VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

VEREINBARUNG ZUR
AUFTRAGSVERARBEITUNG

eyepin GmbH

- im Folgenden „Auftragnehmer“ - genannt
als „Auftragsverarbeiter“ gemäß DSGVO

und

–„Auftraggeber“
als „Verantwortlicher“ gemäß DSGVO

Präambel

Diese Vereinbarung dient als Ergänzung und konkretisiert die Verpflichtungen der Vertragspartner zum Datenschutz für alle bestehenden und zukünftigen rechtswirksamen Verträge, Master Level Agreements, Service Level Agreements, Leistungsbeschreibungen etc. (im Folgenden zusammengefasst als „Vertrag“ oder „Verträge“ bezeichnet) zwischen dem Auftraggeber und dem Auftragnehmer. Sie findet Anwendung auf alle Tätigkeiten, die mit den Verträgen zwischen Auftraggeber und Auftragnehmer in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (im Folgenden „Daten“ genannt) des Auftraggebers als Verantwortlichen im Auftrag verarbeiten. Im Übrigen gelten für dieses Dokument alle Bestimmungen und Begriffe der EU-Datenschutzgrundverordnung (DSGVO).

1 Gegenstand, Ort und Dauer der Auftragsverarbeitung

1.1 Aus den Verträgen zwischen den Parteien ergeben sich jeweils detailliert Gegenstand und Dauer des Auftrags, Art und Zweck sowie Ort der Verarbeitung und gegebenenfalls die verarbeiteten Datenkategorien sowie die Kategorien der betroffenen Personen. Unter Anwendung der DSGVO obliegt es dem Auftraggeber als Verantwortlichen, ein Verzeichnis von Verarbeitungstätigkeiten nach Art 30 Abs 1 DSGVO zu führen. Diese Verpflichtung entfällt, wenn für den Auftraggeber die Ausnahmeregelung nach Art 30 Abs 5 DSGVO zutrifft. Davon unberührt obliegt es dem Auftragnehmer als Auftragsverarbeiter nach Art 30 Abs 2 DSGVO, ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung zu führen, welche sich aus dem Kontext der Verträge ergeben.

1.2 Über den Ort der Verarbeitung unter Berücksichtigung des Kapitels V DSGVO entscheidet ausschließlich der Auftraggeber als Verantwortlicher. Er weist den Auftragnehmer vertraglich oder mittels Weisung entsprechend an, die Verarbeitung entweder ausschließlich innerhalb der EU bzw. des EWR durchzuführen oder diese teilweise oder zur Gänze unter Berücksichtigung der dafür anwendbaren Rechtsgrundlagen auch in vom Auftraggeber zu benennenden Drittländern oder an bestimmten vom Auftraggeber zu benennenden spezifischen Standorten durchzuführen.

1.3 Die Laufzeit der Auftragsverarbeitung richtet sich nach der Laufzeit der Verträge und den darin vereinbarten Bestimmungen zwischen Auftraggeber und Auftragnehmer, sofern sich aus den Bestimmungen dieser Vereinbarung oder aufgrund gesetzlicher Bestimmungen nicht darüberhinausgehende Verpflichtungen ergeben.

2 Anwendungsbereich und Verantwortlichkeit

2.1 Der Auftragnehmer verarbeitet Daten im Auftrag des Auftraggebers. Dies umfasst jene Tätigkeiten, die in den Verträgen konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Verträge für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Verarbeitung an sich sowie der Datenweitergabe an den Auftragnehmer als Auftragsverarbeiter allein verantwortlich („Verantwortlicher“ im Sinne des Art 4 Nr. 7 DSGVO).

2.2 Die Weisungen des Auftraggebers werden durch die Verträge festgelegt und können vom Auftraggeber in schriftlicher Form (auch elektronische Textform) an Auftragnehmer durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisungen). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Etwaige mündliche Weisungen sind unverzüglich schriftlich bzw. in Textform zu bestätigen.

3 Pflichten des Auftragnehmers als Auftragsverarbeiter nach DSGVO

3.1 Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse nur im Rahmen des Auftrages gemäß Vertrag und der Weisungen des Auftraggebers zu verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Art 28 Abs 3 lit a DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung dieser

Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

3.2 Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit, insbesondere auch zur Wahrung des Datengeheimnisses. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit dem Datenverkehr beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht. Die Verpflichtung zur Verschwiegenheit ist auch für Daten von juristischen Personen und handelsrechtlichen Personengesellschaften einzuhalten.

3.3 Der Auftragnehmer hat in seinem Verantwortungsbereich die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragnehmer trifft technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers, die den Anforderungen des Art 32 DSGVO genügen. Der Auftragnehmer trifft hierbei insbesondere Maßnahmen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

3.4 Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer ohne gesonderte Ankündigung dann vorbehalten, wenn das vertraglich vereinbarte Schutzniveau dadurch nicht unterschritten wird und sie nicht der DSGVO widersprechen. Im Standardfall handelt es sich dabei um Verbesserungen der Datensicherheit durch Maßnahmen im Sinne von Informationssicherheit, Datenschutz und Qualitätsmanagement.

3.5 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Rechte der betroffenen Personen nach Kapitel III DSGVO. Darüberhinausgehend unterstützt der Auftragnehmer auf Wunsch den Auftraggeber bei der Einhaltung der in Art 33 bis 36 DSGVO genannten Pflichten des Auftraggebers, wobei der Auftragnehmer hierbei berechtigt ist, den entstandenen Aufwand dem Auftraggeber nach vorheriger Ankündigung in Rechnung zu stellen.

3.6 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes der Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten (entsprechend der Weisung durch den Auftraggeber) zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

3.7 Allgemeine Datenschutzfragen des Auftraggebers können jederzeit an die explizit hierfür eingerichtete Stelle des Auftragnehmers per E- Mail an dataprotection-officer@eyepin.com gestellt werden. Unabhängig von gesetzlichen Erfordernissen hat der Auftragnehmer für alle verbundenen Gesellschaften einen gemeinsamen Datenschutzbeauftragten (DSB) benannt, der die Einhaltung der datenschutzrechtlichen Vorschriften beim Auftragnehmer überwacht und für den Auftraggeber als Hauptansprechpartner zu Datenschutzfragen im Zuge der Vertragserfüllung fungiert. Name und Kontaktdaten des DSB des Auftragnehmers werden jeweils aktuell auf der Unternehmenshomepage veröffentlicht. Zum Zeitpunkt des Abschlusses der gegenständlichen Vereinbarung benannter Datenschutzbeauftragter des Auftragnehmers sowie seiner verbundenen Tochterunternehmen ist:

Thomas Sillipp
dataprotection-officer@eyepin.com

Tel. Deutschland/International: +49 30 1388 288-401
Tel. Österreich: +43 1 961 7777-401

3.8 Der Auftragnehmer verpflichtet sich zur Sicherheit der Verarbeitung nach Art 32 Abs 1 lit a bis c DSGVO als Auftragsverarbeiter unter Berücksichtigung der Machbarkeit im Rahmen der gültigen Verträge mit dem Auftraggeber und gewährleistet nach Art 32 Abs 1 lit d DSGVO ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen einzusetzen. Einzelheiten zu den vom Auftragnehmer nach Art 32 DSGVO getroffenen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sind im ANHANG 1 angeführt.

3.9 Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelweisung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht anders im Vertrag vereinbart. Der Auftragnehmer ist hierbei berechtigt, dem Auftraggeber den entstandenen Aufwand nach vorheriger Ankündigung in Rechnung zu stellen. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht bereits im Vertrag geregelt.

3.10 Daten, Datenträger sowie sämtliche sonstige Materialien werden vom Auftragnehmer nach Vertragsende auf Verlangen des Auftraggebers entweder herausgegeben oder gelöscht. In den automatischen Datenbackups des Auftragnehmers enthaltene Daten des Auftraggebers werden organisch über die laufenden Backup-Zyklen aus den Datenbackups des Auftragnehmers gelöscht. Im Falle von Test- und Ausschussmaterialien ist eine Einzelweisung für die Löschung nicht erforderlich. Entstehen zusätzliche Kosten durch vom Auftraggeber abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

3.11 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art 82 DSGVO, verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr des Anspruches im Rahmen ihrer Möglichkeiten zu unterstützen.

4 Pflichten des Auftraggebers als Verantwortlicher nach DSGVO

4.1 Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Verarbeitung an sich sowie der Datenweitergabe an Auftragnehmer als Auftragsverarbeiter allein verantwortlich („Verantwortlicher“ im Sinne des Art 4 Punkt 7 DSGVO).

4.2 Der Auftraggeber als Verantwortlicher stellt sicher, dass die Verarbeitung gemäß den Grundsätzen nach Kapitel II DSGVO erfolgt und die von Auftragnehmer als Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen (gem. ANHANG 1) unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die

Rechte und Freiheiten natürlicher Personen entsprechend DSGVO angemessen sind.

4.3 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

4.4 Dem Auftraggeber sind die in ANHANG 1 dieser Vereinbarung angeführten technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese und jene in den Verträgen gegebenenfalls darüberhinausgehend festgelegten Maßnahmen für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

4.5 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art 82 DSGVO gilt Punkt 3.11 sinngemäß.

5 Anfragen betroffener Personen

5.1 Wendet sich eine betroffene Person mit Forderungen nach Kapitel III DSGVO (z.B. Berichtigung, Löschung oder Auskunft) an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung zum Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten und auf Weisung des Auftraggebers, soweit dies in den Verträgen nicht anders vereinbart ist.

5.2 Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

6 Nachweismöglichkeiten

6.1 Der Auftragnehmer weist bei Bedarf gegenüber dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach.

6.2 Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten vom Auftragnehmer ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit von mindestens zwei Wochen durchgeführt. Der Auftragnehmer darf diese Inspektionen von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich firmeninterner Informationen des Auftragnehmers, der Daten anderer Kunden des Auftragnehmers und der eingerichteten technischen und organisatorischen Maßnahmen, abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zum Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Der Auftraggeber stimmt dann der Benennung eines unabhängigen externen Prüfers durch den

Auftragnehmer zu, sofern der Auftragnehmer eine Kopie des Auditberichts zur Verfügung stellt.

6.3 Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der nicht vergütungspflichtige Aufwand von Inspektionen ist für den Auftragnehmer grundsätzlich auf einen Personentag pro Kalenderjahr begrenzt, sofern in den Verträgen nicht gesondert geregelt.

6.4 Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt Punkt 6.2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

7 Weitere Auftragsverarbeiter

7.1 Der Auftraggeber erteilt seine Zustimmung zur Verarbeitung der Daten durch verbundene Unternehmen des Auftragnehmers als weitere Auftragsverarbeiter, soweit dies für die Leistungserbringung gemäß Verträgen erforderlich ist. Der Auftragnehmer verpflichtet sich hierbei zur Überbindung der gesetzlichen und vertraglichen Datenschutzverpflichtungen an diese weiteren Auftragsverarbeiter und hat hierfür „Corporate Rules“ in Form einer Rahmenvereinbarung zur Auftragsverarbeitung als verbindliches Rechtsinstrument innerhalb der Auftragnehmer-Unternehmensgruppe etabliert. Eine Auflistung dieser verbundenen Unternehmen im obenstehenden Sinn ist im ANHANG 2 angeführt.

7.2 Der Einsatz von Subunternehmern als weitere Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher schriftlich zugestimmt hat. Die Regelung zu Subunternehmern in Angeboten oder Verträgen zwischen Auftraggeber und Auftragnehmer gilt vorrangig zu dieser Regelung und entspricht einer solchen schriftlichen Zustimmung des Auftraggebers. Der Auftragnehmer bedient sich Subunternehmen im Bereich Serverhosting und Rechenzentrums-Dienstleistungen. Diese Unternehmen sind in ANHANG 2 als Subunternehmen aufgelistet und bedürfen keiner zusätzlichen Zustimmung durch den Auftraggeber.

7.3 Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der in den Verträgen zwischen Auftraggeber und Auftragnehmer vereinbarten Leistung beauftragt, sofern diese als weitere Auftragsverarbeiter fungieren und eine Zustimmung nicht bereits aus den Verträgen zwischen Auftraggeber und Auftragnehmer hervorgeht.

7.4 Erteilt der Auftragnehmer nach erfolgter schriftlicher Zustimmung des Auftraggebers Aufträge an Subunternehmen, so obliegt es dem Auftragnehmer, die gesetzlichen und vertraglichen Datenschutzverpflichtungen, denen der Auftragnehmer gegenüber dem Auftraggeber unterliegt, an diese weiteren Auftragsverarbeiter zu überbinden.

7.5 Eine Auflistung der Subunternehmen, die als zustimmungspflichtige weitere Auftragsverarbeiter in Erscheinung treten ist in ANHANG 2 angeführt.

8 Informationspflichten, Schriftformklausel und Rechtswahl

8.1 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Agierenden unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DSGVO liegen.

8.2 Änderungen und Ergänzungen dieses Dokuments und all seiner Bestandteile – einschließlich etwaiger Zusicherungen von Seiten des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf das schriftliche Formerfordernis.

8.3 Bei etwaigen Widersprüchen gehen Regelungen dieses Dokuments zum Datenschutz den Regelungen der Verträge vor. Sollten einzelne Teile dieses Dokuments unwirksam sein oder werden, so berührt dies die Wirksamkeit des Dokuments im Übrigen nicht.

9 Haftung und Schadensersatz

Der Auftraggeber und der Auftragnehmer haften gegenüber betroffenen Personen datenschutzrechtlich entsprechend der in Art 82 DSGVO getroffenen Regelung. Weitere Haftungs- und Schadenersatzregelungen werden vorranging in den Angeboten und Verträgen zwischen dem Auftraggeber und Auftragnehmer vereinbart.

10 Vertraulichkeits - und Verschwiegenheitspflicht

Beide Parteien verpflichten sich zur Vertraulichkeit und zur Verschwiegenheit bezüglich der Inhalte dieser Vereinbarung. Davon ausgenommen sind gesetzliche Offenlegungspflichten gegenüber Behörden oder in Gerichts- oder Strafverfahren sowie Personen und Auditoren, die sich zur Vertraulichkeit gegenüber dem Auftraggeber und dem Auftragnehmer vertraglich verpflichten oder einer Verschwiegenheitsverpflichtung gemäß Punkt 6.4 unterliegen.

Anhang 1

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

STAND: 17. Oktober 2018

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Die technischen und organisatorischen Maßnahmen werden vom Auftragnehmer entsprechend Art 32 DSGVO umgesetzt. Sie werden vom Auftragnehmer laufend nach Machbarkeit und Stand der Technik – nicht zuletzt auch im Sinne der aktiven ISO 27001 Zertifizierungen – verbessert und auf ein höheres Sicherheits- und Schutzniveau gebracht.

11 Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren:

- Der Auftragnehmer betreibt ein mehrschichtiges Zutrittssystem zu den Datenverarbeitungsanlagen. Sämtliche Mitarbeiter erhalten angepasste Zutrittskarten, die nur für den jeweiligen Bereich gültig sind.
- Zusätzlich sind biometrische Handflächen Scanner im Einsatz
- Der Zutritt zu den Schrankanlagen ist nur mittels eigener Schlüssel möglich.
- Die gesamten Räumlichkeiten des Ortes der Datenverarbeitung (Rechenzentrum) sind flächendeckend durch Überwachungskameras geschützt.

12 Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Zutritt zu den Serversystemen ist nur von definierten Zutrittspunkten möglich. Dies ist nur über die Büroräumlichkeiten des Auftragnehmers bzw. über eine mehrschichtige und verschlüsselte VPN Einwahl durch die Mitarbeiter des Auftraggebers möglich.

- Der Auftraggeber erhält Zugriff zu seinen Systemen auf einem sicheren und verschlüsselten Weg, sofern es in der Leistungsbeschreibung nicht anders definiert wurde. Der Auftraggeber verwaltet seine Zugriffe selbstständig. Die Kontrolle der Server auf Systemebene (root / Administrator Zugriff) erfolgt bevorzugt über Key-Authentifizierung.

- Sollten Passwörter zum Einsatz kommen, so werden diese nach sehr strengen Kriterien generiert (Zahlen, Buchstaben (Klein-/Großschreibung), Sonderzeichen, min. 15 Zeichen lang).

- Der Zugriff der Systeme ist auch lokal im Rechenzentrum möglich.

- Sämtliche Zugriffe auf die Systeme werden protokolliert und auf Wunsch des Auftraggebers auch extern gespeichert.

- Sollte der Auftragnehmer keinen Zugriff auf die Systeme des Auftraggebers

haben (z. B. unmanaged Server), ist der Auftraggeber selbst für die Zugänge verantwortlich.

13 Zugriffskontrolle auf die Datenverarbeitungssysteme

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

- Die Zugriffe der Systeme erfolgt ausschließlich über die definierten Zugriffspunkte vom Auftragnehmer. Sämtliche Zugriffe werden über SSH komplett verschlüsselt. Administrationssystem auf Web-Basis werden bevorzugt mittels zertifizierten SSL verschlüsselt, um die Gegenstelle verifizieren zu können. Sämtliche Zugriffe werden protokolliert und sicher abgelegt. Diese Protokolle sind nur leitenden Angestellten bzw. Geschäftsführern/Vorständen zugänglich. Die Verwaltung der Zugriffe wird durch den Auftragnehmer vorgenommen.

14 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Sämtliche Systeme werden überwacht und laufend protokolliert.

- Leitende Mitarbeiter kontrollieren die Arbeiten sämtlicher Mitarbeiter. Die Arbeiten finden nur auf zertifizierten Systemen des Auftragnehmers statt.

- Alle Zugriffe erfolgen direkt in das Rechenzentrum und von dort aus werden weitere Systeme gesteuert. Es ist nicht möglich anderwärtig auf diese Systeme zuzugreifen.

- Neue Mitarbeiter erhalten betriebsintern nicht-kritische Aufgaben, bei denen es nicht möglich ist, dass kritische Daten von Kunden eingesehen werden können. Erst nach einem gewissen Vertrauensmaß und internen Kenntnisstand erhalten Mitarbeiter Zugriff auf kritische und vertrauliche Systeme.

- Sollte ein Mitarbeiter das Unternehmen verlassen, so werden sämtliche Zugriffe an zentraler Stelle gesperrt.

15 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Sämtliche Systeme werden komplett protokolliert und mittels eigener Speicherung auf externen Systemen gesichert. Auf diese externen Systeme haben ausschließlich leitende Mitarbeiter Zugriff. Die Protokolle werden mindestens drei Monate gespeichert.

16 Auftragskontrolle

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

- Der Auftragnehmer arbeitet ausschließlich mit festangestellten Mitarbeitern. Externe Mitarbeiter kommen aus Qualitäts- und Sicherheits-Gründen nicht in Frage.

17 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind:

- Eine hochverfügbare Stromversorgung wird durch eine hohe Batterielaufzeit bzw. Diesel-Aggregat gesichert. Server mit mindestens zwei Netzteilen werden an unterschiedliche Notstrom-Anlagen und zusätzlich an unterschiedliche Strom-Absicherungen geschaltet. Somit führen Ausfälle von einzelnen Stromkreisen nicht zum Ausfall entsprechend ausgestatteter Systeme.

- Klimaanlage, Netzwerk sowie Storage-Systeme sind redundant bzw. n+1 ausgelegt

- Datensicherungen werden bevorzugt, aber auf Wunsch des Auftraggebers in ein örtlich getrenntes Rechenzentrum vom Auftragnehmer gesichert. Somit sind die Daten des Auftraggebers bei einer eventuell eintretenden Katastrophe komplett verfügbar.

- Die Datensicherung der Systeme wird entsprechend den Vorgaben und Abstimmungen mit dem Team vom Auftragnehmer und dem Team des Auftraggebers eingerichtet.

- Backup-Daten werden auf spindelbasierten Systemen (z. B. SATA) im RAID-Verbund gespeichert. Auf Wunsch des Auftraggebers kann eine dedizierte Bandsicherung einrichtet werden.

- Im Rahmen des Auftrags des Auftraggebers an den Auftragnehmer, können sich die technischen Maßnahmen entsprechend anpassen. Ziel hierbei soll es sein, personenbezogene Daten jederzeit entsprechend der Kritikalität der Daten, zu verarbeiten.

18 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Die Daten unterschiedlicher Kunden werden vom Auftragnehmer strikt logisch getrennt, damit die Daten aller Kunden vom Auftragnehmer nicht von anderen Kunden eingesehen werden können.

19 Organisation

Der Auftragnehmer hat eine ausgeprägte Informationssicherheits- und Datenschutz-Querschnittsorganisation etabliert, um einen umfassenden Schutz ihrer eigenen Unternehmensinformationen- und Daten sowie der Daten ihrer Kunden und Auftraggeber zu schützen. Dabei sind einerseits die Rollen des Information Security Officers (ISO) und des Datenschutzbeauftragten (DSB) eingerichtet und andererseits ein umfassendes Regelwerk aus internen Verfahrensanweisungen und Regelungen aus dem Informationssicherheitsmanagement (z. B. allgemeine Benutzerrichtlinie, Patchmanagement, Richtlinie für IT-Administratoren etc.) sowie eine explizite Datenschutzrichtlinie festgelegt, die für alle Mitarbeiter verbindlich einzuhalten ist und einen sicheren und DSGVO-konformen Umgang mit Informationen und Daten festlegt. Alle Mitarbeiter sind zur verbindlichen Einhaltung dieser Regelungen verpflichtet und werden laufend vom DSB auf dem Gebiet des Datenschutzes informiert und geschult.

Anhang 2

WEITERE AUFTRAGSVERARBEITER

STAND: 16. Mai 2018

WEITERE AUFTRAGSVERARBEITER

Weitere Auftragsverarbeiter (verbundene Unternehmen) im Geltungsbereich der eyepin
„Corporate Rules“ in Form einer Rahmenvereinbarung zur Auftragsverarbeitung als verbindliches Rechtsinstrument innerhalb der eyepin - Unternehmensgruppe:

- eyepin GmbH, Berlin, Deutschland
- eyepin GmbH, Wien, Österreich

20 Als sonstige weitere Auftragsverarbeiter (Subunternehmen) im Bereich Hosting und Rechenzentrum kommen zum Einsatz:

- ANX Holding GmbH, Klagenfurt, Österreich
- ANEXIA Internetdienstleistungs GmbH, Klagenfurt, Österreich
- ANEXIA Deutschland GmbH, München, Deutschland
- DATASIX Rechenzentrumsbetriebs GmbH, Wien, Österreich