

Vertrag zur Auftragsverarbeitung basierend auf den Standardvertragsklauseln der Kommission nach **Art. 28 Absatz (7) DSGVO**

zwischen

und

lawpilots GmbH
Am Hamburger Bahnhof 3
10557 Berlin
Deutschland

nachstehend „Verantwortlicher“

nachstehend „Auftragsverarbeiter“

Inhaltsverzeichnis

Präambel	3
Abschnitt I – Allgemeines	4
Zweck und Anwendungsbereich	4
Unabänderbarkeit der Klauseln	4
Auslegung	4
Vorrang	4
Abschnitt II – Pflichten der Parteien	5
Beschreibung der Verarbeitung	5
Pflichten der Parteien	5
6.1 Weisungen	5
6.2 Zweckbindung	5
6.3 Dauer der Verarbeitung personenbezogener Daten	5
6.4 Sicherheit der Verarbeitung	6
6.5 Sensible Daten	6
6.6 Dokumentation und Einhaltung der Klauseln	6
6.7 Einsatz von Unterauftragsverarbeitern	7
6.8 Internationale Datenübermittlungen	8
Unterstützung des Verantwortlichen	8
Meldung von Verletzungen des Schutzes personenbezogener Daten	9
8.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten	9
8.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten	10
Abschnitt III – Schlussbestimmungen	11
Verstöße gegen die Klauseln und Beendigung des Vertrags	11
Anhang I. Ergänzende Regelungen	12
Allgemeine Ergänzungen	12
Besondere Regelungen	12
Anhang II. Liste Der Parteien	15
Anhang III. Beschreibung der Verarbeitung	16
Anhang IV. Technische und organisatorische Maßnahmen	17
Anhang V. Liste der Unterauftragsverarbeiter	21

Präambel

Zwischen dem Verantwortlichen und dem Auftragsverarbeiter besteht ein Auftragsverhältnis im Sinne des Art. 28 der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, „DSGVO“).

Dieser Auftragsverarbeitungsvertrag einschließlich aller Anlagen (nachfolgend gemeinsam als „Vereinbarung“ bezeichnet) konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien aus dem zugrundeliegenden Vertrag, der Leistungsvereinbarung und/oder Auftragsbeschreibung einschließlich aller Anlagen (nachfolgend gemeinsam als „Hauptvertrag“ bezeichnet). Sofern Bezug auf die Regelungen des Bundesdatenschutzgesetzes (nachfolgend „BDSG“) genommen wird, so ist damit das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 in der zum Zeitpunkt ab dem 25. Mai 2018 geltenden Fassung gemeint.

Der Auftragsverarbeiter verpflichtet sich gegenüber dem Verantwortlichen zur Erfüllung des Hauptvertrages und dieser Vereinbarung nach Maßgabe der folgenden Bestimmungen:

Allgemeines

Zweck und Anwendungsbereich

- (a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, im Folgenden: DSGVO) sichergestellt werden.
- (b) Die in **Anhang II** aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der DSGVO zu gewährleisten.
- (c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß **Anhang III**.
- (d) **Anhang I** bis **Anhang V** sind Bestandteil der Klauseln.
- (e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der DSGVO unterliegt.
- (f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der DSGVO erfüllt werden.

Unabänderbarkeit der Klauseln

Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

Auslegung

- (a) Werden in diesen Klauseln die in der DSGVO definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
- (b) Diese Klauseln sind im Lichte der Bestimmungen der DSGVO auszulegen.
- (c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der DSGVO vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Vorrang

- (a) Im Falle eines Widerspruchs zwischen dieser Vereinbarung und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden (solche Vereinbarungen nachfolgend auch „**Hauptvertrag**“ genannt), haben die Regelungen dieser Vereinbarung Vorrang.

- (b) Im Falle eines Widerspruchs zwischen den ergänzenden Klauseln in Anhang I und sonstigen Regelungen dieser Vereinbarung haben die übrigen Regelungen dieser Vereinbarung Vorrang gegenüber den ergänzenden Klauseln in Anhang I.

Pflichten der Parteien

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in **Anhang III** aufgeführt.

Pflichten der Parteien

6.1 Weisungen

- (a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.
- (b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die DSGVO oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

6.2 Zweckbindung

- (a) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in **Anhang III** genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

6.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in **Anhang III** angegebene Dauer verarbeitet.

6.4 Sicherheit der Verarbeitung

- (a) Der Auftragsverarbeiter ergreift geeignete technische und organisatorische Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dabei sind Maßnahmen zu treffen, mit denen mindestens (nicht abschließend) die in Anhang IV genannten Schutzziele gesichert werden. Dies umfasst auch den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.
- (b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

6.5 Sensible Daten

Falls die Verarbeitung personenbezogener Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzliche Garantien an.

6.6 Dokumentation und Einhaltung der Klauseln

- (a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
- (b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
- (c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der DSGVO hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

- (d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
- (e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

6.7 Einsatz von Unterauftragsverarbeitern

- (a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens vier Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit (innerhalb von 2 Wochen nach Zugang der Information) ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.
- (b) Die vereinbarte Liste der vom Verantwortlichen genehmigten Unterauftragsverarbeiter findet sich in **Anhang V**. Die Parteien halten **Anhang V** jeweils auf dem neuesten Stand.
- (c) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der DSGVO unterliegt.
- (d) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie eines solchen (Unter-)Auftragsverarbeitungsvertrags und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.
- (e) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

- (f) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den (Unter-)Auftragsverarbeitungsvertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

6.8 Internationale Datenübermittlungen

- (a) Jede Übermittlung von Daten durch den Auftragsverarbeiter und Unterauftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der DSGVO im Einklang stehen.
- (b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 6.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhalten oder nicht ausschließen, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der DSGVO sicherstellen können, indem sie entweder den Angemessenheitsbeschluss oder die Standarddatenschutzklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der DSGVO erlassen wurden (auch als „Standardvertragsklauseln“ bezeichnet), sofern die Voraussetzungen für die Anwendung dieser Standarddatenschutzklauseln erfüllt sind.

Unterstützung des Verantwortlichen

- (a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu in Textform ermächtigt.
- (b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben (a) und (b) befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.
- (c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

- (1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden: „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
 - (2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
 - (3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
 - (4) Verpflichtungen gemäß Artikel 32 der DSGVO.
- (d) Die Parteien legen in Anhang IV die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der DSGVO nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

8.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

- (a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

(b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der DSGVO in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

- (1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- (2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- (3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

(c) bei der Einhaltung der Pflicht gemäß Artikel 34 der DSGVO, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

8.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

(a) Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

- (1) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
- (2) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
- (3) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

- (b) Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.
- (c) Die Parteien legen in Anhang IV alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der DSGVO zu unterstützen.

Schlussbestimmungen

Verstöße gegen die Klauseln und Beendigung des Vertrags

- (a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der DSGVO – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.
- (b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
 - (1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
 - (2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der DSGVO nicht erfüllt;
 - (3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln oder der DSGVO zum Gegenstand hat, nicht nachkommt.
- (c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe (b) verstoßen.

- (d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Anhang I. Ergänzende Regelungen

Allgemeine Ergänzungen

- (a) **Anwendungsbereich:** Die in dieser Vereinbarung enthaltenen Klauseln finden Anwendung auf alle Leistungen der Auftragsverarbeitung im Sinne des Art. 28 DSGVO, die der Auftragsverarbeiter gegenüber dem Verantwortlichen erbringt.
- (b) **Form:** Änderungen und Ergänzungen dieser Vereinbarung sollen mindestens in Textform erfolgen und bedürfen der ausdrücklichen Angabe, dass damit die vorliegenden Bestimmungen geändert und/oder ergänzt werden. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Soweit gemäß dieser Vereinbarung die Schriftform vorgesehen ist, ist die Textform im Sinne von § 126b BGB ausreichend.
- (c) **Rechtswahl:** Diese Vereinbarung unterliegt deutschem Recht.
- (d) **Gerichtsstand:** Gerichtsstand ist Berlin.

Besondere Regelungen

- (a) **Benennung von Weisungsempfängern:** Soweit es der Auftragsverarbeiter für erforderlich hält, kann dieser bestimmte Personen auf Seiten des Auftragsverarbeiters (einschließlich bestimmter Kontaktdaten) benennen, an die der Verantwortliche seine Weisungen zur Verarbeitung von personenbezogenen Daten ausschließlich zu richten hat. Diese Personen und Kontaktdaten wird der Auftragsverarbeiter dem Verantwortlichen schriftlich mitteilen. Soweit der Auftragsverarbeiter von diesem Recht Gebrauch macht, ist der Verantwortliche verpflichtet, sämtliche Weisungen gemäß der Regelung in Klausel 7.1 lit. a) ausschließlich an die vom Auftragsverarbeiter benannten Personen und deren jeweilige Kontaktdaten zu richten. Für den Fall, dass sich diese Personen auf Seiten des Auftragsverarbeiters oder deren genannte Kontaktdaten ändern, wird der Auftragsverarbeiter dies dem Verantwortlichen unter Benennung der jeweils neuen Person bzw. der neuen Kontaktdaten mitteilen.

- (b) **Widerrechtliche Weisungen:** Sofern der Verantwortliche dem Auftragsverarbeiter gegenüber Weisungen erteilt, die nach Auffassung des Auftragsverarbeiters gegen die DSGVO oder geltende Datenschutzbestimmungen der EU oder der EU-Mitgliedstaaten verstoßen (Klausel 7.1 Buchstabe (b)) ist er dazu berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird. Dieses Recht tritt neben das in Klausel 10 Buchstabe c dieser Vereinbarung vorgesehene Kündigungsrecht.
- (c) **Sicherheit der Verarbeitung:** Der Auftragsverarbeiter kann die in Anlage IV dargestellten technisch-organisatorischen Maßnahmen aktualisieren und ändern, vorausgesetzt, dass das Schutzniveau der Maßnahmen insgesamt durch solche Aktualisierungen und/oder Änderungen nicht wesentlich herabgesetzt wird.
- (d) **Unterauftragsverarbeiter:** Ergänzend zu Klausel 6.7 a) gilt: Im Fall einer Ablehnung der Genehmigung oder eines Widerspruchs kann der Auftragsverarbeiter nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder einen alternativen weiteren Unterauftragsverarbeiter vorschlagen und mit dem Verantwortlichen abstimmen. Sofern die Erbringung der Leistung ohne die beabsichtigte Änderung dem Auftragsverarbeiter nicht zumutbar ist – etwa aufgrund von damit verbundenen unverhältnismäßigen Aufwendungen für den Auftragsverarbeiter - oder die Abstimmung eines weiteren Unterauftragsverarbeiters mit dem Verantwortlichen fehlschlägt, können der Verantwortliche und der Auftragsverarbeiter diese Vereinbarung sowie den Hauptvertrag mit einer Frist von einem Monat zum Monatsende kündigen.
- (e) **Bereichsspezifische Vertraulichkeitspflichten:** Sofern der Verantwortliche anderweitigen bzw. speziellen zwingenden gesetzlichen Vertraulichkeitspflichten unterliegt, wird er dies dem Auftragsverarbeiter mitteilen.
- (f) **Haftung:**
- (1) Die Haftung des Auftragsverarbeiters ist in allen Fällen ausgeschlossen, in denen der Auftragsverarbeiter gemäß dieser Vereinbarung und gemäß den Weisungen oder Vorgaben des Verantwortlichen handelt.
 - (2) Die Haftung des Verantwortlichen gegenüber dem Auftragsverarbeiter erstreckt sich auch auf gegen den Auftragsverarbeiter verhängte Geldbußen, soweit diese auf die schuldhaft Verletzung einer datenschutzrechtlichen Pflicht des Verantwortlichen durch diesen, dessen Mitarbeiter bzw. von ihm Beauftragte zurückzuführen sind. Wird in Folge einer solchen Pflichtverletzung des Verantwortlichen ein Bußgeldbescheid gegen den Auftragsverarbeiter rechtskräftig, stellt der Verantwortliche den Auftragsverarbeiter vom verhängten Bußgeld frei, wobei sich die Höhe dieses Freistellungsanspruchs nach der Haftungsquote im Innenverhältnis bemisst. Der Verantwortliche hat die Geldbuße in der Höhe seines Anteils an der Verantwortung

für den durch die Geldbuße sanktionierten Verstoß zu übernehmen. Voraussetzung für die zuvor genannte Haftung des Verantwortlichen ist in jedem Fall, dass der Auftragsverarbeiter den Verantwortlichen unverzüglich schriftlich von einem solchen Fall verständigt, die behauptete Verletzung nicht anerkennt und jegliche gerichtliche oder außergerichtliche Auseinandersetzung, einschließlich etwaiger außergerichtlicher Regelungen, nur im Einvernehmen mit dem Verantwortlichen führt. Der Verantwortliche kann insbesondere verlangen, dass der Auftragsverarbeiter etwaige Bußgeldbescheide gerichtlich durch alle zur Verfügung stehenden Instanzen überprüfen lässt, wobei der Verantwortliche in einem solchen Fall verpflichtet ist, den Auftragsverarbeiter von den entstehenden Prozesskosten in Höhe der gesetzlichen Gebühren freizustellen.

- (3) Der Verantwortliche stellt den Auftragsverarbeiter im Innenverhältnis von allen Schadensersatzansprüchen betroffener Personen im Zusammenhang mit der Verletzung von datenschutzrechtlichen Bestimmungen frei, die diese gegenüber dem Auftragsverarbeiter geltend machen, soweit diese nicht darauf beruhen, dass der Auftragsverarbeiter gegen ihm als Auftragsverarbeiter obliegende Pflichten verstoßen hat oder im Auftrag verarbeitete personenbezogene Daten ohne oder gegen eine Weisung des Verantwortlichen verarbeitet hat. Die Regelungen in obenstehender Klausel 12 lit. (f) Abs. (2) Sätze 4 und 5 dieses Anhangs I gelten entsprechend.

- (g) **Entgelt:** Für die Mitwirkung bei Kontrollen steht dem Auftragsverarbeiter im Rahmen des rechtlich Zulässigen eine dem Mehraufwand entsprechende Vergütung und Erstattung eigener Kosten zu.

Anhang II. Liste Der Parteien

Verantwortliche(r): *[Name und Kontaktdaten des/der Verantwortlichen und gegebenenfalls des Datenschutzbeauftragten des Verantwortlichen]*

Name:

Anschrift:

Name, Funktion und Kontaktdaten der Kontaktperson:

Auftragsverarbeiter: *[Name und Kontaktdaten des/der Auftragsverarbeiter/s und gegebenenfalls des Datenschutzbeauftragten des Auftragsverarbeiters]*

Name: lawpilots GmbH

Anschrift: Am Hamburger Bahnhof 3

10557 Berlin

Deutschland

Name, Funktion und Kontaktdaten der Kontaktperson:

Datenschutzbeauftragte Person:

Nina Ostrerova ISiCO Datenschutz GmbH

Am Hamburger Bahnhof 4

10557 Berlin,

gemäß § 38 Bundesdatenschutzgesetz (BDSG) und Art. 37

Datenschutz-Grundverordnung (DSGVO).

Ort, Datum

Unterschrift (Verantwortlicher)

Ort, Datum

Unterschrift (Auftragsverarbeiter)

Anhang III. Beschreibung der Verarbeitung

Gegenstand des Auftrags:

Der Gegenstand des Auftrags umfasst die Schulung der Mitarbeiter im Rahmen des mit dem Auftragsverarbeiter vereinbarten Umfangs, gemäß dem Hauptvertrag.

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Praktikanten / Werkstudenten die vom Verantwortlichen zur Nutzung des Services autorisiert sind.
- Mitarbeiter (Stammebelegschaft, Auszubildende, Leiharbeiter, freie Mitarbeiter) vom Verantwortlichen zur Nutzung des Services autorisiert sind.

Kategorien personenbezogener Daten, die verarbeitet werden:

- Personenstammdaten der Mitarbeiter vom Verantwortlichen (Name, Vorname, Anrede, Titel/akademischer Grad, Geburtsdatum)
- Kontaktdaten (E-Mail-Adresse, dienstliche Telefonnummer*, Anschrift)
- Weitere Beschäftigtendaten (Position und Abteilung*)
- Schulungsteilnahmedaten (Zeitpunkt, Titel und Sprache der absolvierten Schulung)
- Elektronische Kommunikationsdaten (IP-Adresse, aufgerufene Internetseiten, Angaben zum verwendeten Endgerät, Betriebssystem und Browser)

*Diese personenbezogenen Daten der Mitarbeiter werden ausschließlich bei Buchung des Cyber-Security- Awareness Trainings erhoben.

Art der Verarbeitung:

Übermittlung, Verarbeitung und Speicherung der oben aufgeführten Daten.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

Zur Erfüllung des Verarbeitungszwecks übermittelt der Verantwortliche dem Auftragsverarbeiter die Personenstamm- und Kontaktdaten der Mitarbeiter, ggf. weitere Beschäftigtendaten zur Bereitstellung Dokumentation der Schulungsdienstleistungen, wie im Hauptvertrag beschrieben.

Dauer der Verarbeitung:

Die Dauer dieser Vereinbarung entspricht der Dauer des Hauptvertrags.

Bei der **Verarbeitung durch (Unter-)Auftragsverarbeiter** sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben (siehe Anhang V).

Anhang IV. Technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahme

Maßnahmen zur Verschlüsselung:

Maßnahmen oder Vorgänge, bei denen ein klar lesbarer Text / Information mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine unleserliche, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird:

- Symmetrische / Asymmetrische Verschlüsselung

Weitere Maßnahmen:

Die Passwörter der Management-Cockpit-Zugänge werden verschlüsselt und sind nicht interpretierbar oder lesbar.

Maßnahmen zur Pseudonymisierung:

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren:

Die Teilnahme an der Schulung kann auf Wunsch über pseudonyme TANs durchgeführt werden. Innerhalb dieses Verfahrens werden TANs je Schulungsteilnehmer generiert. Die Zuordnung von TANs auf Mitarbeiter ist nur dem Auftraggeber möglich, Rückschlüsse über die einzelnen Kursteilnehmer sind lawpilots somit nicht möglich.

Maßnahmen zur Sicherung der Vertraulichkeit

Zutrittskontrolle:

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie zu vertraulichen Akten und Datenträgern physisch verwehren:

- Kontrollierte Schlüsselvergabe (Chipkarten / Transpondersysteme)
- Sicherheitsschlösser
- Kontrollierte Schlüsselvergabe, Transpondersystem/Codesperren

Weitere Maßnahmen:

Schlüssel werden zudem nur an Geschäftsführer herausgegeben, die Öffnung der Schließanlagen für Mitarbeiter erfolgt über Zugangs-Chips. Der Netzwerkraum ist zusätzlich und separat über Schlüssel gesichert.

Zugangskontrolle:

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können:

- Login mit Benutzername und Passwort

Weitere Maßnahmen:

lawpilots nutzt ein Kennwortverfahren, bei dem jeder User einen persönlichen und Individuellen Log-In zum System erhält. Die Kennwörter müssen über eine Mindestlänge verfügen und Sonderzeichen enthalten. Zusätzlich setzt lawpilots einen Passwortmanager ein, sodass jeder Account und jeder Log-In über ein individuelles und sicheres Passwort zu erreichen ist.

Accounts werden zudem automatisch gesperrt und sind nur über das Kennwort wieder erreichbar. Ein Berechtigungskonzept begrenzt die Anzahl der berechtigten Mitarbeiter und legt fest, welcher Mitarbeiter, auf welche Daten Zugriff hat. Datenträger werden verschlüsselt.

Zugriffskontrolle:

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Einsatz von Berechtigungskonzepten (Regelungen zur Einrichtung, Einteilung von Benutzerkennungen, Benutzergruppen und Rechteprofilen)
- Verarbeitung personenbezogener Daten entspricht dem Berechtigungskonzept
- Dokumentation der vergebenen Benutzerkennungen, Benutzergruppen und Rechteprofile
- Protokollierung der Zugriffe auf Anwendungen, Apps (Eingabe, Änderung und Löschung von Daten)

Weitere Maßnahmen:

lawpilots hat ein Berechtigungskonzept integriert. Mitarbeitern wird je nach Befugnis ein Profil bzw. eine Rolle zugeordnet. Zudem findet eine Dokumentation statt, welcher Mitarbeiter welche Schritte ausgeführt hat.

Trennungskontrolle:

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist:

- Ein schriftliches Identitäts- und Berechtigungsmanagement ist im Einsatz
- Das Berechtigungsmanagement unterstützt den Grundsatz der Funktionstrennung
- Restriktive Vergabe von Datenbankrechten an Benutzer- und Gruppen-ID
- Getrennte physikalische Aufbewahrung von Clients und der verwendeten Datenbanken von Clients
- Trennung von Produktiv- und Testumgebung (Entwicklung)

Weitere Maßnahmen:

Das Berechtigungskonzept regelt die Trennung. Die Kunden von lawpilots werden softwareseitig auf der Lernplattform voneinander getrennt. Das Produktivsystem ist außerdem vom Testsystem getrennt.

Maßnahmen zur Sicherung der Integrität:

Datenintegrität:

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden:

- Einspielen neuer Releases und Patches mit (Release-/Patchmanagement)
- Funktionstest bei Installation und Releases

Transportkontrolle:

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

- E-Mail-Verkehr ist transportverschlüsselt (TLS)
- Verwendung eines Verschlüsselten Kommunikationsprotokolls auf dem Webserver (https)

Weitere Maßnahmen:

lawpilots übermittelt die Daten über verschlüsselte Verbindungen.

Eingabekontrolle:

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind:

- Dokumentation, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Aufbewahrung von Formularen, deren Daten in automatisierte Verarbeitungen übergegangen sind

Weitere Maßnahmen:

lawpilots speichert und protokolliert die Aktivitäten der lawpilots-Mitarbeiter auf der Lernplattform und bewahrt diese Protokolle mindestens drei Jahre auf.

Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit:

Zuverlässigkeit:

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

- Notfallpläne und Notfallmanagement (Wiederherstellung der Verfügbarkeit)
- Mitarbeiter für Notfallmanagement sensibilisiert

Weitere Maßnahmen:

lawpilots hat einen IT-Notfallkontakt eingerichtet, unter dem Mitarbeiter Fehlfunktionen melden können.

Maßnahmen zur regelmäßigen Evaluation:

Überprüfungsverfahren:

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen:

- Datenschutzmanagement-Software
- Formalisierte Prozesse für Datenschutzvorfälle
- Abschluss der notwendigen Vereinbarungen zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
- Schriftliche Weisungen an den Auftragsverarbeiter
- Verpflichtung der Mitarbeiter des Auftragsverarbeiter auf Datengeheimnis
- Formalisiertes Auftragsmanagement

Weitere Maßnahmen:

lawpilots verfügt über ein Datenschutzmanagement, es findet außerdem eine regelmäßige Re-Zertifizierung statt. Datenschutzvorfälle werden in formalisierten Prozessen abgebildet, sofern sie auftreten. Über dies hinaus findet eine Dokumentierung von Weisungen der Auftraggeber statt.

Maßnahmen zur Auftragskontrolle:

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

- Datenschutzmanagement-Software
- Formalisierte Prozesse für Datenschutzvorfälle
- Prüfung der vom Auftragsverarbeiter getroffenen Maßnahmen
- Abschluss der notwendigen Vereinbarungen zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
- Schriftliche Weisungen an den Auftragsverarbeiter
- Verpflichtung der Mitarbeiter des Auftragsverarbeiter auf Datengeheimnis
- Formalisiertes Auftragsmanagement

Anhang V. Liste der Unterauftragsverarbeiter

Der Auftragsverarbeiter arbeitet derzeit bei der Erfüllung des Auftrags mit den folgenden weiteren Auftragsverarbeitern zusammen, mit deren Beauftragung sich der Verantwortliche einverstanden erklärt. Die Dateverarbeitung findet ausschließlich innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraum statt.

Sofern die Datenverarbeitung außerhalb des Europäischen Wirtschaftsraumes stattfindet oder Zugriffe von außerhalb des Europäischen Wirtschaftsraumes erfolgen, so wird ein angemessenes Datenschutzniveau bei der Verarbeitung gem. Art. 44 ff. DSGVO mithilfe von z.B. EU-Standardvertragsklauseln, BCR oder Angemessenheitsbeschluss der EU-Kommission sichergestellt werden.

Telekom Deutschland	Landgrabenweg 151 53227 Bonn Deutschland	Datenbank der Teilnehmerdaten an Onlineschulungen
Userlike	Probsteigasse 44-46 50670 Köln Deutschland	Kundenservice via Chat
Mailjet SAS	13-13 bis, rue de l'Aubrac 75012 Paris France	Transaktions-E-Mails für die Lernplattform
Hornetsecurity GmbH	Am Listholze 78, 30177 Hannover, Deutschland	Erbringung von Dienstleistungen im Rahmen des Cyber-Security-Aware- ness-Trainings — bei Buchung des Moduls "Phishing Simulation".