Die im Auftrag verarbeiteten personenbezogenen Daten betreffen hinweisgebende Personen, die das Hinweisgebersystem nutzen, um vertraulich potenzielle Compliance-Verstöße im Unternehmen des Auftraggebers zu melden. Der Auftraggeber entscheidet dabei, ob er das Hinweisgebersystem nur seinen Beschäftigten oder auch sonstigen Dritten (Kunden, Lieferanten etc.) zur Verfügung stellt.

Des Weiteren verarbeitet der Auftragnehmer personenbezogene Daten der Personen, die im Rahmen einer Meldung von der hinweisgebenden Person angegeben werden, z. B. als Beschuldigte eines potenziellen Compliance-Verstoßes oder in sonstigem Kontext.

Kategorien von Daten

Im Rahmen der Auftragsverarbeitung werden die personenbezogenen Daten verarbeitet, die die hinweisgebende Person im Rahmen seiner Meldung mitteilt und/oder die im Rahmen der Folgemaßnahmen erhoben und im Hinweisgebersystem erfasst werden.

Dies können sein:

- Name;
- Adresse;
- Arbeitgeber bzw. Niederlassung, in der die Tätigkeit ausgeübt wird;
- E-Mail-Adresse; Telefon-/Mobilfunknummer;
- Funktion im Unternehmen bzw. Beziehung zum Auftraggeber;
- Daten der eines potenziellen Compliance Verstoßes Beschuldigten;
- Inhalte der Meldungen;
- sonstige Daten, die dem Auftragnehmer vom Auftraggeber für die Durchführung seiner Leistungen zur Verfügung gestellt werden bzw. die im Rahmen der Durchführung der Leistungen des Auftragnehmers vom Auftragnehmer für den Auftraggeber erhoben werden;
- technische Informationen, die erforderlich sind für die Zurverfügungstellung der Hinweisgeberseite (IP-Adresse und Geräteinformationen).

Besondere Kategorien personenbezogener Daten

Die im Auftrag verarbeiteten personenbezogenen Daten können besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO (z.B. Gesundheitsdaten) enthalten, wenn solche Daten in einer Meldung enthalten sind bzw. im Rahmen von Folgemaßnahmen erhoben und im Hinweisgebersystem erfasst werden.

Gegenstand und Dauer der Verarbeitung

Die im Auftrag verarbeiteten personenbezogenen Daten werden verarbeitet zur Durchführung der im Hauptvertrag bzw. der Vereinbarung Auftragsverarbeitung vereinbarten Leistungen des Auftragnehmers. Die Daten werden auf Weisung des Auftraggebers verarbeitet, wie in der Vereinbarung Auftragsverarbeitung definiert.

Die Daten werden, wie oben definiert, jederzeit auf Weisung des Auftraggebers gelöscht. Der Auftraggeber kann zudem spezifische Aufbewahrungs- und Löschfristen definieren. Die Daten werden bei Vertragsbeendigung gelöscht.

Der Auftraggeber kann die Daten jederzeit exportieren (mit Ausnahme der Daten zur Identität der hinweisgebenden Person bei pseudonymen Meldungen, die gemäß der spezifischen Weisung bezüglich pseudonymer Meldungen verarbeitet werden).

Die Laufzeit dieser Vereinbarung Auftragsverarbeitung richtet sich nach der Laufzeit der Leistungsvereinbarung.

ANLAGE 2: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Hinsichtlich der technischen und organisatorischen Maßnahmen wird grundsätzlich auf die ISO 27001-Zertifizierung der Compliance.One GmbH verwiesen. Das Zertifikat steht unter www.compliance.one/legal zur Verfügung. In Ergänzung zur ISO 27001-Zertifizierung wird im Folgenden ein Überblick über die technischen und organisatorischen Maßnahmen gegeben:

1. VERTRAULICHKEIT

1.1 Zutrittskontrolle

Das Hosting der Software erfolgt in Rechenzentren der Hetzner Online GmbH in Deutschland.

Die in den Rechenzentren des Unterauftragsverarbeiters Hetzner Online GmbH getroffenen technischen und organisatorischen Maßnahmen sind ausführlich hier beschrieben: https://www.hetzner.com/AV/TOM.pdf

1.2 Zugangskontrolle

Für die Zugangskontrolle sind nachfolgende Maßnahmen von Compliance.One getroffen worden:

Der Zugang zu IT-Systemen erfolgt ausschließlich über den Einsatz von SSH-Schlüsseln mit einer Mindestschlüssellänge von 4096 Bit. Jeder Schlüssel ist zusätzlich durch ein sicheres Passwort geschützt. Die Schlüsselpaare werden regelmäßig geprüft und mindestens einmal jährlich erneuert.

Der Zugriff auf produktive Systeme ist ausschließlich über definierte Jumphosts möglich. Direkte Verbindungen aus externen Netzen zu Servern sind grundsätzlich unterbunden, um ein maximales Sicherheitsniveau zu gewährleisten.

Diese Architektur stellt sicher, dass nur autorisierte Nutzer mit zuvor eingerichteten Zugangsschlüsseln und durch zentral gesteuerte Zugangspunkte auf interne Systeme zugreifen können.Remote-Zugriffe auf IT-Systeme von Compliance.One erfolgen stets über verschlüsselte Verbindungen.

Auf den Servern von Compliance.One ist ein Intrusion-Prevention-System im Einsatz. Alle Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist. Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden.

Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.

Alle Beschäftigten sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen. Passwörter werden grundsätzlich verschlüsselt gespeichert.

1.3 Zugriffskontrolle

Berechtigungen für IT-Systeme und Applikationen von Compliance.One werden ausschließlich von Administratorinnen/Administratoren eingerichtet.

Berechtigungen werden grundsätzlich nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind.

Voraussetzung ist eine entsprechende Anforderung der Berechtigung für eine/n Beschäftigte/n durch eine/n Vorgesetzte/n.

Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.

Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren.

Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

1.4 Trennung

Alle von Compliance.One für Auftraggeber eingesetzten IT-Systeme sind mandantenfähig. Die Trennung von Daten von verschiedenen Auftraggebern ist stets gewährleistet.

1.5 Pseudonymisierung & Verschlüsselung

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen. Darüber hinaus werden Daten auf Server- und Clientsystemen auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Festplattenverschlüsselungssysteme im Einsatz.

2. INTEGRITÄT

2.1 Eingabekontrolle

Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die von Compliance.One im Auftrag verarbeitet werden, wird grundsätzlich protokolliert.

Beschäftigte sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

2.2 Weitergabekontrolle

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Auftraggebern von Compliance.One erfolgt, darf jeweils nur in dem Umfang, wie erfolgen, wie dies mit dem Auftraggeber abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Auftraggeber erforderlich ist.

Alle Beschäftigten, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.

Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.

Die Nutzung von privaten Datenträgern ist den Beschäftigten bei Compliance.One untersagt.

Beschäftigte bei Compliance.One werden regelmäßig zu Datenschutzthemen geschult. Alle Beschäftigten sind auf zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

3. VERFÜGBARKEIT UND BELASTBARKEIT

Daten auf Serversystemen von Compliance.One werden mindestens täglich inkrementell und wöchentlich „voll“ gesichert. Die Sicherungsmedien werden verschlüsselt an einen physisch getrennten Ort verbracht.

Das Einspielen von Backups wird regelmäßig getestet.

Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Serverraum befindet sich eine Brandmeldeanlage sowie eine CO2-Löschanlage. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

Es gibt bei Compliance.One einen Notfallplan, der auch einen Wiederanlaufplan beinhaltet.

4. AUFTRAGSKONTROLLE

Die Datenverarbeitung erfolgt ausschließlich in der Europäischen Union.

Bei der Compliance.One ist ein betrieblicher Datenschutzbeauftragter benannt.

Bei der Einbindung von Unterauftragsverarbeitern wird entsprechend den Vorgaben des jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag nach zuvor durchgeführtem Audit durch den Datenschutzbeauftragten von Compliance.One abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

5. PRIVACY BY DESIGN UND PRIVACY BY DEFAULT

Bei Compliance.One wird schon bei der Entwicklung der Software Sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit schon im Zusammenhang mit Benutzer-Interfaces Rechnung getragen wird. So sind z.B. Formularfelder und Bildschirmmasken flexibel gestaltbar.

Die Software von Compliance.One unterstützt die Eingabekontrolle durch einen flexiblen und anpassbaren Audit-Trail, der eine unveränderliche Speicherung von Änderungen an Daten und Nutzerberechtigungen ermöglicht. Berechtigungen auf Daten oder Applikationen können flexibel und granular gesetzt werden.

6. VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

Bei Compliance.One ist ein umfassendes Datenschutzmanagementsystem implementiert. Es gibt eine Leitlinie zu Datenschutz und Informationssicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird. Die Leitlinie und die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.

Es besteht ein Datenschutz- und Informationssicherheits-Team, das Maßnahmen im Bereich von Datenschutz und Informationssicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.

Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Beschäftigten erkannt und unverzüglich dem Team gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Auftraggebern verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.

ANLAGE 3: TECHNISCHE ÜBERSICHT HINWEISGEBERSYSTEM

- **Verschlüsselung auf dem Transportweg**

  Der Auftragnehmer verwendet für alle Zugriffe auf seine Systeme immer SSL bzw. https als Transportlayer. Unsere SSL-Zertifikate haben eine maximale Lebensdauer von 12 Monaten und werden regelmäßig ausgetauscht. Für SSL wird RSA SHA-256 verwendet.

  Hiermit wird sichergestellt das unbefugte keine Daten auf dem Transportweg mitlesen können.

- **Verschlüsselung bei der Ablage**

  Alle Daten werden standardmäßig verschlüsselt abgelegt. Wir verwenden zur Speicherung von Hinweisen und persönlichen Daten hierfür Hashicorp Vault. Daten werden so mit AES256 GCM gespeichert.

  Die Entschlüsselung der Daten und der Zugriff kann nur nach Entsperrung des Vaults mit mindestens drei Schlüsseln (Shamir's Secret Sharing) erfolgen. Diese drei Schlüssel sind auf verschiedene Personen in unserer Organisation verteilt und werden an keiner Stelle zusammen abgelegt.

- **Applikationssicherheit beim Zugriff auf Daten**

  Um die Daten zusätzlich zu schützen, wird für jeden Kunden eine eigene Instanz innerhalb des Vaults angelegt. Jeder einzelne Zugriff wird mit einem Einmalpasswort (Token) geschützt, so dass Applikationszugangsdaten nur für einen Bruchteil einer Sekunde jeweils gültig sind.

  Hiermit stellen wir sicher, dass Passwörter nicht mehrfach verwendet werden können und es Angreifern unmöglich macht diese mehrfach zu verwenden.

- **Authentifizierung**

  Die Authentifizierung gegen unsere öffentlichen Dienste wird durch einen Usernamen + Passwortauthentifizierung geschützt.

  Die Anforderungen an ein Passwort sind mindestens 8 Zeichen, eine Zahl, ein Sonderzeichen und ein Großbuchstabe Passwörter können jederzeit verändert werden. Wir fordern unsere Kunden regelmäßig zum Wechsel des Passworts auf.

  Außerdem loggen wir jeden fehlerhaften Versuch eines Logins und blocken nach einer vorgegebenen Anzahl an fehlerhaften Versuchen den Zugriff.

  Um die Sicherheit unserer Kunden zu erhöhen, bieten wir zusätzlich 2-Faktoren-Authentifizierung. Hierbei unterstützen wir Yubikey Tokens und softwarebasierte Tokens (z.B. Authy oder Google Authenticator).

- **Zugriff auf Server**

  Der Zugriff auf Server ist nur einer sehr kleinen Gruppe von Beschäftigten direkt möglich. Hierbei kommen PKI basierte Zugriffsverfahren (SSH) mit mindestens 4096 Bit Schlüssellänge zum Einsatz.

  Außerdem ist der Zugriff via Firewall nur bestimmten IP-Adressen vorbehalten.

- **Serverstandort und Sicherheitsmaßnahmen vor Ort**

  Alle unsere Server stehen in Rechenzentren in Deutschland. Unsere Rechenzentrum Partner sind DIN ISO/IEC 27001 zertifiziert. Hierzu zählt der Zugriff auf die Hardware, Notstromversorgung, Zugang zum Rechenzentrum und der Betrieb der Infrastruktur.

ANLAGE 4: ÜBERSICHT UNTERAUFTRAGSVERARBEITER

Compliance.One setzt bei der Erbringung der Leistungen aus dem Hauptvertrag folgende Unterauftragsverarbeiter ein:

Unterauftragsverarbeiter	Leistungen des Unterauftragsverarbeiters	Ort der DV
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Deutschland	Hosting des Hinweisgebersystems	EU
Sendinblue GmbH Köpenicker Straße 126, 10179 Berlin, Deutschland	Versand von Transaktionsmails (E-Mail-Versand-Plattform Brevo)	EU
Friendly Captcha GmbH Am Anger 3-5, 82237 Wörthsee, Deutschland	Betrugs- und Bot-Prävention und -Abwehr	EU

Der Auftragnehmer kann die Beauftragung einzelner Unterauftragsverarbeiter beenden oder zusätzliche Unterauftragsverarbeiter beauftragen. Der Auftragnehmer wird den Auftraggeber bei der Beauftragung zusätzlicher Unterauftragsverarbeiter auf elektronischem Wege mindestens 30 Tage vor Einsatz des zusätzlichen Unterauftragsverarbeiters über dessen geplanten Einsatz informieren. Sollte der Auftraggeber einen wesentlichen Grund haben, dem Einsatz eines Unterauftragsverarbeiters zu widersprechen, wird der Auftraggeber dies dem Auftragnehmer spätestens 15 Tage nach der Information über den geplanten Einsatz des Unterauftragsverarbeiters schriftlich und unter Nennung des wesentlichen Grundes mitteilen. Sollte der Auftraggeber innerhalb dieser Zeitspanne nicht widersprechen, so wird der Einsatz des zusätzlichen Unterauftragsverarbeiters als vom Auftraggeber genehmigt angesehen.

Sollte der Auftraggeber widersprechen, kann der Auftragnehmer den Widerspruch wie folgt heilen: (1.) Der Auftragnehmer wird den zusätzlichen Unterauftragsverarbeiter für die Verarbeitung personenbezogener Daten des Auftraggebers nicht einsetzen, oder (2.) der Auftragnehmer wird Maßnahmen ergreifen, um den wesentlichen Grund für den Widerspruch des Auftraggebers auszuräumen, oder (3.) der Auftragnehmer kann die Erbringung des von dem Einsatz des zusätzlichen Unterauftragsverarbeiters betroffenen Aspekts der Leistung gegenüber dem Auftraggeber vorübergehend oder dauerhaft einstellen und dem Auftraggeber die für die Erbringung des Aspekts der Leistung eventuell bereits vorab gezahlte Vergütung zurückerstatten. Sollte keine dieser drei Optionen machbar sein und wurde dem Widerspruch nicht innerhalb von 15 Tagen nach Zugang des Widerspruchs abgeholfen, kann jede Partei den Vertrag mit angemessener Frist außerordentlich kündigen.