Smart Lens Dienstleistungsvereinbarung

Inhalt

„Smart Lens SaaS-Endnutzerbedingungen“

zwischen der

FiveX GmbH
Linkstr. 2
10785 Berlin

als Anbieter der Smart Lens SaaS-Lösung

- Im Folgenden als **„Anbieter“** bezeichnet. -

und

Endnutzer

- Im Folgenden als **„gewerblicher Endkunde"** bezeichnet. -

- Gemeinsam als **„die Vertragsparteien“** bezeichnet. -

Präambel

„Smart Lens SaaS“ ist eine cloudbasierte Cyber Security Lösung zur kontinuierlichen Überwachung von Webseiten/URLs auf vorher definierte Schwachstellen.

„Smart Lens SaaS“ darf ausschließlich für legale Zwecke durch berechtigte Nutzer zur Schwachstellenprüfung von Webseiten/URLs genutzt werden, für die der gewerbliche Endkunde rechtlich zur Schwachstellenprüfung berechtigt ist.

„Smart Lens SaaS“ wird ausschließlich als SaaS-Lösung („Software-as-a-Service“) zur entgeltlichen Nutzung vom Anbieter bereitgestellt. Eine lokale zur Verfügungstellung von Hardware oder Software durch den Anbieter bei dem gewerblichen Endkunden erfolgt nicht. Der Zugriff und die Nutzung von „Smart Lens SaaS“ durch den gewerblichen Endkunden erfolgt ausschließlich Webbasiert als SaaS-Lösung.

„Smart Lens SaaS“ ist eine reine Business-to-Business (B2B)-Lösung. Endkunden des Anbieters können nur Unternehmer im Sinne von § 14 BGB werden. Ein Abschluss von Verträgen mit Verbrauchern im Sinne von § 13 BGB ist nicht möglich und durch die Endnutzerbedingungen ausgeschlossen.

1. Geltungsbereich, gewerbliche Endkunden, erweiterte Endnutzerbedingungen

Diese Endnutzerbedingungen gelten ausschließlich für das Produkt „Smart Lens SaaS“.

Smart Lens SaaS ist eine reine B2B-SaaS-Lösung. Gewerbliche Endkunden können nur Unternehmer im Sinne von § 14 BGB werden. Ein Abschluss von Verträgen mit Verbrauchern im Sinne von § 13 BGB ist ausgeschlossen. Der gewerbliche Endkunde garantiert mit Zustimmung zu diesen Endnutzerbedingungen, dass er Unternehmer gemäß § 14 BGB ist. Er wird im Rahmen der Abfrage vor online-Vertragsschluss die dort integrierte Abfrage wahrheitsgemäß ausfüllen.

Es gelten ergänzend die „erweiterten Endnutzerbedingungen Smart Lens SaaS“, welche im Anhang „Erweiterte Endnutzerbedingungen Smart Lens SaaS“ niedergelegt sind.

2. Vertragsgegenstand

Diese Smart Lens SaaS Endnutzerbedingungen und deren Anlagen regeln **a)** die Rechte und Pflichten der Vertragsparteien betreffend den Zugriff und den Umfang der entgeltlichen Nutzung der Funktionalitäten der Smart Lens SaaS-Lösung durch den gewerblichen Endkunden und **b)** die Einräumung von einfachen Nutzungsrechten zur Nutzung von Smart Lens SaaS durch den Anbieter.

3. Umfang der Nutzung und Endnutzerbedingungen von Smart Lens SaaS

Die Smart Lens SaaS-Lösung und ihre Funktionalitäten werden **„As-it-Is“** zur Verfügung gestellt. Die Funktionalitäten und Elemente von Smart Lens SaaS sind vorgegeben und werden nicht weiter individualisiert.

Der gewerbliche Endkunde verpflichtet sich alle rechtlichen Anforderungen im Zusammenhang mit Nutzung von Funktionalitäten von Smart Lens SaaS selbst zu prüfen und einzuhalten.

Der Umfang der Nutzung und die Nutzungsrechte von Smart Lens SaaS richten sich nach dem **Anhang „Erweiterte Endnutzerbedingungen Smart Lens SaaS“**.

4. Leistungsbeschreibung

Die jeweils aktuelle Produkt- und Leistungsbeschreibung von Smart Lens SaaS ergeben sich aus der **Anlage „Endnutzer - Leistungs- und Produktbeschreibung Smart Lens SaaS“**.

Der Umfang der Leistungen ist abhängig von der durch den gewerblichen Endnutzer getroffenen Produktauswahl.

5. Verfügbarkeit, Performance und Support der Smart Lens

Die Verfügbarkeit, Performance und Support von Smart Lens SaaS richten sich nach der **Anlage „Endnutzer - SLA“**.

6. Hard- und Software Anforderungen

Eine Anbindung des gewerblichen Endkunden an das Internet, die Beschaffung und/oder Bereitstellung von für die Nutzung von Smart Lens SaaS erforderlichen Hard- und Software stellt die Verpflichtung gewerblichen Endkunden selbst dar und ist nicht durch den Anbieter geschuldet.

Die zur Nutzung von Smart Lens SaaS durch den gewerblichen Endkunden erforderliche Software und Hardware ergeben sich aus der **Anlage „Endnutzer - Hard- und Software-Anforderungen“**.

7. Vertragsschluss Smart Lens SaaS Endnutzerbedingungen

Der Vertragsschluss über die Smart Lens SaaS-Lösung erfolgt ausschließlich Online.

8. Vergütung

Die Vergütung richtet sich nach der Preisangabe zum jeweiligen Lizenzmodell.

Alle Preise **sind Nettopreise zuzüglich** der jeweils in der Bundesrepublik Deutschland gültigen gesetzlichen **Umsatzsteuer**. Unternehmen innerhalb der EU, aber außerhalb Deutschlands, die über eine gültige Umsatzsteuer-Identifikationsnummer (USt-IdNr.) verfügen, wird in der Regel keine deutsche Umsatzsteuer berechnet. Stattdessen wird das Reverse-Charge-Verfahren angewendet, bei dem der Käufer die Umsatzsteuer im eigenen Land deklarieren und abführen.

9. Vertragslaufzeit

Die Smart Lens SaaS Endnutzerbedingungen werden für einen Monat geschlossen und verlängern sich automatisch um jeweils einen weiteren Monat, wenn sie nicht von einer Vertragspartei wirksam gemäß den Regelungen im **Anhang „Erweiterte Endnutzerbedingungen Smart Lens SaaS“** gekündigt wurden. Die Laufzeit beginnt mit dem Onlinevertragsschluss.

10. Unterauftragnehmer

Der Anbieter ist grundsätzlich zum Einsatz von Unterauftragnehmern bei der Leistungserbringung berechtigt, soweit der Einsatz eines spezifischen Unterauftragnehmers für den gewerblichen Endkunden nicht unzumutbar ist. Der gewerbliche Endkunde erteilt hierzu seine grundsätzliche Einwilligung. Bei Unterauftragnehmern, die personenbezogene Daten des gewerblichen Endkunden im Auftrag (unter)verarbeiten, gehen die Regelungen zur Unterbeauftragung von Unterauftragsverarbeitern im **Anhang II „Endnutzer Auftragsverarbeitungsvereinbarung Smart Lens SaaS“** dieser Regelung vor.

11. Rangfolge

Die Vertragsbestandteile gelten in folgender Rangfolge:

1. Diese „Smart Lens SaaS Endnutzerbedingungen“
2. Die Anlage C1 „Endnutzer - Leistungs- und Produktbeschreibung Smart Lens SaaS“
3. Die Anlage C2 „Endnutzer - Hard- und Software-Anforderungen“
4. Die Anlage C3 „Endnutzer - Service Level Agreement“
5. Der Anhang „Erweiterte Endnutzerbedingungen Smart Lens SaaS“

Der Anhang II „Auftragsverarbeitungsvereinbarung Smart Lens SaaS (AVV)“ geht in ihrem Anwendungsbereich bei der Verarbeitung im Auftrag von personenbezogenen Auftraggeberdaten den Smart Lens SaaS Endnutzerbedingungen den anderen Vertragsbestandteilen vor.

Anhang „Erweiterte Endnutzerbedingungen Smart Lens SaaS“

1. Abweichende Geschäftsbedingungen, Individualvereinbarungen, Ausschluss § 327 ff BGB

(1) Abweichende Allgemeine Geschäftsbedingungen des gewerblichen Endkunden werden nicht Vertragsbestandteil. Das Vorstehende gilt dann nicht, wenn und soweit der Anbieter abweichenden Allgemeinen Geschäftsbedingungen des gewerblichen Endkunden ausdrücklich zugestimmt hat. Diese Zustimmung soll zu Beweiszwecken zumindest in Textform dokumentiert werden. Die Beweislast trifft diejenige Vertragspartei, die sich auf abweichende Allgemeine Geschäftsbedingungen beruft.

(2) Zwischen dem gewerblichen Endkunden und dem Anbieter getroffene Individualvereinbarungen haben stets Vorrang vor diesem Vertrag. Diese sollen zu Beweiszwecken in Textform dokumentiert werden. Die Beweislast trifft diejenige Vertragspartei, die sich auf die jeweilige Individualvereinbarung beruft.

(3) Der Anbieter schließt Verträge über die Nutzung von Smart Lens SaaS ausschließlich mit gewerblichen Endkunden i.S.d. § 14 BGB ab. Eine Leistungserbringung an Verbraucher oder zur Erbringung einer gegenüber einem Verbraucher geschuldeten eigenen Leistung des gewerblichen Endkunden liegt nicht vor. § 327 BGB - § 327 s BGB liegen nicht vor und werden zwischen den Vertragsparteien vorsorglich ausgeschlossen. Die Anwendbarkeit der § 327 t BGB und § 327 u BGB werden ebenfalls vorsorglich ausgeschlossen.

2. Nutzungsrechte Smart Lens SaaS

(1) Der Anbieter räumt dem gewerblichen Endkunden mit Bezahlung der entsprechenden Vergütungen entgeltlich einfache Nutzungsrechte zum Zugriff und der Nutzung von Leistungen und Funktionen von Smart Lens SaaS ein. Der Zugriff und die Nutzung sind zeitlich auf die Dauer der ungekündigten Smart Lens SaaS Endnutzerbedingungen, örtlich auf das Gebiet der Europäischen Union und inhaltlich auf den Zweck der Eigennutzung durch ausschließlich den gewerblichen Endkunden i.S.d. § 14 BGB beschränkt. Eine Untervermietung und/oder eine Nutzung zu Zwecken der eigenen Leistungserbringung gegenüber Dritten sind nicht zulässig.

(2) Der Anbieter räumt den Zugriff und Nutzung von Smart Lens SaaS in der jeweils aktuellen Produkt-Version ein. Individuelle Anpassungen der Funktionalitäten von Smart Lens SaaS erfolgen nicht.

(3) Nutzungsrechte am Source Code und/oder Bearbeitungsrechte werden nicht eingeräumt. Eine Überlassung des Source-Codes ist nicht geschuldet.

(4) Der gewerbliche Endkunde ist ausschließlich dann berechtigt Bestandteile der Smart Lens SaaS zu dekompilieren, wenn und soweit dies gesetzlich vorgesehen ist.

(5) Smart Lens SaaS wird ausschließlich „As it Is“ zur Nutzung bereitgestellt. Eine Offenlegung von Schnittstellenbeschreibungen ist nicht geschuldet.

(6) Smart Lens SaaS wird kontinuierlich um neue Funktionalitäten und technische Möglichkeiten erweitert. Der Umfang der berechtigten Nutzung und die Rechte zur Nutzung gemäß dieser Ziffer gelten entsprechend für den jeweils aktuellen Stand der Smart Lens SaaS.

3. Vertragsschluss, Vertragsanpassungen dieser Nutzungsbedingungen

(1) Die Smart Lens SaaS Endnutzerbedingungen können ausschließlich online durch Auswahl des Produkts abgeschlossen werden.

(2) Smart Lens SaaS ist ein Produkt in Progress. Die Funktionalitäten von Smart Lens SaaS werden nach eigenem Ermessen des Betreibers Smart Nexus kontinuierlich erweitert.

(3) Der Anbieter hat ein legitimes organisatorisches Bedürfnis nach einer einfachen Vertragsabwicklung. Um diesem Bedürfnis zu entsprechen und dabei die legitimen Belange des gewerblichen Endkunden zu schützen, vereinbaren die Vertragsparteien die folgende Regelung zur Anpassung dieser Nutzungsbedingungen.

(4) Der Anbieter ist berechtigt, diese Nutzungsbedingungen einseitig anzupassen, wenn dies notwendig ist, um Änderungen der technischen, rechtlichen und wirtschaftlichen Rahmenbedingungen zu berücksichtigen, die nach Vertragsschluss eintreten und die nicht durch den Anbieter verursacht wurden. Die Anpassungen sollen insbesondere auch dazu dienen, dass sich der Anbieter rechtskonform verhalten und eigene vertragliche Pflichten gegenüber Dritten einhalten kann, die Grundlage seiner angebotenen Leistung gegenüber dem gewerblichen Endkunden sind.

(5) Unter diese Klausel dürfen nur Änderungen fallen, die für den gewerblichen Endkunden zumutbar sind, den bestimmungsgemäßen Vertragszweck nicht gefährden und keine Hauptleistungspflichten betreffen.

(6) Eine Anpassung der Preise fällt nicht unter den Anwendungsbereich dieser Klausel und ist einer eigenständigen Regelung vorbehalten.

(7) Der Anbieter wird den gewerblichen Endkunden mindestens dreißig Tage vor dem geplanten Inkrafttreten der Anpassungen in zumindest Textform über die geplanten Anpassungen informieren. Die Information erfolgt unter optischer Hervorhebung der geplanten Anpassungen und klarer deutlicher Beschreibung der geplanten Anpassungen, deren Auswirkungen für den gewerblichen Endkunden und eines Hinweises auf ein Widerspruchsrecht des gewerblichen Endkunden sowie den Auswirkungen seiner Ausübung und/oder Nichtausübung seines Widerspruchsrechts.

(8) Der gewerbliche Endkunde kann den geplanten Anpassungen innerhalb von 21 Tagen nach Zugang der Anpassungsbenachrichtigung in zumindest Textform widersprechen. Widerspricht der gewerbliche Endkunde den Anpassungen nicht innerhalb dieser Frist und nutzt der gewerbliche Endkunde das Produkt Smart Lens über 30 Tage nach Zugang der Anpassungsbenachrichtigung hinaus weiter, gelten die Anpassungen als durch den gewerblichen Endkunden angenommen.

(9) Widerspricht der gewerbliche Endkunde fristgerecht, steht beiden Vertragsparteien das Recht zu, die zum Zeitpunkt vor der Anpassung geltende Nutzungsvereinbarung über das Produkt Smart Lens mit einer Kündigungsfrist von einem Monat ab Zugang des Widerspruchs zu kündigen.

(10) Der Anbieter kann die optische und graphische Gestaltung, die Funktionalitäten und die eingesetzte Technik nach eigenem billigem Ermessen unter Berücksichtigung der berechtigten Interessen des gewerblichen Endkunden jederzeit ändern, soweit es zu keiner unbilligen Einschränkung der zum Zeitpunkt des Vertragsschlusses wesentlichen Merkmale kommt, welche den gewerblichen Endkunden unbillig und unangemessen einschränken. Der gewerbliche Endkunde hat für diesen Fall ein jederzeitiges außerordentliches Kündigungsrecht.

(11) Smart Lens SaaS unterliegt den jeweiligen Nutzungs-/Lizenzbedingungen von Smart Nexus. Der Anbieter hat auf deren Gestaltung keinen Einfluss. Für den Fall, dass der Smart Nexus seine eigenen Nutzungs-/Lizenzbedingungen ändert, ist der Anbieter berechtigt diese Änderungen auch gegenüber seinem gewerblichen Endkunden vertraglich weiterzugeben. Der gewerbliche Endkunde hat auch in diesem Fall ein außerordentliches Kündigungsrecht.

4. Hosting von Smart Lens SaaS Nutzungsdaten

(1) Soweit der Anbieter Daten im Rahmen der Nutzung von Smart Lens SaaS für den gewerblichen Endkunden hostet, wird der Anbieter angemessene Maßnahmen zur Datensicherheit treffen.

(2) Eine gesonderte Verpflichtung des Anbieters Sicherungskopien dieser Daten anzufertigen, besteht nicht. Der Anbieter ist nicht mit der Datensicherung für den gewerblichen Endkunden beauftragt.

5. Zahlungsbedingungen, Fälligkeit der Vergütung

Die Zahlungen werden über den Zahlungsdienstleister Stripe automatisiert eingezogen und sind sofort fällig.

6. Pflichten des gewerblichen Endkunden

(1) Der gewerbliche Endkunde nennt dem Anbieter einen Ansprechpartner, der sämtliche zur Durchführung der Smart Lens SaaS Endnutzerbedingungen erforderlichen Informationen und Auskünfte erteilen kann und rechtsverbindliche Willenserklärungen und Handlungen vornehmen kann.

(2) Der gewerbliche Endkunde verpflichtet sich zur Einhaltung aller rechtlichen Vorgaben bei der Nutzung von Smart Lens SaaS. Der gewerbliche Endkunde verpflichtet sich insbesondere wettbewerbsrechtliche, strafrechtliche und datenschutzrechtliche Bestimmungen einzuhalten.

Insbesondere verpflichtet er sich, die erlangten Informationen aus der Anwendung der Software lediglich zur Verbesserung der Sicherheit von Webseiten und nicht zum Schaden von Dritten zu verwenden.

(3) Der gewerbliche Endkunde benennt dem Anbieter Art und Umfang möglicher Störungen bei der Softwareanwendung, um die Bedingungen der vereinbarten Service Level geltend machen zu können.

7. Kündigung, außerordentliches Kündigungsrecht

(1) Die Smart Lens SaaS Endnutzerbedingungen können von beiden Vertragsparteien ordentlich zum Ende eines Monats für den übernächsten Monat gekündigt werden.

(2) Beiden Vertragsparteien bleibt das Recht zur außerordentlichen Kündigung unbenommen.

(3) Dem Anbieter steht ein außerordentliches Kündigungsrecht insbesondere dann zu, wenn ein gewerblicher Endkunde in Publikationen und Meinungsäußerungen insbesondere extremistische, geringschätzende Verlautbarungen in den Bereichen Ethnie, Geschlecht oder

Religion äußert. Die Gültigkeit der Umsatzsteuer-ID, die Nennungen auf der US-Sanktionsliste sowie im Sinne dieses Vertrages ungeeignete Publikationen des gewerblichen Endkunden werden von im Sinne dieses Absatzes als wichtiger Kündigungsgrund angesehen werden.

(4) Alle Kündigungen haben schriftlich an die von den Vertragsparteien benannten postalischen Adressen zu erfolgen.

8. Wohlverhaltenspflichten bei Vertragsbeendigung

(1) Bei Beendigung des Vertrages über Smart Lens SaaS, gleich aus welchem Rechtsgrund, verpflichten sich die Vertragsparteien den Vertrag ordnungsgemäß abzuwickeln.

(2) Der Anbieter wird die über Smart Nexus SaaS gespeicherten Daten des gewerblichen Endkunden auf seine Kosten in dem von dem Anbieter festgelegten Format in digitaler Form an die vom gewerblichen Endkunden hinterlegte E-Mail-Adresse in verschlüsselter Form übermitteln oder zum Download anbieten.

(3) Nach erfolgreicher Übermittlung der Daten und einer diesbezüglichen Bestätigung des gewerblichen Endkunden wird der Anbieter die Daten des gewerblichen Endkunden löschen, soweit für den Anbieter keine gesetzlichen/vertraglichen Aufbewahrungspflichten und/oder Aufbewahrungsrechte vorliegen.

9. Gewährleistung

(1) Der Anbieter leistet Gewähr, dass Smart Lens SaaS die in Leistungs- und Produktbeschreibung sowie den SLAs beschriebenen Funktionalitäten und Performancewerte im Wesentlichen erfüllt.

(2) Mängelansprüche bestehen nicht bei einer unerheblichen Abweichung von der vereinbarten oder vorausgesetzten Beschaffenheit und bei nur unerheblicher Beeinträchtigung der Gebrauchstauglichkeit.

(3) Der gewerbliche Endkunde übermittelt dem Anbieter eine ausführliche Beschreibung des aufgetretenen Mangels, seiner Begleitumstände und der damit verbundenen Relevanz in Textform.

(4) Fehlerbehebungen dürfen, soweit es dem gewerblichen Endkunden zumutbar ist auch durch Umgehungslösungen erbracht werden.

(5) Der Anbieter weist ausdrücklich auf § 536 b und § 536 c BGB hin. Beide Paragrafen und die daraus resultierenden Verpflichtungen finden Anwendung.

(6) Die Anwendung des § 536 a II BGB (Selbstbeseitigungsrecht des Mieters) ist ausgeschlossen.

(7) Die verschuldensunabhängige Haftung des Anbieters nach § 536 a I BGB für bereits zum Zeitpunkt des Vertragsschlusses vorhandene Fehler bei Software wird ausdrücklich ausgeschlossen.

(8) Soweit sich ein Mangel auf eine Leistung von eingebundenen Unterauftragnehmern des Anbieters bezieht, beschränkt sich die Mängelgewährleistung des Anbieters auf alle zumutbaren Maßnahmen, die unter finanziellen und technischen Gesichtspunkten durch den

Anbieter in zumutbarer Weise nach allgemeiner Verkehrsauffassung erwartet werden können.

10. Allgemeine Haftung

(1) Der Anbieter haftet für Vorsatz und grobe Fahrlässigkeit. Für leichte Fahrlässigkeit haftet der Anbieter nur bei Verletzung einer wesentlichen Vertragspflicht, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der gewerbliche Endkunde regelmäßig vertrauen darf sowie bei Schäden aus der Verletzung des Lebens, des Körpers, der Gesundheit, Produkthaftung, arglistigem Verschweigen oder einer Garantie.

(2) Die Haftung ist im Falle leichter Fahrlässigkeit summenmäßig beschränkt auf die Höhe des vorhersehbaren Schadens, mit dessen Entstehung typischerweise gerechnet werden muss.

(3) Maximal ist die Haftung für leichte Fahrlässigkeit jedoch beschränkt auf die geleisteten Zahlungen für die Produktnutzung, aber maximal beschränkt auf 10.000,- EUR pro Schadensfall und insgesamt auf 50.000,- EUR. Die Vertragsparteien sehen diese Summen als die maximalen vorhersehbaren Schäden an.

(4) Für den Verlust von Daten haftet der Anbieter insoweit nicht als der Schaden darauf beruht, dass es der gewerbliche Endkunde unterlassen hat, Datensicherungen durchzuführen und dadurch sicherzustellen, dass verlorengegangene Daten mit vertretbarem Aufwand wiederhergestellt werden können.

(5) Die vorstehenden Regelungen gelten auch zugunsten der Organe, Mitarbeiter und Erfüllungsgehilfen des Anbieters.

11. Rechte Dritter, Rechtsmängel

Macht ein Dritter gegenüber dem gewerblichen Endkunden Ansprüche wegen der Verletzung von Schutzrechten durch die Nutzung der Smart Lens SaaS geltend und wird deren Nutzung hierdurch beeinträchtig oder untersagt, haftet Smart Nexus ergänzend zu Ziffer 10 wie folgt:

(1) Der Anbieter kann im Rahmen seines Wahlrechts auf eigene Kosten entweder Smart Lens SaaS so ändern oder ersetzen, dass es das Schutzrecht nicht verletzt, aber im Wesentlichen noch den vereinbarten Funktions- und Leistungsmerkmalen in für den gewerblichen Endkunden in zumutbarer Weise entspricht, oder den gewerblichen Endkunden von Ansprüchen gegenüber dem jeweiligen Schutzrechtsinhaber freistellen.

(2) Die Vertragsparteien werden sich unverzüglich wechselseitig über geltend gemachte Ansprüche Dritter verständigen. Der gewerbliche Endkunde wird hierbei die behauptete Schutzrechtsverletzung nicht anerkennen und jegliche Auseinandersetzung einschließlich etwaiger außergerichtlicher Regelungen entweder dem Anbieter überlassen oder nur im Einvernehmen mit dem Anbieter führen. Der Anbieter erstattet dem gewerblichen Endkunden im Falle einer rechtskräftigen gerichtlichen Entscheidung notwendige Verteidigungskosten und sonstige Schäden, soweit dem gewerblichen Endkunden aus Rechtsgründen die geeigneten Abwehrmaßnahmen und Vergleichsverhandlungen vorbehalten bleiben bzw. bleiben müssen. Der gewerbliche Endkunde hat in diesem Fall Anspruch auf einen Vorschuss in Höhe der geschätzten notwendigen Verteidigungskosten.

(3) Soweit der gewerbliche Endkunde die Schutzrechtsverletzung selbst zu vertreten hat, sind Ansprüche gegen den Anbieter ausgeschlossen.

(4) Die Rechtsmängelhaftung erstreckt sich nicht auf Ansprüche wegen Patentverletzungen und Gebrauchsmusterverletzungen im Sinne der deutschen Rechtsordnung, die Dritte gegen den gewerblichen Endkunden geltend machen, wegen dessen Nutzung von Funktionalitäten der Smart Lens SaaS außerhalb der Europäischen Union.

12. Höhere Gewalt

(1) Der Anbieter haftet nicht in Fällen „Höherer Gewalt“. Fälle „Höherer Gewalt“ sind alle unvorhersehbaren Ereignisse sowie Ereignisse, die, soweit sie vorhersehbar gewesen wären, außerhalb der Einflusssphären der Vertragsparteien liegen. Darunter fallen insbesondere und nicht abschließend die folgenden Ereignisse:

(2) Naturkatastrophen wie Überschwemmungen, Sturmfluten, Orkan und Taifun sowie andere Unwetter im Ausmaß einer Katastrophe, Erdbeben, Blitzschlag, Lawinen- und Erdrutsche, Feuer, Seuchen, Pandemien, Epidemien und infektiöse Krankheiten (soweit eine solche von der WHO oder einem Ministerium ausgerufen wurde oder durch das Robert-Koch-Institut ein Gefahrenniveau von mindestens „mäßig“ festgelegt wurde), Krieg oder kriegsähnliche Zustände, Aufruhr, Revolution, Militär- oder Zivilputsch, Aufstand, Blockaden, Behörden und Regierungs-anordnungen, Streiks, Aussperrung.

(3) Tritt ein solches Ereignis „Höherer Gewalt“ ein, so ist der Anbieter verpflichtet, den gewerblichen Endkunden unverzüglich, spätestens innerhalb von 5 Werktagen nach Kenntnis in zumindest Textform über den Eintritt des Ereignisses und die Folgen seiner Leistungsbeeinträchtigung zu informieren.

(4) Der Anbieter ist in diesem Fall berechtigt, seine Leistungen je nach Umfang und Dauer des Ereignisses Höherer Gewalt und seiner Folgen anzupassen, ohne dass dem gewerblichen Endkunden ein Kündigungsrecht der Smart Lens SaaS Endnutzerbedingungen oder ein Schadensersatzanspruch zu gewähren ist. Für den Zeitraum der berechtigten Einschränkungen und/oder Verzögerungen gerät der Anbieter nicht in Verzug.

(5) Der Anbieter ist verpflichtet, alles in seiner Macht Stehende und Zumutbare zur Schadensminderung zu unternehmen.

(6) Soweit Einschränkungen und Ausfälle durch ein Ereignis Höherer Gewalt länger als einen Monat andauert, sind die Vertragsparteien zur gänzlichen oder teilweisen Kündigung der Smart Lens SaaS Endnutzerbedingungen berechtigt, ohne dass der gewerbliche Endkunde hieraus Ersatzansprüche ableiten kann

13. Konfliktvermeidung und Konfliktlösung

(1) Im Hinblick auf auftretende Meinungsverschiedenheiten und im Vorfeld etwaiger gerichtlicher Maßnahmen werden die Vertragsparteien versuchen, solche Meinungsverschiedenheiten partnerschaftlich zu lösen.

(2) Im Falle einer auftretenden Meinungsverschiedenheit werden die Vertragsparteien sich in Textform über mögliche Meinungsverschiedenheiten informieren. Diese Information enthält alle relevanten Fakten sowie Art und Umfang der Meinungsverschiedenheit. In Folge der Mitteilung in Textform werden die Vertragsparteien die Meinungsverschiedenheit partnerschaftlich diskutieren. Die Vertragsparteien werden für einen Zeitraum von mindestens fünf (5) Arbeitstagen versuchen, für die Meinungsverschiedenheit eine Lösung zu finden. Sofern und sobald eine Lösung gefunden ist, werden die Ansprechpartner diese in zumindest Textform dokumentieren.

(3) Sofern eine Meinungsverschiedenheit nicht gemäß der vorstehenden Ziffer gelöst wurde, kann jede Vertragspartei dies in Textform mitteilen und die Eskalation an die Vorstands- bzw. Geschäftsführerebene verlangen. Die Mitglieder der Vorstands- bzw. Geschäftsführerebene werden dann für einen Zeitraum von weiteren fünf (5) Arbeitstagen partnerschaftlich zusammenarbeiten, um die Meinungsverschiedenheit zu lösen. Sofern die Meinungsverschiedenheit auch innerhalb dieses Zeitraums nicht gelöst werden kann, ist jede Vertragspartei berechtigt, das Eskalationsverfahren für gescheitert zu erklären.

14. Gerichtsstand, Anwendbares Recht

(1) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des Kollisionsrechts. UN-Kaufrecht (CISG) gilt nicht.

(2) Die Vertragssprache ist deutsch.

(3) Ist der gewerbliche Endkunde Kaufmann ist der Gerichtsstand für alle Streitigkeiten aus diesem Vertragsverhältnis der Unternehmenssitz des Anbieters gemäß Impressum, sofern nicht ein ausschließlicher Gerichtsstand gegeben ist.

15. Salvatorische Klausel

Sollten einzelne Klauseln dieser Vereinbarung ganz oder teilweise unwirksam sein, so bleibt die Wirksamkeit der übrigen Klauseln unberührt.

Anlage C1 „Leistungs- und Produktbeschreibung Smart Lens SaaS“

1. Leistungsbeschreibung für IT-Monitoring

Smart Lens ist eine agentenfreie IT-Monitoring-Lösung, die speziell für Unternehmen entwickelt wurde, die eine effiziente Überwachung ihrer Netzwerkinfrastruktur suchen. Diese Plattform bietet fortschrittliche Monitoring-Funktionen ohne die Notwendigkeit, Agenten auf Zielgeräten zu installieren, wodurch sie ideal für Umgebungen mit hohen Sicherheitsanforderungen oder für Geräte, auf denen keine Software installiert werden kann, ist.

Hauptmerkmale

- Ping-Monitoring

Ständige Überwachung der Erreichbarkeit von Netzwerkgeräten und Diensten durch regelmäßige Ping-Anfragen. Dies hilft, die Verfügbarkeit kritischer Infrastrukturen zu gewährleisten und Probleme schnell zu identifizieren.

- Port-Monitoring

Überprüfung der Zugänglichkeit spezifischer Netzwerkports, um sicherzustellen, dass alle notwendigen Dienste verfügbar und funktionsfähig sind oder aber um sicherzustellen, dass eben diese Dienste nicht verfügbar sind.

Zusammenfassung

Smart Lens bietet eine leistungsfähige und flexible Lösung für das IT-Monitoring, das ohne die Installation von Agenten auf den Zielgeräten auskommt. Mit Funktionen wie Ping- und Portmonitoring hilft Smart Lens Unternehmen, ihre IT-Systeme effizient zu überwachen und zu verwalten. Diese Lösung ist ideal für Organisationen, die eine zuverlässige, skalierbare und sichere Monitoring-Plattform suchen, die minimale Eingriffe in die Zielumgebung erfordert.

2. Leistungsbeschreibung für Webseiten-Monitoring-Software

Einführung

Smart Lens ist eine hochentwickelte Webseiten-Monitoring-Lösung, die darauf ausgelegt ist, die Sicherheit, Verfügbarkeit und Reaktionsfähigkeit von Webdiensten zu gewährleisten. Dieses Tool bietet Unternehmen die Möglichkeit, ihre Webinfrastruktur umfassend zu überwachen, indem es kritische Aspekte wie SSL/TLS, DNS, und HTTP-Sicherheit kontinuierlich überprüft und analysiert.

Hauptmerkmale

- Verfügbarkeit und Reaktionszeiten

Ständige Überwachung der Verfügbarkeit Ihrer Webseiten und Messung der Reaktionszeiten, um sicherzustellen, dass Nutzer eine optimale Erfahrung erhalten.

- SSL/TLS-Monitoring

Kontinuierliche Überprüfung der SSL/TLS-Konfigurationen Ihrer Webseiten zur Sicherstellung der Verschlüsselungsstandards und Schutz sensibler Daten.

- TLS-Validierung

Überwachung und Validierung Ihrer TLS-Konfigurationen.

- HTTP-Header Security Check

Automatische Prüfung der HTTP-Header auf Sicherheitsrisiken und Empfehlung von Best Practices zur Minimierung von Schwachstellen.

- Port-Monitoring

Überwachung der Netzwerkports, die von Ihren Webanwendungen verwendet werden, um unautorisierten Zugriff und potenzielle Sicherheitslücken zu identifizieren.

- Footprinting der Anwendungsumgebung

Detaillierte Analyse und Kartierung der Webanwendungsumgebung, um ein vollständiges Bild der verwendeten Technologien und potenzieller Risiken zu erhalten.

- CVE-Scan

Regelmäßige Scans nach bekannten Schwachstellen (Common Vulnerabilities and Exposures - CVEs), um Sicherheitsrisiken proaktiv zu identifizieren und zu mittigeren.

Zusammenfassung

Mit Smart Lens bieten wir eine umfassende und robuste Lösung zur Überwachung und Sicherung Ihrer Webinfrastruktur. Durch den Einsatz modernster Technologien und konformer Standards verbessern Sie nicht nur die Leistung und Verfügbarkeit Ihrer Webdienste, sondern erhöhen auch deren Sicherheit. Mit Smart Lens können Sie sich darauf verlassen, dass Ihre Webpräsenz rund um die Uhr überwacht und geschützt wird, sodass Sie sich auf Ihr Kerngeschäft konzentrieren können.

3. Leistungsbeschreibung für Automatisierte Penetrationstests

Einführung

Smart Lens bietet eine leichtgewichtige Lösung für automatisierte Penetrationstests, die speziell entwickelt wurde, um die Sicherheitslücken in IT-Infrastrukturen systematisch zu identifizieren und zu bewerten. Diese Plattform ermöglicht es Unternehmen, ihre Netzwerke, Webseiten und IP-Adressen umfassend zu testen und somit ihre Verteidigungsstrategien gegen Cyberangriffe zu stärken.

Hauptmerkmale

- Scan von Webseiten

Detaillierte Sicherheitsanalyse von Webseiten, um Schwachstellen wie XSS, SQL Injection und andere Webbasierte Bedrohungen zu erkennen.

- Information Gathering (Footprinting der Zielsysteme)

Sammlung und Analyse von Informationen über die Zielsysteme, um eine Basis für weiterführende Angriffsszenarien zu schaffen.

- CVE-Scan Blackbox / Greybox

Durchführung von Schwachstellenscans unter Nutzung von Blackbox- oder Greybox-Ansätzen, um unbekannte Sicherheitslücken effektiv aufzudecken.

- Service Bruteforce (Check auf unsichere Anmeldedaten)

Testen der Robustheit von Service-Anmeldedaten gegenüber Bruteforce-Angriffen, um unsichere Passwörter zu identifizieren.

- Service Discovery (Spezifische Checks von Services auf Fehlkonfigurationen)

Untersuchung spezifischer Services auf Fehlkonfigurationen und potenzielle Sicherheitsmängel.

- Automatisierte wiederkehrende Scans

Möglichkeit zur Einrichtung automatisierter Scans, die in regelmäßigen Abständen durchgeführt werden, um die kontinuierliche Sicherheit zu gewährleisten.

- PDF-Berichte per E-Mail versende

Automatisiertes Versenden detaillierter Berichte in PDF-Form an vorgegebene E-Mail-Adressen nach Abschluss der Scans.

Zusammenfassung

Smart Lens stellt eine umfassende und anpassbare Lösung für automatisierte Penetrationstests dar, die darauf ausgerichtet ist, die Sicherheitsarchitektur von Unternehmen kontinuierlich zu überprüfen und zu verbessern. Durch die Integration fortschrittlicher Technologien und maßgeschneiderter Testmethoden ermöglicht Smart Lens eine aktive Erkennung und Behebung von Sicherheitsrisiken, um die Integrität und Sicherheit Ihrer IT-Infrastruktur zu gewährleisten.

4. Allgemeine Definitionen

a. Ausfallzeit

Eine Ausfallszeit kann sich auf folgende Bereiche beziehen:

- Nicht-Verfügbarkeit der Web-Oberfläche von Smart Lens
- Fehlfunktion der automatischen Scan-Planung
- Ausfall des automatischen Reporting bei hohen und kritischen Resultaten zum Zeitpunkt der Entdeckung

b. Messung der Verfügbarkeit bzw. Betriebszeit

Web-Oberfläche:

- Nutzung des Dienstleisters sentry.io
- Fehler-Monitoring durch den Anbieter
- Nutzung des Dienstleisters DigitalOcean
- Betriebszeiten-Monitoring durch den Anbieter

c. Scan-Planung

- Worker

Ein Worker ist ein Element in der Smart Lens Infrastruktur, dass für einzelne Aspekte des Scannings verantwortlich ist. Jeder Worker läuft in einem Node in einem Kubernetes-Cluster von Digital Ocean. Wir beziehen uns auf das Betriebs-zeiten-Monitoring des Anbieters Digital Ocean.

- Automatisches Reporting
- Supabase

Supabase wird als Auslöser für das automatische Reporting verwendet, weswegen wir uns auf die Betriebszeitenangaben von Supabase beziehen.

- MailerSend

Für den Mail-Transport wird MailerSend verwendet. Dieser Dienst stellt eine Statuspage zur Verfügung auf den Bezug genommen wird.

d. Ausschluss

Bezeichnet jede Störung oder Nichtverfügbarkeit der Dienste, die verursacht wird durch:

- Geplante Ausfallzeiten
- Ausrüstung, Software, Netzwerkverbindungen, Infrastruktur und andere Systeme des Kunden
- Nutzung der Dienste in Verletzung des Vertrags
- Nutzung von Diensten Dritter
- Änderungen an den Diensten, die nicht oder ohne Autorisierung durch vorgenommen wurden
- Systeme Dritter oder Handlungen oder Unterlassungen Dritter (z. B. DDoS-Angriffe)
- ein Ereignis höherer Gewalt oder Ausfall des Internets

e. Uptime

Bezeichnet die Serververfügbarkeit für die Dienste, ausgedrückt als Prozentsatz

f. Durchführung von Scans

- Verfügbarkeit für Scans: Smart Lens ermöglicht das Durchführen von Instant-Angriffsflächenscans zu jeder Zeit, ohne signifikante Verzögerungen.

g. Erstellung von Berichten

- Report-Generierung: Die Lösung bietet die Funktionalität, sowohl Executive als auch Technical Reports zu generieren. Diese Berichte sollen innerhalb von 15 Minuten nach Abschluss eines Scans verfügbar sein und detaillierte Einblicke in die Scan-Ergebnisse liefern.

h. Planung von Scans

- Planungsfunktionalität: Benutzer haben die Möglichkeit, Scans nach eigenem Zeitplan zu planen. Die Planungsfunktion ist durch eine intuitive Benutzeroberfläche zugänglich und ermöglicht das Einrichten, Bearbeiten und Löschen von geplanten Scans.

i. Mehrfachnutzung und Verwaltung

- Zugänglichkeit für IT-Mitarbeiter: Die Smart Lens-Lösung unterstützt die Verwaltung durch mehrere IT-Mitarbeiter gleichzeitig. Das System gewährleistet eine konsistente Leistung und Nutzbarkeit auch bei simultanem Zugriff durch verschiedene Nutzer.

j. Überwachung und Berichterstattung

- Zur Überwachung von Fehlern und der Verfügbarkeit unserer Dienste nutzen wir die Services von sentry.io. Sentry erfasst und aggregiert Fehlerdaten in Echtzeit und benachrichtigt das zuständige Personal, damit die identifizierten Probleme umgehend behoben werden können. Zusätzlich verwenden wir diese Informationen zur Aktualisierung unserer Statusseite, https://smart-lens.io, auf der der aktuelle Zustand des Dienstes „Smart Lens“ für Endkunden transparent dargestellt wird.

Support Typ	Starter Abo	Professional Basic	Professional Plus	Premium	Enterprise
E-Mail und Ticket-System zur Fehlermeldung	Ja	Ja	Ja	Ja	Ja
Aufbewahrung von Sicherungskopien der Produktionsdaten	n/a	7 Tage	10 Tage	14 Tage	30 Tage
Vorfall Klassifizierung	n/a	Ja	Ja	Ja	Ja

Leistungsindikatoren (KPIs)

1. Dauer des Angriffsflächenscans

Zielzeit für Scans: Jeder Angriffsflächenscan soll innerhalb von 15 Minuten abgeschlossen sein. Diese Zeitbeschränkung gilt nicht für Penetration-Testing-Maßnahmen, die aufgrund ihrer Komplexität eine längere Durchführungszeit erfordern.

2. Report-Generierung:

Verfügbarkeit der Berichterstellung: Nach Abschluss eines Scans muss es jederzeit möglich sein, alle verfügbaren Arten von Reports zu erstellen. Diese Funktion gewährleistet, dass Nutzer zeitnah Zugriff auf detaillierte Ergebnisse ihrer Sicherheitsanalysen erhalten.

3. Automatische Benachrichtigungen:

Reaktionsmechanismus bei kritischen Funden: Im Falle der Identifizierung von Problemen mit der Einstufung „Kritisch“ oder „Hoch“, erfolgt eine automatische Benachrichtigung der registrierten Nutzer per E-Mail. Dies stellt sicher, dass betroffene Parteien umgehend über wichtige Sicherheitsrisiken informiert sind und schnellstmöglich Maßnahmen zur Behebung einleiten können.

Anlage C2 „Hard- und Software-Anforderungen“

Hardwareanforderungen

Desktop:

1. Prozessor: Mindestens Dual-Core Prozessor (Intel i3 oder AMD-Äquivalent)

2. RAM: Mindestens 4 GB RAM, empfohlen 8 GB oder mehr

3. Speicherplatz: 100 MB freier Speicherplatz für Browserdaten und temporäre Dateien

4. Bildschirmauflösung: Mindestens 1366 x 768, empfohlen Full HD (1920 x 1080) oder höher

5. Internetverbindung: Breitbandinternet mit mindestens 5 Mbps Download- und Upload-Geschwindigkeit

Smartphone

1. Prozessor: Mindestens Quad-Core Prozessor (Snapdragon 450 oder höher, oder Äquivalent)

2. RAM: Mindestens 2 GB RAM, empfohlen 4 GB oder mehr

3. Speicherplatz: 50 MB freier Speicherplatz für Browserdaten und temporäre Dateien

4. Bildschirmauflösung: Mindestens 720p (1280 x 720), empfohlen Full HD (1920 x 1080) oder höher

5. Internetverbindung: Mobilfunkverbindung mit mindestens 4G LTE-Geschwindigkeit

Softwareanforderungen

Betriebssystem

- Desktop: Windows 10 oder höher, MacOS 10.13 (High Sierra) oder höher, neueste Linux-Distributionen

- Mobiltelefon: Android 8.0 (Oreo) oder höher, iOS 12.0 oder höher

Browser

- Unterstützte Browser: Google Chrome (neueste Version), Mozilla Firefox (neueste Version), Microsoft Edge (neueste Version), Safari (neueste Version)

- JavaScript: Muss aktiviert sein

- Cookies: Müssen aktiviert sein

- SSL/TLS: Unterstützung für TLS 1.2 oder höher

Zusätzliche Softwareanforderungen:

1. Plugins: Keine speziellen Plugins erforderlich, der Dienst sollte ohne zusätzliche Erweiterungen funktionieren

2. Frameworks und Bibliotheken: Sicherstellen, dass alle gängigen JavaScript-Frameworks (wie Angular, React, Vue.js) und Bibliotheken unterstützt werden, falls erforderlich

3. Kompatibilitätstests: Regelmäßige Tests zur Sicherstellung der Kompatibilität mit den oben genannten Betriebssystemen und Browsern

Sicherheitsanforderungen:

1. Authentifizierung: Unterstützung von 2-Faktor-Authentifizierung (2FA)

2. Verschlüsselung: Datenverschlüsselung sowohl während der Übertragung (SSL/TLS) als auch im Ruhezustand

3. Datenschutz: Einhaltung von Datenschutzbestimmungen wie GDPR, CCPA etc.

Anlage C3 „Service Level Agreement“

Einleitung	Diese Service Level Agreements „SLA“ unterstreichen unser Engagement für die Gewährleistung einer hohen Verfügbarkeit unserer Dienste für unsere Kunden. In diesem Dokument werden die spezifischen Vereinbarungen für jedes Produkt dargelegt, für das eine SLA besteht.
Begriffsbestimmung	
Geplante Ausfallzeit	Zeiträume der Ausfallzeit im Zusammenhang mit Netzwerk-, Hardware-, Software- oder Dienstwartung oder -Upgrades sowie das Patchen der Infrastruktur. Der Anbieter veröffentlicht mindestens drei Tage vor Beginn einer solchen Ausfallzeit eine entsprechende Mitteilung.
Wartungsfenster	generell: Fr. 22h - Mo. 4h die genauen Zeiten für diese Wartungsarbeiten können variieren, um den spezifischen Anforderungen unserer Kunden gerecht zu werden. Der genaue Zeitraum der Wartung wird 48h im Voraus angekündigt.
Notfallwartung	In Fällen, in denen dringende Notfallmaßnahmen erforderlich sind, um z.B. die Sicherheit und/oder Integrität der Dienste zu gewährleisten. Kunden werden über solche Maßnahmen so früh wie möglich informiert, wobei die Art der Maßnahme und der erwartete Einfluss auf den Service mitgeteilt wird.
Serviceverfügbarkeit	Der Prozentsatz der Gesamtzeit, während der die Dienstleistung des Anbieters verfügbar und funktionsfähig ist. Als Prozentwert angegeben. Die Serviceverfügbarkeit schließen geplante Wartungsfenster, geplante Ausfallzeiten und Notfallwartungen aus.
vereinbarten Betriebszeiten	Die vereinbarten Betriebszeiten bezeichnen den spezifischen Zeitraum, in dem ein IT-Service oder eine IT-Infrastruktur verfügbar und funktionsfähig sein muss. Die vereinbarten Betriebszeiten schließen geplante Wartungsfenster, geplante Ausfallzeiten und Notfallwartungen aus. Diese Zeiten werden gesondert vereinbart und kommuniziert und zählen nicht zu den vereinbarten Betriebszeiten. Während dieser Ausschlusszeiten ist der Dienstleister berechtigt, notwendige Wartungsarbeiten und Updates durchzuführen, ohne dass dies als Verstoß gegen die SLA-Verfügbarkeit gewertet wird.
überwachter Betrieb	Ein Dienstleistungsmodus, bei dem die Systemleistung und -verfügbarkeit kontinuierlich überwacht werden, um potenzielle Probleme frühzeitig zu erkennen und zu beheben.

Störungsmeldung	Eine Störungsmeldung beinhaltet die erforderlichen Informationen eines Anwenders, die zur Problemidentifikation erforderlich sind und die er dem für die Softwareprogrammierung Verantwortlichen Ansprechpartner per E-Mail oder Ticketsystem übermittelt. Dazu gehören insbesondere: Eine ausführliche Beschreibung des Vorfalls. Informationen über den Zeitpunkt und die Dauer der Ausfallzeit. Die Anzahl und den Standort der betroffenen Benutzer (falls zutreffend). Beschreibungen Ihrer Bemühungen, den Vorfall zum Zeitpunkt des Auftretens zu beheben.
Fehlerklassen	Schweregrad 1 Der Kunde kann das Produkt oder den Dienst größtenteils oder vollständig nicht nutzen (z. B. laden die meisten Seiten des Produkts nicht oder zeigen eine Fehlermeldung an). Es ist zu Datenkorruption oder Datenverlust gekommen oder wird dazu kommen.
	Schweregrad 2 Der Kunde wird daran gehindert, einen oder mehrere kritische Geschäftsprozesse auszuführen für eine erhebliche Anzahl von Nutzern, oder die Dienste sind mit eingeschränkten Fähigkeiten nutzbar und/oder es treten intermittierende Unterbrechungen auf, die ernsthafte geschäftliche Auswirkungen haben.
	Schweregrad 3 Die primäre Funktionalität des Produkts ist schwer beeinträchtigt und unbenutzbar. Kunden können ein gängiges Feature nicht vollständig nutzen. Es gibt eine Umgehungslösung, die Kunden nutzen können. Daten werden möglicherweise nicht wie erwartet angezeigt, sind aber nicht verloren. Es gibt keine kommerziell vernünftige Umgehungslösung für die Kunden.
	Schweregrad 4 Es wird eine Funktion vermisst, die nicht entwickelt ist. Oder einige Kunden erhalten intermittierende Fehlermeldungen und es gibt eine Umgehungslösung, die Kunden nutzen können.
Reaktionszeit	Die Zeit die ab Eingang einer Störungsmeldung bis zur ersten Reaktion des Dienstleisters vergeht.
Entstörzeit	Die Zeit die ab Eingang einer Störungsmeldung bis zur Behebung und Wiederherstellung des Normalbetriebes.

SLA's	**Wertebereich**
Serviceverfügbarkeit	im Monatsmittel 99,9%
überwachter Betrieb	5x10 - werktags Montag bis Freitag jeweils von 8:00 - 18:00
Reaktionszeit für Fehler des Schweregrad 1	1h innerhalb des überwachten Betriebes
Reaktionszeit für Fehler des Schweregrad 2	3h innerhalb des überwachten Betriebes
Reaktionszeit für Fehler des Schweregrad 3	24h innerhalb des überwachten Betriebes
Reaktionszeit für Fehler des Schweregrad 4	nicht vereinbart
Entstörzeit für Fehler des Schweregrad 1	8h innerhalb des überwachten Betriebes
Entstörzeit für Fehler des Schweregrad 2	24h innerhalb des überwachten Betriebes
Entstörzeit für Fehler des Schweregrad 3	140h innerhalb des überwachten Betriebes
Entstörzeit für Fehler des Schweregrad 4	nicht vereinbart
Diese Entstörzeiten stehen jedoch unter dem Vorbehalt höherer Gewalt oder anderer unvorhersehbarer und unkontrollierbarer Umstände, die von Dritten zu vertreten sind.	
Weiterentwicklungen	Die Unausschließbarkeit neuer Leistungsbausteine und Bedingungen der zugelieferten Dienste von Drittanbietern gewährleistet, dass alle Nutzer unabhängig von individuellen Beiträgen oder Nutzungsverhalten Zugang zu den vollen Funktionen und Diensten haben.

Revisionsrecht	Wir behalten uns das Recht vor, diese SLAs zu überarbeiten, um Anpassungen an technologische Entwicklungen oder Änderungen in den betrieblichen Anforderungen zu reflektieren.

Anhang II „Auftragsverarbeitungsvereinbarung Smart Lens SaaS (AVV)“

1. Allgemeines

(1) Smart Cyber Security verarbeitet personenbezogene Daten im Auftrag des Smart Nexus Partners i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 - Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

(1) Der Gegenstand des Auftrags ergibt sich aus § 1 „Smart Lens SaaS-Endnutzerbedingungen“ als SaaS-Vertrag zwischen den Parteien.

(2) Die Informationen zur Art der Daten und der Kategorien der betroffenen Personen sind in der SaaS-Plattform bzw. der jeweiligen Internetplattform des Smart Nexus Partners unter dem Menüpunkt „Datenschutz“ beschrieben.

3. Rechte und Pflichten des Smart Nexus Partners

(1) Der Smart Nexus Partner ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch Smart Cyber Security. Smart Cyber Security steht nach Ziff. 4 Abs. 5 das Recht zu, den Smart Nexus Partner darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Smart Nexus Partner ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Smart Cyber Security wird den Smart Nexus Partner unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber Smart Cyber Security geltend machen.

(3) Der Smart Nexus Partner hat das Recht, im Rahmen der von diesem zugesicherten Leistung jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber Smart Cyber Security zu erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Smart Nexus Partners bei Smart Cyber Security entstehen, bleiben unberührt.

(5) Der Smart Nexus Partner informiert Smart Cyber Security unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch Smart Cyber Security feststellt.

(6) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Smart Nexus Partner geltenden gesetzlichen Meldepflicht besteht, ist der Smart Nexus Partner für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten seitens Smart Nexus

(1) Smart Cyber Security verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Smart Nexus Partner erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Smart Cyber Security ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt Smart Cyber Security dem Smart Nexus Partner diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Smart Nexus Partners. Eine hiervon abweichende Verarbeitung von Daten ist Smart Cyber Security untersagt, es sei denn, dass der Smart Nexus Partner dieser schriftlich zugestimmt hat.

(2) Smart Cyber Security verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. **Eingebundene Zahlungs- oder ERP-Dienstleister haben mindestens Maßnahmen getroffen, um sicherzustellen, dass die Datenverarbeitung den Datenschutzanforderungen der DSGVO entspricht, einschließlich der Verwendung von Standardvertragsklauseln für Datenübertragungen außerhalb des EWR.**

(3) Smart Cyber Security sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) Smart Cyber Security ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Smart Nexus Partners verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Smart Cyber Security wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Smart Nexus Partner abstimmen.

(5) Smart Cyber Security wird den Smart Nexus Partner unverzüglich darüber informieren, wenn eine vom Smart Nexus Partner erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Smart Cyber Security ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Smart Nexus Partner bestätigt oder geändert wird. Sofern Smart Cyber Security darlegen kann, dass eine Verarbeitung nach Weisung des Smart Nexus Partners zu einer Haftung durch Smart Cyber Security nach Art. 82 DSGVO führen kann, steht Smart Cyber Security das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Die Verarbeitung von Daten im Auftrag des Smart Nexus Partners außerhalb von Betriebsstätten Smart Cyber Security oder Subunternehmern ist nur mit Zustimmung des Smart Nexus Partners in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Smart Nexus Partner in Privatwohnungen ist nur mit Zustimmung des Smart Nexus Partners in Schriftform oder Textform im Einzelfall zulässig.

(7) Smart Cyber Security wird die Daten, die er im Auftrag für den Smart Nexus Partner verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

5. Datenschutzbeauftragter des Smart Cyber Security

(1) Smart Cyber Security bestätigt, dass sie einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Smart Cyber Security trägt Sorge dafür, dass der

Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Smart Cyber Security wird dem Smart Nexus Partner den Namen und die Kontaktdaten auf seiner Webseite https://www.smart-nexus.de/de/rechtliches/datenschutz nennen.

(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Smart Nexus Partners entfallen, wenn er nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen und Smart Cyber Security nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Smart Nexus Partners gewährleisten.

6. Meldepflichten der Smart Cyber Security

(1) Smart Cyber Security ist verpflichtet, dem Smart Nexus Partner jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Smart Nexus Partners, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die Smart Cyber Security im Auftrag des Smart Nexus Partners verarbeitet.

(2) Ferner wird Smart Cyber Security den Smart Nexus Partner unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber Smart Cyber Security tätig wird und dies auch eine Kontrolle der Verarbeitung, die Smart Cyber Security im Auftrag des Smart Nexus Partners erbringt, betreffen kann.

(3) Smart Cyber Security ist bekannt, dass für den Smart Nexus Partner eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Smart Cyber Security wird den Smart Nexus Partner bei der Umsetzung der Meldepflichten unterstützen. Smart Cyber Security wird dem Smart Nexus Partner insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Smart Nexus Partners verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung Smart Cyber Security an den Smart Nexus Partner muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

- eine Beschreibung der von Smart Cyber Security ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten seitens Smart Cyber Security

(1) Smart Cyber Security unterstützt den Smart Nexus Partner bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

(2) Smart Cyber Security wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Smart Nexus Partner mit. Er hat dem Smart Nexus Partner die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Smart Cyber Security unterstützt den Smart Nexus Partner unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8. Kontrollbefugnisse

(1) Der Smart Nexus Partner hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Smart Nexus Partners durch den Smart Cyber Security jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Smart Cyber Security ist dem Smart Nexus Partner gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Smart Nexus Partner kann eine Einsichtnahme in die von Smart Cyber Security für den Smart Nexus Partner verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Der Smart Nexus Partner kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte von Smart Cyber Security zu den jeweils üblichen Geschäftszeiten vornehmen. Der Smart Nexus Partner wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe von Smart Cyber Security durch die Kontrollen nicht unverhältnismäßig zu stören.

(5) Smart Cyber Security ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Smart Nexus Partner i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Smart Nexus Partner zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Smart Nexus Partner ist über entsprechende geplante Maßnahmen von Smart Cyber Security zu informieren.

9. Unterauftragsverhältnisse

(1) Die Beauftragung von Unteranbietern durch Smart Cyber Security ist nur mit Zustimmung des Smart Nexus Partners in Textform zulässig. Smart Cyber Security nennt alle bestehenden Unterauftragsverhältnisse gem. Anlage II. Ein Wechsel der Unterauftragsnehmer sind dem Smart Nexus Partner unverzüglich mitzuteilen

(2) Smart Cyber Security hat den Unteranbieter sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Smart Nexus Partner und Smart Cyber Security getroffenen Vereinbarungen einhalten kann. Smart Cyber Security hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unteranbieter die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Smart Cyber Security zu dokumentieren und auf Anfrage dem Smart Nexus Partner zu übermitteln.

(3) Smart Cyber Security ist verpflichtet, sich vom Unteranbieter bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unteranbieter benannt worden ist, hat Smart Cyber Security den Smart Nexus Partner hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unteranbieter gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.

(4) Smart Cyber Security hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Smart Nexus Partners auch gegenüber dem Unteranbieter gelten.

(5) Smart Cyber Security hat mit dem Unteranbieter einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat Smart Cyber Security dem Unteranbieter dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Smart Nexus Partner und Smart Cyber Security festgelegt sind. Dem Smart Nexus Partner ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Smart Cyber Security ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieses Vertrages) des Smart Nexus Partners und von Aufsichtsbehörden auch gegenüber dem Unteranbieter gelten und entsprechende Kontrollrechte von Smart Nexus Partner und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unteranbieter diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(7) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die Smart Cyber Security 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 Smart Cyber Security für den Smart Nexus Partner erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Smart Cyber Security ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betreffen, die auch im Zusammenhang mit der Erbringung von Leistungen für den Smart Nexus Partner genutzt werden und bei der Wartung auf personenbezogene Daten zugegriffen werden kann, die im Auftrag des Smart Nexus Partners verarbeitet werden.

10. Vertraulichkeitsverpflichtung

(1) Smart Cyber Security ist bei der Verarbeitung von Daten für den Smart Nexus Partner zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Smart Cyber Security verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Smart Nexus Partner obliegen. Der Smart Nexus Partner ist verpflichtet, Smart Cyber Security etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Smart Cyber Security sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Smart Cyber Security sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Smart Cyber Security sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Smart Nexus Partners informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Smart Nexus Partner auf Anfrage nachzuweisen.

11. Wahrung von Betroffenenrechten

(1) Der Smart Nexus Partner ist für die Wahrung der Betroffenenrechte allein verantwortlich. Smart Cyber Security ist verpflichtet, den Smart Nexus Partner bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Smart Cyber Security hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Smart Nexus Partner erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung Smart Cyber Security für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Smart Nexus Partner erforderlich ist, wird Smart Cyber Security die jeweils erforderlichen Maßnahmen nach Weisung des Smart Nexus Partners treffen. Smart Cyber Security wird den Smart Nexus Partner nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Smart Nexus Partner bei Smart Cyber Security entstehen, bleiben unberührt.

12. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

13. Vergütung

Es ist neben dem Hauptvertrag keine gesonderte Vergütung vereinbart.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Smart Cyber Security verpflichtet sich gegenüber dem Smart Nexus Partner zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird Smart Cyber Security im Voraus mit dem Smart Nexus Partner abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können von Smart Cyber Security ohne Abstimmung mit dem Smart Nexus Partner umgesetzt werden. Der Smart Nexus Partner kann jederzeit eine aktuelle Fassung der von Smart Cyber Security getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Smart Cyber Security wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird Smart Cyber Security den Smart Nexus Partner informieren.

15. Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und wird auf unbestimmte Zeit geschlossen.

(2) Er ist mit einer Frist des Hauptvertrages kündbar.

(3) Der Smart Nexus Partner kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß Smart Cyber Security gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, Smart Cyber Security eine Weisung des Smart Nexus Partners nicht ausführen kann oder will Smart Cyber Security den Zutritt des Smart Nexus Partners oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

16. Beendigung

(1) Nach Beendigung des Vertrages hat Smart Cyber Security sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Smart Nexus Partners an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Smart Nexus Partner gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Smart Nexus Partner unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

(2) Der Smart Nexus Partner hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten Smart Cyber Security zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Smart Cyber Security erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Smart Nexus Partner angekündigt werden.

(3) Bei Beendigung dieses Vertrags hat der Geschäftskunde jegliche Nutzung der Software einzustellen.

17. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch Smart Cyber Security i. S. d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

18. Schlussbestimmungen

(1) Sollte das Eigentum des Smart Nexus Partners bei Smart Cyber Security durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat Smart Cyber Security den Smart Nexus Partner unverzüglich zu informieren. Smart Cyber Security wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Anlage 1 zum Vertrag zur Verarbeitung von Daten im Auftrag (AVV)

Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO in Verbindung mit §64 BDSG-neu.

Organisationskontrolle			
Organisatorische Maßnahmen zur Sicherstellung der besonderen Anforderung des Datenschutzes			
	Ja	**Nein**	**Bemerkungen**
Datenschutzbeauftragter vorhanden?	X		
Bitte nennen Sie uns Namen und Kontaktdaten des Datenschutzbeauftragten			Dr. Uwe Nolte info@datenschutz-qm.de
Gibt es ein IT-Sicherheitskonzept?	X		
Gibt es IT-Sicherheitsrichtlinien?	X		
Gibt es Datenschutzverpflichtungserklärungen Ihrer Mitarbeiter/ Werden Mitarbeiter auf den Datenschutz verpflichtet?	X		
Sonstiges: Gibt es die Rolle eines CISO?	X		Benjamin Gnahm
Zutrittskontrollen			
Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen mit personenbezogenen Daten zu verwehren			
	Ja	**Nein**	**Bemerkungen**
Gibt es einen Werkschutz?		X	Compliance-Abteilung ist zuständig
Gibt es eine Besucherregelung? Bitte geben Sie an, ob Besucherausweise ausgegeben werden o.ä.	X		Ja, ohne Ausweise für Besucher der Betriebsstätte
Gibt es eine Schlüsselregelung bzw. Zutrittskonzept? Bitte geben Sie dies an	X		Empfang für Besucherbereich, **Transponder Schlüsselsystem**
Alarmanlage		X	
Serverräume / -zugänge gesondert gesichert	X		
Automatisches Zugangskontrollsystem		X	
Schließsystem mit Codesperre		X	
Biometrische Zugangssperre		X	geplant, Angebote wurden eingeholt
Lichtschranken / Bewegungsmelder		X	
Schlüsselregelung (Ausgabe etc.)	X		
Besucherprotokollierung	X		
Sorgfältige Auswahl von Wachpersonal			Nicht relevant.

Absicherung von Gebäudeschächten			Nicht relevant.
Chipkarten- / Transponderschließsystem	X		
Manuelles Schließsystem	X		
Videoüberwachung der Zugänge		X	Angebote zur Beauftragung liegen vor.
Sicherheitsschlösser	X		
Personenkontrolle beim Pförtner / Eingang	X		
Sorgfältige Auswahl von Reinigungspersonal	X		
Tragepflicht von Berechtigungsausweisen		X	
Sonstiges:			keine Regelung
Zugangskontrolle			
Maßnahmen, die unbefugte an der Nutzung der Datenverarbeitungssysteme hindern			
	Ja	**Nein**	**Bemerkungen**
Zuordnung von Benutzerrechten	X		
Dokumentation von Benutzerzugängen	X		
Passwortvergabe	X		
Wie wird sichergestellt, dass nur erforderliche Berechtigungen eingeräumt werden?	X		Freigabesystem für alle Berechtigungen
Gibt es unternehmensexterne Zugänge zum Datenverarbeitungssystem? (Home-Office etc.)	X		Remote-Zugang via Remote-Desktop über gesicherte Leitungsverbindung
Werden eingeräumte Berechtigungen periodisch überprüft? Bitte geben Sie die Häufigkeit an.	X		jährlich
Authentifikation mit Benutzernamen / Passwort	X		
Wird eine Passwortkomplexität verlangt, bzw. technisch erzwungen?	X		
Wird eine Mindestpasswortlänge verlangt bzw. technisch erzwungen?	X		
Wird eine Mindestpasswortlänge verlangt bzw. technisch erzwungen?	s.o.		
Regelmäßige Änderung des Passworts	X		lt. BSI-Empfehlung nur anlassbezogene Änderungen
Gehäuseverriegelung sichergestellt	X		nur Remote-Desktops im Einsatz
Sperrung von externen Schnittstellen wie USB sichergestellt	X		Externe Schnittstellen müssen nicht gesperrt werden, da rein virtuelles Setup
Einsatz von Intrusion-Detection-Systemen		X	laufende Überwachung firmeninternen durch CISO
Werden mobile IT-Systeme verschlüsselt?	X		

Werden mobile Datenträger verschlüsselt?	X		Einsatz von hardwareseitig verschlüsselten Festplatten und USB-Sticks.
Verschlüsselung von Smartphone-Inhalten		X	geplant in 2024
Einsatz von Anti-Viren-Software	X		
Einsatz einer Hardware-Firewall	X		
Erstellen von Benutzerprofilen	X		
Authentifikation mit biometrischen Verfahren		X	teilweise
Überprüfen Sie die Dienstleister, die in Kontakt mit personenbezogenen Daten gelangen sorgfältig?	X		
Wie werden unberechtigte Zugriffe von Dritten auf IT-Systeme erkannt und unterbunden?	X		Logging und laufende Überwachung durch RZ
Zuordnung von Benutzerprofilen zu IT-Systemen	X		
Einsatz von VPN-Verschlüsselung	X		
Sicherheitsschlösser	X		
Verschlüsselung von Datenträgern in Laptops- / Notebooks	X		
Einsatz einer Software-Firewall	X		
Sonstiges:			keine Regelung
Zugriffskontrolle			
Nur Personen mit Zugriffsberechtigung können auf die der Zugriffsberechtigung unterliegenden Daten zugreifen. Personenbezogene Daten können zudem bei der Verarbeitung, Nutzung oder Speicherung nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden.			
	Ja	**Nein**	**Bemerkungen**
Bestehen eines Berechtigungskonzepts	X		
Werden Benutzerrollen/Berechtigungen regelmäßig überprüft? Wenn ja, wie oft?	X		jährlich
Wie wird sichergestellt, dass Benutzerrechte nach dem Ausscheiden der Person oder Wechsel der Aufgabe entzogen/geändert werden?	X		Einsatz dynamischer Berechtigungsgruppen. Automatisiertes On- und Off-Boarding.
Wie wird sichergestellt, dass Datenträger sicher gelöscht/vernichtet werden?	X		Relevant nur für Notebooks: Physischer Ausbau und Vernichtung durch professionellen Entsorgungsdienstleister
Wie wird die Vernichtung der Datenträger nachgewiesen?	X		

Anzahl der Administratoren auf kleinste notwendige Menge reduziert	X		Nutzung von Privileged Identity Management
Protokollierung von Zugriffen auf Anwendungen, insbesondere bei Eingabe, Änderung und Löschung von Daten	X		
Wie lange werden die Zugriffsprotokolle gespeichert?	X		Unterschiedlich, je nach Anwendung; i.d.R 30 – 90 Tage
Wer hat Zugriff auf diese Protokolle?	X		IT-Admin, nach schriftl. Aufforderung
Physische Löschung von Datenträgern vor Wiederverwendung	X		
Einsatz von Aktenvernichtern	X		
Einsatz von Dienstleistern zu Aktenvernichtung mit Gütesiegel	X		
Verschlüsselung von Datenträgern	X		Einsatz von hardwareseitig verschlüsselten Festplatten und USB-Sticks. Mobile Datenträger in Form von Notebooks via Bitlocker.
Verwaltung der Rechte durch Systemadministrator	X		
Passwortrichtlinie inkl. Passwortlänge und -wechsel	X		
Sichere Aufbewahrung von Datenträgern	X		OnSite NAS Speicher in verschlossenem Server Raum.
Ordnungsgemäße Vernichtung von Datenträgern	X		durch Beauftragung professioneller Dienstleister
Protokollierung der Vernichtung	X		Gemäß Standardprozess „Protokollierung von Löschung von Daten“ s.o.
Sonstiges:			keine Regelung
Weitergabekontrolle			
Sicherungsmaßnahmen, die gewährleisten, dass personenbezogene Daten bei elektronischer Übertragung, oder während des Transports, oder Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können, und dass überprüft und festgestellt werden kann, an welcher Stelle eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.			
	Ja	**Nein**	**Bemerkungen**
Wie wird der Schutz der Daten während des Transports gewährleistet?	X		Festplatten- USB-Verschlüsselung
Wie wird gewährleistet, dass Daten nach Beendigung des Auftrags sicher gelöscht werden?	X		per Arbeitsanweisungen

Wird die Löschung dokumentiert?	X		per Bestätigung der Arbeitsanweisung
Einrichtung von Standleitungen bzw. VPN-Tunneln	X		VPN für sie Site to Data Center Verbindung. RDP für die Client zu Data Center Verbindung.
E-Mail-Verschlüsselung des Transportweges	X		TLS-Verschlüsselung
Dokumentation der Empfänger von Daten und der geplanten Zeitspanne der Überlassung bzw. vereinbarter Löschfristen		X	
Sorgfältige Auswahl von Transportpersonal und -fahrzeugen bei physischem Transport gewährleistet	X		Keine physischen Transporte
Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen sichergestellt	X		Keine physischen Transporte
Sichere Transportbehälter/-verpackungen bei physischem Transport gegeben	X		Keine physischen Transporte
Sonstiges:			keine Regelung
Wiederherstellbarkeit			
Gewährleistung, dass System im Störungsfall wiederhergestellt werden kann			
	Ja	**Nein**	**Bemerkungen**
Sind Serverräume klimatisiert?	X		
Sind Datensicherungen verschlüsselt?		X	Backup erfolgt auf zentrale zentralisiert und ordnungsgemäß organisierter und abgesicherter Backupinfrastruktur
Gibt es einen Notfallplan?	X		Bestandteil der zentralen Infrastruktur des RZ-Dienstleisters
Wie wird eine rasche Datenwiederherstellung gewährleistet?	X		Durch Nutzung virtueller Systeme
Wo werden Datensicherungen aufbewahrt?	X		Rechenzentrum
Bitte beschreiben Sie ihr Datensicherungs- & Wiederherstellungskonzept	X		Tägliches Backup, Wiederherstellung automatisiert auf Anforderung

Gibt es Feuer- & Rauchmeldeanlagen? Bitte beschreiben	X		
Existiert eine unterbrechungsfreie Stromversorgung für die Server?	X		
Bestehen eines Back-Ups oder Festplattenspiegelung?	X		
Regelmäßige Datensicherung	X		
Sonstiges:			keine Regelung
Zuverlässigkeit			
Gewährleistung, dass Systemfehler gemeldet und behoben werden			
	Ja	**Nein**	**Bemerkungen**
Systemchecks	X		Automatisierte Durchführung
IT-Support	X		24/7
Durchführung von Updates	X		täglich automatisierter Prozess
Sonstiges:			
Auftragskontrolle			
Gewährleistung, dass Daten nur nach Weisung des Auftraggebers verarbeitet werden			
	Ja	**Nein**	**Bemerkungen**
Datenschutzschulungen der Mitarbeiter	X		
Übersendung von Protokollen über die Datennutzung bei Anfrage des Auftraggebers	X		
Sonstiges:			Keine Regelung
Trennbarkeit			
Daten die zu unterschiedlichen Zwecken erhoben werden, werden auch getrennt verarbeitet			
Bitte geben Sie die hierzu getroffenen Maßnahmen an			
Wie stellen Sie sicher, dass Daten, die zu verschiedenen Zwecken verarbeitet werden, auch getrennt verarbeitet werden?	X		Mittels Trennung in jeweils separaten Datenbanken
Wie wird sichergestellt, dass Daten von verschiedenen Kunden getrennt voneinander verarbeitet werden und ein Zugriff von Kunden auf Daten anderer Kunden ausgeschlossen ist.	X		Mehrmandantenfähigkeit des Dashboards, Rechteverwaltung

Wie stellen die Trennung von Test- und Produktivsystemen sicher?			Nutzung einer Mehr-System-Landschaft
Pseudonymisierung			
Kommt eine Pseudonymisierung oder Verschlüsselung von Daten zum Einsatz? Wenn ja, beschreiben Sie diese bitte	Nein		
Verfahren zur Überprüfung, Bewertung/Evaluierung			
	Ja	**Nein**	**Bemerkungen**
Übernimmt die Unternehmensleitung Verantwortung für Datenschutz- und Informationssicherheit übernommen?	X		
Gibt es Schulungsnachweise über die Verpflichtung der Mitarbeiter auf den Datenschutz?	X		Zertifikate
Werden die Beschäftigten zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet? Wenn ja, durch welche Maßnahme	X		Regelmäßige Unterweisungen und Arbeitsanweisungen
Wird die Umsetzung von Datenschutz durch Technikgestaltung und durch Datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) gewährleistet?	X		Technische und organisatorische Anforderungen an IT-Systeme werden sowohl bei der Planung als auch bei der Durchführung einer Verarbeitung in einen fortlaufenden Prozess berücksichtigt. Der Verantwortliche legt Zweck und Mittel der Verarbeitung, als den Zeitpunkt der Verarbeitung fest, achtet auf datenschutzfreundliche Voreinstellungen und dokumentiert diese gem. der Anforderungen bzgl. Privacy by Design.
Gibt es Richtlinien für Beschäftigte zum Umgang mit personenbezogenen Daten?	X		

Wie wird sichergestellt, dass Datenschutzverletzungen erkannt und unverzüglich gemeldet werden?			Halbjährliche Unterweisung aller Beschäftigten, die Zugang zur Verarbeitung von Personenbezogenen Daten haben und ggf. Selbstanzeige von möglichen Vorfällen beim ULD - Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. Datenschutzbeauftragter ist extern bestellt.
Gibt es einen Prozess zur Durchführung von Datenschutzfolgeabschätzungen?	X		
Wie wird sichergestellt, dass Anfragen von Betroffenen fristgemäß bearbeitet werden?	X		Prozessbeschreibung im DSMS.
Gibt es ein Verzeichnis für Verarbeitungstätigkeiten gem. Art. 30 Abs. 1 und 2 DSGVO?	X		
Welche Maßnahmen sind ansonsten getroffen worden, um die Umsetzung der Vorgaben der DSGVO im Unternehmen zu gewährleisten?	X		Einsatz eines externen DSB; Kontinuierlicher Verbesserungsprozess im Rahmen des DSMS.
Ist ein Datenschutzmanagementsystem (DSMS) implementiert worden?	X		
Sonstiges:			

Anlage 2 zum AVV - Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer).

Es handelt sich um nachfolgende Unternehmen:

- SPEL Stripe Payments Europe, Limite
- ERPnext von Frappe Technologies Pvt. Ltd in der Frappe Cloud
- Microsoft Corporation
- Smart Data Center GmbH
- Smart Cyber Security GmbH - in ihrem Verhältnis zum gewerblichen Endkunden
- AuA24 Kundenbetreuungsgesellschaft mbH