Verpflichtungserklärung zur Auftragsverarbeitung nach Art. 28 Abs. 9 DSGVO

Unternehmen
Lukmann Consulting GmbH
Packerstraße 131a
A-8561 Söding

als „**Auftragsverarbeiter**“

verpflichtet sich gegenüber dem **Verantwortlichen** (= Auftraggeber, Kunde) wie folgt:

1. Vertragsgegenstand

a. Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen im Bereich Software as a Service (Compliance-Plattform (im Folgenden kurz „CP“) für die durch den Auftragsverarbeiter angebotenen Dienstleistungen, sowie Support Leistungen für die CP auf Grundlage der AGB abrufbar unter https://www.dsgvoschutzteam.com/agb/ („Hauptvertrag“). Dabei erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Verantwortlichen. Umfang und Zweck der Datenverarbeitung durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag. Dem Verantwortlichen obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

b. Die Laufzeit dieser Verpflichtungserklärung richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen ergeben.

2. Art der verarbeiteten Daten, Kreis der Betroffenen

Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragsverarbeiter Zugriff auf die hier näher spezifizierten personenbezogenen Daten.

Kategorie von Personen	Kategorie von Daten	Zweck der Verarbeitung
User	• Persönliche Identifikationsdaten	• Zuordnung von Aufgaben, Überprüfungen, Verarbeitungen für Verantwortliche, Verarbeitungen für Auftragsverarbeiter, Data Breach, Betroffenenrechte • Übermittlung von Mails zu Tätigkeiten die dem User zugeordnet wurden • Durchführung von Support Leistungen • Protokollierung von Zugriffen und Datenänderungen
Mitarbeiter	• Persönliche Identifikationsdaten	• Zuordnung zu online Trainings inkl. Zertifikaten
Lieferanten	• Persönliche Identifikationsdaten	• Dokumentation von Ansprechpartnern bei Empfängern für Verantwortliche
Kunden	• Persönliche Identifikationsdaten	• Dokumentation von Ansprechpartnern von Kunden für Auftragsverarbeiter

3. Weisungsrecht

a. Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragsverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

b. Der Verantwortliche ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Einschränkung von Daten. Der Verantwortliche wird vor einer solchen Weisung, alle ihm in der Software selbst zur Verfügung stehende Mittel nutzen, bevor er sich an den Auftragsverarbeiter wendet. Soweit einzelne Weisungen den vertraglich vereinbarten Leistungsumfang übersteigen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

c. Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

4. Schutzmaßnahmen des Auftragsverarbeiters

a. Der Auftragsverarbeiter ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Verantwortlichen erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

b. Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen gem. Art.32 DSGVO, insbesondere mindestens die in Anlage 1 aufgeführten Maßnahmen der Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungskontrolle.
Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

c. Den bei der Datenverarbeitung durch den Auftragsverarbeiter beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragsverarbeiter wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im Folgenden „Mitarbeitende“ genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art.28 Abs.3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung des Hauptvertrages oder des Beschäftigungsverhältnisses zwischen den Mitarbeitenden und dem Auftragsverarbeiter bestehen bleiben. Dem Verantwortlichen sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

5. Informationspflichten des Auftragsverarbeiters

a. Der Auftragsverarbeiter führt ein Verzeichnis, zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält.

b. Bei Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragsverarbeiters, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragsverarbeiter den Verantwortlicher unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragsverarbeiters durch die Datenschutz-Aufsichtsbehörde.

c. Über wesentliche Änderung der Sicherheitsmaßnahmen nach Punkt 4. hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu unterrichten.

6. Kontrollrechte des Verantwortlichen

a. Der Verantwortliche kann sich jederzeit vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters überzeugen. Hierfür kann er z. B. Auskünfte des Auftragsverarbeiters einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter steht. Der Verantwortliche wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragsverarbeiters dabei nicht unverhältnismäßig stören. Für die Durchführung einer Prüfung darf der Auftragsverarbeiter eine dem Aufwand entsprechende Vergütung verlangen. Die Durchführung einer Prüfung ist für den Verantwortlichen auf ein Mal pro Kalenderjahr begrenzt.

b. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf dessen schriftliche Anforderung innerhalb einer angemessenen Frist die Ergebnisse seines letzten internen Audits zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters erforderlich sind.

c. Der Auftragsverarbeiter weist dem Verantwortlichen die Verpflichtung der Mitarbeitenden nach Punkt 4. lit c auf Verlangen nach.

7. Einsatz von Subunternehmern

a. Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Anlage 2 genannten Subunternehmer durchgeführt. Der Auftragsverarbeiter ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Er setzt den Verantwortlichen hiervon auf Wunsch in Kenntnis.

b. Der Auftragsverarbeiter ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragsverarbeiter hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Verpflichtungserklärung ebenso zu verpflichten und dabei sicherzustellen, dass der Auftragsverarbeiter seine Rechte aus dieser Verpflichtungserklärung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragsverarbeiter sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragsverarbeiter wird dem Verantwortlichen auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

c. Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Verantwortlichen erbringt und Bewachungsdienste.

8. Anfragen und Rechte Betroffener

a. Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 DSGVO sowie 32 bis 36 DSGVO. Der Verantwortliche wird vor einer Aufforderung zur Unterstützung durch den Auftragsverarbeiter alle ihm in der Software zur Verfügung stehende Mittel nutzen um seinen Pflichten gegenüber dem Betroffenen nachzukommen. Der Auftragsverarbeiter darf für die Unterstützung eine dem Aufwand entsprechende Vergütung verlangen.

b. Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragsverarbeiter geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Verantwortlichen und wartet dessen Weisungen ab.

9. Haftung

a. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragsverarbeiter alleine der Verantwortliche gegenüber dem Betroffenen verantwortlich.

b. Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

10. Beendigung des Hauptvertrags

a. Der Auftragsverarbeiter wird dem Verantwortlichen nach Beendigung des Hauptvertrags und bis 30 Tage nach Beendigung des Hauptvertrages auf dessen Anforderung alle ihm überlassenen Daten in Form von CSV Dateien zurückgeben und sofern nicht nach dem Unionsrecht oder dem Recht der Republik Österreich eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – spätestens 30 Tage nach Beendigung des Hauptvertrages löschen. Spätestens 65 Tage nach Beendigung des Hauptvertrages sind die Daten des Verantwortlichen auch von allen Datensicherungen beim Auftragsverarbeiter gelöscht. Der Auftragsverarbeiter hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

b. Der Verantwortliche hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragsverarbeiter in geeigneter Weise zu kontrollieren.

c. Der Auftragsverarbeiter ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Verpflichtungserklärung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragsverarbeiter über personenbezogene Daten verfügt, die ihm vom Verantwortlichen zugeleitet wurden oder die er für diesen erhoben hat.

11. Schlussbestimmungen

a. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

b. Diese Vereinbarung unterliegt österreichischem Recht. Ausschließlicher Gerichtsstand ist Graz.

c. Der Auftragsverarbeiter ist berechtigt, jederzeit rechtskonforme Änderungen an dieser Verpflichtungserklärung vorzunehmen. Sollte er eine Änderung vornehmen (müssen), verpflichtet er sich, die jeweils letztgültige Version dieser Verpflichtungserklärung unaufgefordert dem Verantwortlichen in elektronischer Form zu übermitteln.

Söding, am

Für den Auftragsverarbeiter:

_____

Dipl. Ing. Walter Lukmann, CEO
Lukmann Consulting GmbH
Packerstrasse 131a
A-8561 Söding

Anlagen
Anlage 1 – Technische und organisatorische Maßnahmen des Auftragsverarbeiters
Anlage 2 –Subunternehmer

Anlage 1 – Technisch-organisatorische Maßnahmen des Auftragsverarbeiters

a) Vertraulichkeit

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen

• Der Zutritt zu Einrichtungen, in denen Daten des Verantwortlichen verarbeitet werden, beschränkt sich auf benannte autorisierte Personen. • Der Betrieb des Rechenzentrums ist örtlich von der Betriebsstätte des Auftragsverarbeiters getrennt. Mitarbeitende haben nur Zutritt zur Betriebsstätte. Der Betrieb des Rechenzentrums erfolgt im Gebiet der EU durch einen Betreiber, der geeignete und überprüfbare Zertifizierungen, aufweist. • Der Zutritt zur Betriebsstätte ist via Chipcode gesichert.

- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung,

• Der Zugang von Nutzern auf Daten des Kunden ist über das SSL Protokoll verschlüsselt und gesichert. Zusätzlich erhält jeder Nutzer mit dem Zugang einen Token, der in definierten Abständen automatisch erneuert wird. Auf Daten des Systems kann der Nutzer nur mit gültiger Kennung und gültigem Token zugreifen. • Lukmann Consulting verwendet Verfahren nach Branchenstandard, um Nutzer zu identifizieren und zu authentifizieren, die versuchen, auf Informationssysteme zuzugreifen. • Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Lukmann Consulting vor, dass die Kennwörter regelmäßig erneuert werden müssen. • Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Lukmann Consulting vor, dass das Kennwort mindestens acht Zeichen umfassen muss. • Lukmann Consulting stellt sicher, dass deaktivierte oder abgelaufene Kennungen keiner anderen Person gewährt werden. • Lukmann Consulting überwacht wiederholte Versuche, sich mit ungültigen Kennwörtern Zugriff auf die Informationssysteme zu verschaffen. • Lukmann Consulting unterhält Verfahren nach Branchenstandard zur Deaktivierung von Kennwörtern, die beschädigt oder versehentlich offengelegt wurden. • Lukmann Consulting verwendet Verfahren nach Branchenstandard zum Schutz von Kennwörtern, einschließlich Verfahren, die die Vertraulichkeit und Integrität von Kennwörtern wahren sollen, wenn sie zugewiesen und verteilt werden sowie während der Speicherung. • Lukmann Consulting und erhält Verfahren nach Branchenstandard um den Zugang zu Datenbanken zu beschränken und verschlüsselt Datenbanken nach Branchenstandard.

- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems,

• Zugriffsrichtlinie.
  ○ Lukmann Consulting führt Unterlagen über Sicherheitsberechtigungen einzelner Personen, die auf Kundendaten zugreifen.
• Zugriffsautorisierung
  ○ Lukmann Consulting führt und aktualisiert Unterlagen zu den Mitarbeitenden, die für den Zugriff auf Lukmann Consulting-Systeme, die Kundendaten enthalten, autorisiert sind.
  ○ Lukmann Consulting deaktiviert Anmeldedaten, die über einen Zeitraum, der sechs Monate nicht überschreiten darf, nicht verwendet wurden.
  ○ Lukmann Consulting benennt diejenigen Mitarbeitenden, die berechtigt sind, den autorisierten Zugriff auf Daten und Ressourcen zu gewähren, zu ändern oder zu widerrufen.
  ○ Wenn mehrere Personen Zugriff auf die Systeme haben, auf denen Kundendaten enthalten sind, stellt Lukmann Consulting sicher, dass diese Personen über separate Kennungen/Anmeldedaten verfügen.
• Geringste Berechtigung
  ○ Technischen Supportmitarbeitenden ist der Zugriff auf Kundendaten nur erlaubt, wenn dies erforderlich ist oder vom Kunden autorisiert wurde.
  ○ Lukmann Consulting beschränkt den Zugriff auf Kundendaten nur auf die Personen, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuführen.
• Integrität und Vertraulichkeit
  ○ Lukmann Consulting weist ihre Mitarbeitenden an, Administrationssitzungen zu deaktivieren, wenn sie Einrichtungen unter der Kontrolle von Lukmann Consulting verlassen oder wenn Computer anderweitig unbeaufsichtigt gelassen werden.
  ○ Lukmann Consulting speichert Kennwörter so, dass sie während ihres Geltungszeitraums nicht lesbar sind.

- **Pseudonymisierung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.

• Userdaten (Bearbeiter/Mitarbeiter) werden in der Datenbank verschlüsselt abgelegt.

- **Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

Geheim	
Vertraulich	
Intern	Persönliche Identifikationsdaten
Öffentlich	

b) Integrität

- **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport,

• SSL Verschlüsselung zwischen Browser und Rechenzentrum • SSL Verschlüsselung bei der Übertragung von Daten an Subunternehmen

- **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind,

• Event-Logging.   ○ Lukmann Consulting zeichnet den Zugriff und die Nutzung von Informationssystemen auf, die Kundendaten enthalten, indem die Zugriffs-ID, Zugriffszeit, gewährte oder verweigerte Autorisierung und entsprechende Aktivität registriert werden.

c) Verfügbarkeit und Belastbarkeit

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitenden;

• Verfahren zur Datenwiederherstellung
  ○ Lukmann Consulting bzw. ihre Subunternehmer erstellen fortlaufend, jedoch keinesfalls seltener als ein Mal pro Woche (es sei denn, es wurden in dem Zeitraum keine Kundendaten aktualisiert) mehrere aktuelle Kopien von Kundendaten, von denen Kundendaten wiederhergestellt werden können, und bewahrt diese auf.
  ○ Lukmann Consulting bzw. ihre Subunternehmer bewahren Kopien von Kundendaten und Datenwiederherstellungsverfahren an einem anderen Ort als an dem Ort auf, an dem sich die primären Computergeräte, die die Kundendaten verarbeiten, befinden.
  ○ Lukmann Consulting bzw. ihre Subunternehmer verfügen über bestimmte Verfahren, die den Zugriff auf Kopien von Kundendaten regeln.
  ○ Lukmann Consulting bzw. ihre Subunternehmen prüfen die Datenwiederherstellungsverfahren mindestens alle zwölf Monate.
  ○ Lukmann Consulting bzw. ihrer Subunternehmen protokollieren Datenwiederherstellungsmaßnahmen, einschließlich der verantwortlichen Person, der Beschreibung der wiederhergestellten Daten, gegebenenfalls der verantwortlichen Person sowie welche Daten (gegebenenfalls) beim Datenwiederherstellungsverfahren manuell eingegeben werden mussten.
• Malware und Virenschutz
  ○ Lukmann Consulting bzw. ihre Subunternehmer verfügen über Antimalwarekontrollen, um zu verhindern, dass Malware unbefugten Zugriff auf Kundendaten erhält, einschließlich Malware aus öffentlichen Netzwerken.
  ○ Lukmann Consulting sorgt für einen aktuellen Virenschutz auf Rechnern ihrer Mitarbeitenden.
• Notfallpläne und Wiederherstellbarkeit
  ○ Lukmann Consulting unterhält Notfallpläne oder stellt sicher das Notfallpläne von Subunternehmen für die Einrichtungen existieren, in denen Kundendaten des Auftragverarbeiters verarbeitet werden.
  ○ Der redundante Speicher von Lukmann Consulting bzw. ihrer Subunternehmen sowie ihre Verfahren zur Wiederherstellung von Daten sind so konzipiert, dass versucht wird, Kundendaten in ihrem ursprünglichen oder ihrem zuletzt replizierten Zustand vor dem Zeitpunkt des Verlusts oder der Vernichtung zu rekonstruieren.
• Löschfristen für Logdaten
  ○ Lukmann Consulting verwendet Verfahren bei denen das Verhalten der Applikation überwacht und protokoliert werden, dabei werden auch indirekt personenbezogene Daten gespeichert. Diese Daten werden nach spätestens 30 Tagen gelöscht.
  ○ Lukmann Consulting protokolliert Änderungen an Daten des Verantwortlichen. Diese Daten werden nach spätestens 30 Tagen gelöscht, ausgenommen der Verantwortliche kann andere Einstellungen vornehmen.

d) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Verantwortung für den Datenschutz
    - Lukmann Consulting hat einen Datenschutzbeauftragten bestimmt, der für die Koordination und Überwachung der Datenschutzverfahren verantwortlich ist.
- Funktionen und Verantwortlichkeiten in Bezug auf Datenschutz.
    - Mitarbeitende von Lukmann Consulting mit Zugriff auf Kundendaten unterliegen Vertraulichkeitsverpflichtungen.
- Datenschutz Schulungen
    - Lukmann Consulting informiert ihre Mitarbeitenden über relevante Sicherheitsverfahren und ihre jeweiligen Aufgaben. Außerdem informiert Lukmann Consulting ihre Mitarbeitenden über mögliche Konsequenzen beim Verstoß gegen die Sicherheitsvorschriften und -verfahren. Lukmann Consulting verwendet in Schulungen ausschließlich anonyme Daten.
- Verfahren für die Reaktion auf Zwischenfälle
    - Lukmann Consulting führt Unterlagen über Sicherheitsverletzungen unter Angabe einer Beschreibung der Verletzung, des Zeitraums, der Konsequenzen der Verletzung, sowie des Verfahrens zur Wiederherstellung von Daten.
    - Für jede Sicherheitsverletzung, die ein Sicherheitsvorfall ist, erfolgt eine Meldung durch Lukmann Consulting ohne schhuldhaftes Zögern, auf jeden Fall aber innerhalb von 72 Stunden.
    - Lukmann Consulting dokumentiert jeden gemeldeten Fehler in einer eigenen Fehlerdatenbank. Dabei wird festgehalten, wer den Fehler gemeldet hat. Fehler werden spätestens 30 Tage nach deren Behebung gelöscht
- Datenschutzfreundliche Voreinstellungen
    - Lukmann Consulting stellt dem Verantwortlichen Funktionen zur Verfügung um Löschfristen für die eigenen Daten zu definieren und auszuführen.

e) Auftragskontrolle

Die Dienstleister, denen sich der Auftragsverarbeiter bedient, werden von diesem unter Anlage strenger Kriterien ausgewählt und kontrolliert.

- Lukmann Consulting wählt nur Subunternehmen die ihren Sitz in der EU oder einem Staat mit Angemessenheitsbeschluss haben.
- Lukmann Consulting wählt nur Subunternehmen auf Grund ihrer Datenschutzmaßnahmen ein für die übertragene Aufgabe ausreichendes Datenschutzniveau nachweisen kann. Der Nachweis erfolgt in der Regel durch geeignete Sicherheitszertifikate und aktueller Prüfungsergebnisse

Anlage 2 – Auflistung der Subunternehmer

Subunternehmer	Land	Leistung
Microsoft www.microsoft.com	Irland	• Hosting der CP Lösung in Mitteleuropa • Authentifizierung • Zugriffsautorisierung • Event Logging Infrastruktur • Malware Schutz • Verfahren zur Datenwiederherstellung
MailChimp www.mailchimp.com	USA SCC	• Versenden von Mails zu Produktneuigkeiten und Informationen im Bereich Datenschutz
Cituro GmbH https://www.cituro.com	Deutschland	• Terminbuchungssoftware • Buchung von Terminen • Versand von Terminbuchungserinnerungen
Chargebee Inc. https://www.chargebee.com	USA DPF	• Rechnungssoftware • Versand von Rechnungen