# Vereinbarung zur Auftragsverarbeitung

*gemäß Art. 28 Abs. 3 DSGVO für Beratungs- und Auditdienstleistungen*

zwischen

dem im Hauptvertrag bezeichneten Kunden

– Verantwortlicher / Auftraggeber –

und

Einzelunternehmen Thomas Ili
Thomas Ili
Denickestraße 149
21075 Hamburg
E-Mail: thomas@ili.de

– Auftragsverarbeiter / Auftragnehmer –

## Präambel

Der Auftragnehmer erbringt Beratungs-, Auditierungs- und Unterstützungsleistungen in den Bereichen Managementsysteme, Informationssicherheit, Datenschutz, Qualität und Prozesse grundsätzlich remote. Die Parteien erwarten, dass der Auftraggeber personenbezogene Daten soweit möglich entfernt, anonymisiert, pseudonymisiert oder schwärzt. Da ein Zugriff auf personenbezogene Daten bei Audits und Beratungen dennoch nicht sicher ausgeschlossen werden kann, regelt diese Vereinbarung vorsorglich jede Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers.

Diese Vereinbarung gilt für alle Verarbeitungen personenbezogener Daten, die der Auftragnehmer im Rahmen der beauftragten Beratungs-, Unterstützungs- und Auditdienstleistungen im Auftrag des Auftraggebers durchführt. Dies umfasst insbesondere Tätigkeiten als externer Informationssicherheitsbeauftragter, interne Audits sowie Auditierungsleistungen im Auftrag einer Zertifizierungsstelle. Die fachliche Unabhängigkeit, Objektivität und Unparteilichkeit des Auftragnehmers bleiben unberührt.

Soweit für einzelne Leistungen eine abweichende datenschutzrechtliche Rollenverteilung gilt, wird diese bei Abschluss des Hauptvertrags im Angebot, Auftrag oder in der Leistungsbeschreibung ausdrücklich festgelegt. Ohne eine solche Festlegung gilt für die vertragsgegenständliche Verarbeitung diese Vereinbarung. Wird der Auftragnehmer von einer Zertifizierungsstelle beauftragt, ist die Zertifizierungsstelle Auftraggeber im Sinne dieser Vereinbarung; die Zertifizierungsentscheidung verbleibt ausschließlich bei ihr.

## 1. Gegenstand, Dauer und Rang

1.1 Gegenstand sind die in der Hauptvereinbarung beschriebenen Beratungs-, Auditierungs-, Dokumentations- und Unterstützungsleistungen, soweit dabei personenbezogene Daten verarbeitet oder eingesehen werden können.

1.2 Die Verarbeitung beginnt mit dem ersten tatsächlichen Zugriff und endet mit Abschluss des Hauptvertrags sowie Löschung oder Rückgabe der Auftragsdaten, soweit keine gesetzliche Aufbewahrungspflicht besteht.

1.3 Bei Widersprüchen gehen diese Vereinbarung und zwingendes Datenschutzrecht hinsichtlich der Verarbeitung personenbezogener Daten vor. Weisungen, die gegen geltendes Recht verstoßen, muss der Auftragnehmer nicht ausführen; er informiert den Auftraggeber unverzüglich.

1.4 Diese Vereinbarung wird mit der Annahme des Hauptvertrags gleichzeitig Bestandteil der vertraglichen Vereinbarungen und tritt zu diesem Zeitpunkt in Kraft. Eine gesonderte Unterzeichnung ist nicht erforderlich.

## 2. Art und Zweck der Verarbeitung

Die Verarbeitung kann insbesondere das strukturierte Sichten, Erheben im Interview, Ordnen, Auswerten, Prüfen, Dokumentieren, Übermitteln, Einschränken und Löschen von Daten umfassen. Zwecke sind ausschließlich die Vertragserfüllung, insbesondere Gap-Analysen, Aufbau und Weiterentwicklung von Managementsystemen, Risikoanalysen, interne oder externe Audits, Erstellung von Berichten und Nachweisen sowie vereinbarte Projektkommunikation.

## 3. Grundsatz der Datenminimierung

3.1 Der Auftraggeber stellt grundsätzlich nur Informationen bereit, die für die konkrete Leistung erforderlich sind. Vor der Bereitstellung sollen personenbezogene Daten entfernt, anonymisiert, pseudonymisiert oder geschwärzt werden, sofern der Arbeitszweck dadurch nicht beeinträchtigt wird.

3.2 Insbesondere sollen keine vollständigen Personalakten, privaten Kontaktdaten, Ausweiskopien, Gesundheitsdaten, Zugangspasswörter, privaten Kommunikationsinhalte oder nicht erforderlichen Protokolldaten übermittelt werden.

3.3 Ein pauschaler Ausschluss personenbezogener Daten gilt nicht, wenn tatsächlich Namen, geschäftliche Kontaktdaten, Benutzerkennungen, Auditinterviews, Tickets, Vorfallsdaten oder andere auf Personen beziehbare Informationen zugänglich werden. In diesem Fall gilt diese Vereinbarung uneingeschränkt.

## 4. Weisungen des Auftraggebers

4.1 Der Auftragnehmer verarbeitet Auftragsdaten nur auf dokumentierte Weisung des Auftraggebers, soweit keine unionsrechtliche oder mitgliedstaatliche Pflicht entgegensteht. Die Weisung umfasst den in Abschnitt 13 geregelten zeitweisen eigenen Fernzugriff aus Staaten außerhalb von EU und EWR.

4.2 Erstweisungen ergeben sich aus Hauptvertrag, Leistungsbeschreibung und Anlagen. Weitere Weisungen erfolgen in Textform. Mündliche Weisungen werden vom Auftragnehmer dokumentiert und vom Auftraggeber bestätigt.

4.3 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn eine Weisung nach seiner Auffassung gegen Datenschutzrecht verstößt, und setzt die betroffene Verarbeitung bis zur Klärung aus, soweit dies rechtlich und tatsächlich möglich ist.

## 5. Pflichten des Auftragnehmers

- Vertraulichkeit aller zur Verarbeitung befugten Personen und angemessene Unterweisung;
- Umsetzung und regelmäßige Überprüfung geeigneter technischer und organisatorischer Maßnahmen gemäß Anlage 2;
- Unterstützung des Auftraggebers bei Betroffenenrechten, Datenschutz-Folgenabschätzungen, Konsultationen und Nachweispflichten, soweit die Art der Verarbeitung dies ermöglicht;
- unverzügliche Meldung bekannt gewordener Verletzungen des Schutzes personenbezogener Daten mit den verfügbaren Informationen;
- Führung der erforderlichen Verzeichnisse und Bereitstellung erforderlicher Nachweise;
- keine Nutzung der Auftragsdaten für eigene Zwecke, Werbung oder Training allgemeiner KI-Modelle;
- keine dauerhafte lokale Speicherung, soweit sie für die vereinbarte Leistung nicht erforderlich ist.

## 6. Vertraulichkeit und Personal

Der Auftragnehmer setzt nur Personen ein, die auf Vertraulichkeit verpflichtet und über die maßgeblichen Datenschutz- und Sicherheitsanforderungen unterrichtet wurden. Zugriffsrechte werden nach dem Erforderlichkeitsprinzip vergeben und nach Wegfall unverzüglich entzogen.

## 7. Technische und organisatorische Maßnahmen

Die in Anlage 2 beschriebenen Maßnahmen bilden das vereinbarte Schutzniveau. Der Auftragnehmer darf Maßnahmen an die technische Entwicklung anpassen, sofern das Sicherheitsniveau nicht abgesenkt wird. Er berücksichtigt Art, Umfang, Umstände und Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere der Risiken.

## 8. Unterauftragsverarbeiter

8.1 Die in Anlage 3 genannten Unterauftragsverarbeiter gelten als genehmigt. Ist Anlage 3 leer, sind keine Unterauftragsverarbeiter vereinbart. Die Beauftragung eines neuen Unterauftragsverarbeiters bedarf einer Ergänzung der Anlage 3 in Textform; bis dahin erhält dieser keinen Zugriff auf Auftragsdaten.

8.2 Der Auftragnehmer verpflichtet Unterauftragsverarbeiter mindestens zu gleichwertigen Datenschutzpflichten. Bleibt ein Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für dessen Pflichterfüllung nach den gesetzlichen Vorschriften.

## 9. Kontroll- und Nachweisrechte

9.1 Der Auftragnehmer stellt alle Informationen zur Verfügung, die zum Nachweis der Einhaltung von Art. 28 DSGVO erforderlich sind, und ermöglicht angemessene Audits einschließlich Inspektionen.

9.2 Kontrollen erfolgen grundsätzlich durch aktuelle Zertifikate, Prüfberichte, Fragebögen oder Remote-Audits. Vor-Ort-Prüfungen sind bei konkretem Anlass oder unzureichenden anderen Nachweisen nach angemessener Ankündigung möglich. Betriebs- und Geschäftsgeheimnisse sowie Rechte anderer Kunden sind zu schützen.

9.3 Ein angemessener, über gesetzliche Mitwirkungspflichten hinausgehender Aufwand kann nach vorheriger Vereinbarung vergütet werden.

## 10. Betroffenenrechte

Anfragen betroffener Personen leitet der Auftragnehmer unverzüglich an den Auftraggeber weiter, soweit er nicht selbst zur Beantwortung verpflichtet ist. Ohne Weisung beantwortet er keine Anfrage inhaltlich. Er unterstützt Suche, Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch durch geeignete Maßnahmen.

## 11. Datenschutzverletzungen

Der Auftragnehmer meldet dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden. Die Meldung enthält, soweit verfügbar, Art und Umfang des Vorfalls, Daten- und Personenkategorien, mögliche Folgen, getroffene oder vorgeschlagene Maßnahmen und einen Ansprechpartner. Weitere Erkenntnisse werden nachgereicht.

## 12. Rückgabe und Löschung

Nach Ende der Leistung löscht oder übergibt der Auftragnehmer nach Wahl des Auftraggebers alle Auftragsdaten und vorhandenen Kopien, soweit keine gesetzliche Aufbewahrungspflicht besteht. Sicherungskopien werden im regulären Löschzyklus überschrieben und bis dahin gesperrt. Die Löschung kann auf Anforderung bestätigt werden.

## 13. Zeitweilige Tätigkeit aus Staaten außerhalb von EU/EWR

13.1 Der Auftragnehmer hat seinen Unternehmens- und Dienstsitz in Hamburg und erbringt seine Leistungen überwiegend von dort. Der Auftraggeber ist darüber informiert und weist den Auftragnehmer mit Annahme dieser Vereinbarung an, die Leistungen zeitweise auch durch eigenen Fernzugriff aus einem Staat außerhalb von EU und EWR zu erbringen, für den unter Umständen kein Angemessenheitsbeschluss der Europäischen Kommission besteht.

13.2 Der Zugriff erfolgt ausschließlich durch Thomas Ili als Inhaber desselben in Hamburg niedergelassenen Einzelunternehmens oder einem in Anlage 3 genannten Unterauftragsverarbeiter. Ein rechtlich selbständiger Datenempfänger oder Unterauftragsverarbeiter wird im Drittland nicht eingesetzt. Der Auftragnehmer bleibt alleiniger Vertragspartner und Adressat der Weisungen.

13.3 Der Auftragnehmer und etwaige Unterauftragsnehmer gewährleisten auch während des Auslandsaufenthalts die Einhaltung dieser Vereinbarung und der technischen und organisatorischen Maßnahmen. Auftragsdaten werden nur im erforderlichen Umfang aufgerufen. Übertragungen erfolgen verschlüsselt; Datenträger und gespeicherte Daten sind verschlüsselt; Software und Schutzsysteme werden aktuell gehalten; sichere Passwörter und, soweit verfügbar, Mehrfaktor-Authentisierung werden eingesetzt; Netzabschottung, Malware-Schutz, Datensicherung, automatische Bildschirmsperre und Zutrittsschutz werden gewährleistet.

13.4 Der Auftragnehmer und etwaige Unterauftragsnehmer schützen Bildschirm und Gespräche vor Einsicht und Mithören, nutzen keine öffentlich zugänglichen Endgeräte und vermeiden Ausdrucke sowie lokale Kopien, soweit sie für die Leistung nicht erforderlich sind. Verlust, Beschlagnahme, behördliche Zugriffsforderungen und Sicherheitsvorfälle werden dem Auftraggeber unverzüglich gemeldet, soweit eine Mitteilung rechtlich zulässig ist.

13.5 Anfragen ausländischer Behörden werden nicht freiwillig erfüllt. Der Auftragnehmer prüft Rechtmäßigkeit und Zuständigkeit, nutzt zumutbare verfügbare Rechtsmittel und legt Daten nur offen, soweit hierzu eine zwingende rechtliche Verpflichtung besteht. Der Auftraggeber wird vorab informiert, soweit dies rechtlich zulässig ist.

13.6 Verlegt der Auftragnehmer seinen Unternehmens- oder Dienstsitz in einen Staat außerhalb von EU und EWR oder erhält dort eine rechtlich selbständige Person oder Stelle Zugriff auf Auftragsdaten, ist dieser Abschnitt nicht mehr ausreichend. Eine solche Verarbeitung beginnt erst, nachdem die nach Kapitel V DSGVO erforderlichen Voraussetzungen geschaffen und vertraglich einbezogen wurden.

## 14. Haftung und Schlussbestimmungen

Es gelten die gesetzlichen Haftungsregelungen, insbesondere Art. 82 DSGVO, sowie ergänzend die wirksam vereinbarten Haftungsregelungen des Hauptvertrags. Änderungen dieser Vereinbarung bedürfen der

Textform, soweit nicht strengere Form vorgeschrieben ist. Sollten einzelne Regelungen unwirksam sein, bleibt die Wirksamkeit der übrigen Regelungen unberührt.

Anwendbares Recht und Gerichtsstand richten sich nach dem Hauptvertrag und zwingendem Datenschutzrecht. Rechte betroffener Personen und Zuständigkeiten von Aufsichtsbehörden werden dadurch nicht eingeschränkt.

# Anlage 1 – Beschreibung der Verarbeitung

## A. Gegenstand und Zwecke

Gegenstand und konkreter Leistungsumfang ergeben sich aus dem Hauptvertrag. Zwecke sind die beauftragte Beratung, Unterstützung und Auditierung von Managementsystemen, insbesondere zu Informationssicherheit, Datenschutz, Qualität, Prozessen und den jeweils vereinbarten Regelwerken.

## B. Verarbeitungstätigkeiten

Remote-Beratung, Workshops, Dokumentenreview, Gap-Analyse, Risikobewertung, Auditplanung, Interviews, Stichprobenprüfung, Berichterstellung und vereinbarte Nachbereitung.

## C. Kategorien betroffener Personen

- Beschäftigte und freie Mitarbeitende des Auftraggebers
- Geschäftsführung, Führungskräfte und Beauftragte
- Ansprechpersonen bei Kunden, Lieferanten und Geschäftspartnern
- Nutzerinnen und Nutzer von IT-Systemen
- sonstige Personen nur, soweit im Einzelfall erforderlich und dokumentiert

## D. Datenkategorien

- geschäftliche Stamm- und Kontaktdaten
- Rollen, Funktionen, organisatorische Zuordnungen und Benutzerkennungen
- Interviewaussagen, Auditnachweise und Schulungsnachweise
- Ticket-, Protokoll-, Berechtigungs- und Vorfallsdaten in erforderlichen Stichproben
- Vertrags- und Lieferanteninformationen mit Personenbezug

## E. Ausgeschlossene Daten

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, Strafdaten nach Art. 10 DSGVO, vollständige Personalakten, private Kommunikation, Ausweiskopien und Zugangsdaten sind ausgeschlossen, sofern sie nicht ausdrücklich schriftlich vereinbart, zwingend erforderlich und durch zusätzliche Schutzmaßnahmen abgesichert wurden.

## F. Dauer und Löschung

Die Verarbeitung dauert für die Laufzeit des Hauptvertrags. Erforderliche Arbeitskopien werden spätestens 90 Tage nach Beendigung des Hauptvertrags gelöscht, sofern der Auftraggeber keine frühere Löschung oder

Rückgabe verlangt und keine gesetzliche Aufbewahrungspflicht entgegensteht. Gesetzlich aufzubewahrende Vertrags- und Abrechnungsunterlagen werden getrennt und zweckgebunden aufbewahrt.

### G. Arbeitsorte

Die Verarbeitung erfolgt überwiegend am Unternehmens- und Dienstsitz in Hamburg sowie zeitweise durch Thomas Ili persönlich im Wege des Fernzugriffs aus einem Staat außerhalb von EU und EWR nach Maßgabe von Abschnitt 13.

## Anlage 2 – Technische und organisatorische Maßnahmen

### Verschlüsselung

- verschlüsselter Datenverkehr bei der Übertragung von Auftragsdaten
- verschlüsselte Datenspeicherung auf den eingesetzten Datenträgern und Systemen

### Authentisierung und Bildschirmschutz

- sichere Nutzung starker, einzigartiger Passwörter
- Mehrfaktor-Authentisierung, soweit diese für den jeweiligen Zugang verfügbar ist
- automatische Bildschirmsperre bei Nichtbenutzung

### Software- und Netzwerksicherheit

- regelmäßige Installation verfügbarer Software- und Sicherheitsupdates
- Netzabschottung durch Firewall und geeignete Netzwerkkonfiguration
- aktuell gehaltener Schutz vor Schadsoftware

### Verfügbarkeit und physischer Schutz

- regelmäßige Datensicherung der erforderlichen Arbeitsdaten
- Zutrittsschutz zu den eingesetzten Systemen und zur Arbeitsumgebung

### Datenminimierung und Vertraulichkeit

- Verarbeitung nur der für den jeweiligen Auftrag erforderlichen personenbezogenen Daten
- Schwärzung, Anonymisierung oder Pseudonymisierung, soweit dies ohne Beeinträchtigung des Arbeitszwecks möglich ist
- vertrauliche Behandlung der Auftragsdaten und Schutz von Bildschirm und Gesprächen vor Einsicht oder Mithören
- geordnete Ablage und Trennung von Auftragsdaten verschiedener Kunden

### Löschung, Vorfälle und Überprüfung

- Löschung nicht mehr erforderlicher Arbeitskopien entsprechend den vereinbarten Löschfristen
- unverzügliche Meldung erkannter Datenschutz- und Sicherheitsvorfälle an den Auftraggeber
- gelegentliche und anlassbezogene Überprüfung der eingesetzten Sicherheitsmaßnahmen

# Anlage 3 – Unterauftragsverarbeiter

Zum Zeitpunkt des Vertragsschlusses sind keine Unterauftragsverarbeiter vereinbart.

| Anbieter | Leistung | Ort | Datenarten | Transfergrundlage |
|---|---|---|---|---|
| | | | | |