42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln

+49 221 - 291997 86
crm@42he.com

Auftragsverarbeitungsvereinbarung (AVV)

zwischen

SpotVision GmbH
Flurweg 2
82024 Taufkirchen
Taufkirchen

Kundennummer: SPO08242
(nachfolgend „Auftraggeber“ genannt) und der

42he GmbH, Marktstr. 10, Gebäude E8, 50968 Köln

(nachfolgend „Auftragnehmer“ genannt)
- beide Vertragsparteien nachfolgend auch einzeln Partei und gemeinsam Parteien genannt -

Vorbemerkung und Feststellungen (V)

Zwischen den Parteien wurde ein Vertrag (nachfolgend „der VERTRAG“ oder „der zugrundeliegende Vertrag“) geschlossen, auf dessen Basis der Auftragnehmer als Verarbeiter im Sinne der EU-Datenschutzgrundverordnung (DSGVO) für den Auftraggeber tätig werden soll. Dieser Vertrag liegt mit folgenden Spezifikationen der vorliegenden Auftragsverarbeitungsvereinbarung zugrunde (V(1) bis V(4)):

(1) Zugrundeliegender Vertrag: Vertrag über die Nutzung der Anwendung CentralStationCRM auf Grundlage der jeweils gültigen Allgemeinen Geschäftsbedingungen von 42he
(2) Datum des Vertragsschlusses: 22.05.2018
(3) Gegenstand des Auftrags: Anlage 1
(4) Dauer des Auftrags: wie zugrundeliegender Vertrag über die Nutzung von CentralStationCRM

Es werden zudem folgende Festlegungen zwischen den Parteien getroffen (V(5) bis V(8)):
(5) Zugelassene/r Subauftragnehmer von Auftragnehmer: siehe Anlage 3
(6) Empfangsberechtigter zu Weisungen: siehe Anlage 4
(7) Stellvertretender Empfangsberechtigter: siehe Anlage 4
(8) Löschkonzept, Recht auf Vergessenwerden, Möglichkeiten und Umsetzung von Berichtigungen und Datenportabilität sind durch den Auftraggeber sicher zu stellen, Ziffer 7.2, sofern dies zwischen den Parteien im zugrundeliegenden Vertrag nicht ausdrücklich abweichend geregelt wurde.
Zur Erfüllung von im zugrundeliegenden Vertrag übernommenen Leistungspflichten wird der

Sitz der Gesellschaft: Köln
Amtsgericht Köln, HRB 70598
UST-ID NR: DE274568548

Bankverbindung:
Sparkasse KölnBonn
IBAN: DE60 3705 0198 1929 7712 67
BIC: COLSDE33XXX
Gläubiger ID: DE23ZZZ00000112172

Geschäftsführung:
Axel von Leitner

42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln

+49 221 - 291997 86
crm@42he.com

Auftragnehmer im Auftrag des Auftraggebers personenbezogene Daten erheben, verarbeiten und/oder nutzen.
Hierzu treffen die Parteien was folgende Vereinbarung (nachfolgend „AUFTRAG“):

1. Gegenstand und Dauer des Auftrags

1.1 Der Auftragnehmer wird im Rahmen der Erfüllung der im Vertrag übernommenen Leistungspflichten im Auftrag des Auftraggebers personenbezogene Daten (Auftragsdaten) verarbeiten (§ 28 DSGVO).

1.2 Die Laufzeit des Auftrags richtet sich nach der Dauer des zugrundliegenden Vertrags, sofern in der Vorbemerkung oben keine abweichende Regelung getroffen wurde. Die Regelungen zur ordentlichen Kündigung des Hauptvertrags gelten entsprechend. Wird der Vertrag durch den Auftraggeber ordentlich gekündigt, so gilt diese Kündigung – sofern durch den Auftraggeber nicht ausdrücklich eine andere Vorgehensweise formuliert wird – zugleich als ordentliche Kündigung dieses Auftrags.

1.3 Der Auftraggeber ist zu einer jederzeitigen außerordentlichen Kündigung dieses Auftrags bei Vorliegen eines diese Kündigung rechtfertigenden wichtigen Grundes berechtigt.

2. Konkretisierung des Auftragsinhalts, Art. 28 Abs. 3 S. 1

2.1 Der Auftraggeber ist – jedenfalls im Verhältnis zum Auftragnehmer - Inhaber aller etwaigen Rechte, die die Daten betreffen.

2.2 Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret und abschließend beschrieben in der Anlage 1 Nr. 1 „Art und Zweck der Verarbeitung“.

2.3 Die Art der verwendeten personenbezogenen Daten ist festgelegt in Anlage 1 Nr. 2 „Art der Daten“.

2.4 Die Kategorien der betroffenen Personen sind in Anlage 1 Nr. 3 „Kategorien der betroffenen Personen“ aufgeführt.

2.5 Die Verarbeitung der Auftragsdaten findet ausschließlich im Gebiet der Europäischen Union bzw. in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Der Auftragnehmer stellt im Falle einer Verlagerung der Verarbeitung in ein Drittland ein angemessenes Schutzniveau sicher und garantiert dieses gegenüber dem Auftraggeber.

Sitz der Gesellschaft: Köln
Amtsgericht Köln, HRB 70598
UST-ID NR: DE274568548

Bankverbindung:
Sparkasse KölnBonn
IBAN: DE60 3705 0198 1929 7712 67
BIC: COLSDE33XXX
Gläubiger ID: DE23ZZZ00000112172

Geschäftsführung:
Axel von Leitner

42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln

+49 221 - 291997 86
crm@42he.com

3. Weisungen des Auftraggebers

3.1 Weisungen des Auftraggebers haben ausschließlich über die Oberfläche der Anwendung zu erfolgen.

3.2 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diese Vereinbarung, den zugrundeliegenden Vertrag oder einschlägige datenschutzrechtliche oder andere gesetzliche Bestimmungen verstößt, teilt er dem Auftraggeber dies unverzüglich elektronisch mit. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

3.3 Führen Weisungen des Auftraggebers dazu, dass bei dem Auftragnehmer Kosten entstehen, etwa durch Einbindung des Datenschutzbeauftragten, eines Rechtsanwalts oder sonstige Kosten, so hat diese der Auftraggeber zu tragen.

3.4 Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

3.5 Soweit von 42he vorgesehen, sind die weisungsberechtigten Personen des Auftraggebers in der entsprechend von 42he zur Verfügung gestellten Form (z.B. in der Anwendung) vom Auftraggeber zu benennen.

4. Pflichten des Auftraggebers

4.1 Der Auftraggeber bleibt verantwortliche Stelle im datenschutzrechtlichen Sinn. Er ist für die Rechtmäßigkeit der auftragsgemäßen Verarbeitung der Auftragsdaten verantwortlich.

4.2 Etwaige Fehler oder Unregelmäßigkeiten im Rahmen der Verarbeitung der Auftragsdaten durch den Auftragnehmer teilt der Auftraggeber jeweils unverzüglich elektronisch mit.

5. Pflichten des Auftragnehmers

5.1 Der Auftragnehmer wird die Auftragsdaten ausschließlich entsprechend den Weisungen des Auftraggebers, dieses Auftrags, des zugrundeliegenden Vertrags sowie den einschlägigen datenschutzrechtlichen Bestimmungen verarbeiten. Jedwede andere Verwendung bedarf der vorherigen elektronischen Zustimmung des Auftraggebers.

5.2 Der Auftragnehmer wird die ihm überlassenen Daten ohne vorherige Zustimmung des Auftraggebers

Sitz der Gesellschaft: Köln
Amtsgericht Köln, HRB 70598
UST-ID NR: DE274568548

Bankverbindung:
Sparkasse KölnBonn
IBAN: DE60 3705 0198 1929 7712 67
BIC: COLSDE33XXX
Gläubiger ID: DE23ZZZ00000112172

Geschäftsführung:
Axel von Leitner

42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln

+49 221 - 291997 86
crm@42he.com

nicht vervielfältigen. Ausgenommen sind die für die Erfüllung der übernommenen Leistungspflichten erforderlichen Vervielfältigungen, z.B. zu Zwecken der Datensicherung.

5.3 Der Auftragnehmer ist verpflichtet, den Auftraggeber über Verletzungen der einschlägigen datenschutzrechtlichen Vorschriften oder der Bestimmungen dieser Vereinbarung unverzüglich elektronisch zu unterrichten. Soweit den Auftraggeber aufgrund einer solchen Verletzung Pflichten nach der DSGVO treffen, hat der Auftragnehmer den Auftraggeber hierbei im Rahmen des Erforderlichen zu unterstützen.

5.4 Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in dieser Vereinbarung eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Der Auftragnehmer gewährleistet, dass mit der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer nur Personen betraut werden, die sich entsprechend zur Vertraulichkeit verpflichtet haben oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

5.5 Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen der Aufsichtsbehörden, soweit sich diese auf diesen Auftrag und/ oder die im Auftrag verarbeiteten Daten des Auftraggebers beziehen.

6. Allgemeine Organisationspflichten, technische und organisatorische Maßnahmen

6.1 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. Dieser Verpflichtung kommt der Auftragnehmer durch Umsetzung der in Anlage 2 zu diesem Auftrag aufgeführten technisch-organisatorischen Maßnahmen (TOM) nach.

6.2 Der Auftragnehmer hat die Umsetzung der in dem TOM aufgeführten technischen und organisatorischen Maßnahmen und deren Eignung zur Erfüllung der gesetzlichen Verpflichtung regelmäßig zu prüfen und zu dokumentieren. Die Dokumentation hat durch den Datenschutzbeauftragten des Auftragnehmers oder eine sonstige unabhängige Stelle zu erfolgen und inhaltlich Bezug auf durch

Sitz der Gesellschaft: Köln
Amtsgericht Köln, HRB 70598
UST-ID NR: DE274568548

Bankverbindung:
Sparkasse KölnBonn
IBAN: DE60 3705 0198 1929 7712 67
BIC: COLSDE33XXX
Gläubiger ID: DE23ZZZ00000112172

Geschäftsführung:
Axel von Leitner

42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln

+49 221 - 291997 86
crm@42he.com

den Auftragnehmer vorgenommene Auftragsverarbeitungen zu nehmen. Auf Anfrage des Auftraggebers wird der Auftragnehmer die jeweils aktuelle Dokumentation dem Auftraggeber zur Verfügung stellen.

6.3 Die in den TOM aufgeführten Maßnahmen sind Grundlage des Auftrags.

6.4 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in der Anlage 2 festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

7. Berichtigung, Löschung und Sperrung von Daten – Rechte der Betroffenen

7.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

7.2 Soweit nicht ausdrücklich anders vereinbart, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers und auf dessen Kosten durch den Auftragnehmer sicherzustellen.

8. Berechtigung zur Begründung von Unterauftragsverhältnissen

8.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen, in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

8.2 Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher elektronischer oder schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

8.3 Der Auftraggeber stimmt hiermit der Begründung der Unterauftragsverhältnisse gemäß Anlage 3 im

Sitz der Gesellschaft: Köln
Amtsgericht Köln, HRB 70598
UST-ID NR: DE274568548

Bankverbindung:
Sparkasse KölnBonn
IBAN: DE60 3705 0198 1929 7712 67
BIC: COLSDE33XXX
Gläubiger ID: DE23ZZZ00000112172

Geschäftsführung:
Axel von Leitner

42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln

+49 221 - 291997 86
crm@42he.com

Sinne von Ziffer 8.2 zu.

8.4 Der Auftragnehmer ist verpflichtet, Unterauftragnehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einbindung von Unterauftragnehmern diese entsprechend der Regelungen dieser Vereinbarung zu verpflichten und sicherzustellen, dass der Auftraggeber die Rechte aus dieser Vereinbarung (insbesondere Prüf- und Kontrollrechte) direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

8.5 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

8.6 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU / des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Diese Verarbeitung von Daten im Auftrag bedarf zudem einer gesonderten Zustimmung in Textform.

9. Kontrollrechte des Auftraggebers

9.1 Dem Auftraggeber ist bekannt, dass der Auftragnehmer für zahlreiche Auftraggeber als Auftragsverarbeiter tätig ist und ein ständiges Durchführen von Kontrollen die Arbeitsabläufe des Auftragnehmers erheblich erschweren kann. Es besteht seitens beider Parteien vor diesem Hintergrund ein erhebliches Interesse daran, die Zahl der notwendigen Kontrollen im Hause des Auftragnehmers möglichst gering zu halten.

9.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann nach Wahl des Auftragnehmers erfolgen durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren).

9.3 Der Auftraggeber ist berechtigt, die Einhaltung der Vorgaben dieses Vertrags durch den Auftragnehmer nach vorheriger angemessener Ankündigung zu prüfen. Hierzu kann der Auftraggeber sich auch eines zur Berufsverschwiegenheit verpflichteten oder gegenüber dem Auftraggeber über eine entsprechende Vereinbarung zur Verschwiegenheit verpflichteten Dritten bedienen, der zum Auditieren der datenschutzrechtlichen Vorgaben geeignet ist. Der Auftragnehmer wird den Auftraggeber bei den

Sitz der Gesellschaft: Köln
Amtsgericht Köln, HRB 70598
UST-ID NR: DE274568548

Bankverbindung:
Sparkasse KölnBonn
IBAN: DE60 3705 0198 1929 7712 67
BIC: COLSDE33XXX
Gläubiger ID: DE23ZZZ00000112172

Geschäftsführung:
Axel von Leitner

42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln

+49 221 - 291997 86
crm@42he.com

Prüfungen unterstützen und ihm auf Anforderung alle erforderlichen Auskünfte erteilen. Der Auftraggeber ist maximal einmal jährlich zu einer entsprechenden Prüfung berechtigt und hat zur Planung seitens des Auftragnehmers den Prüftermin möglichst langfristig vorab mitzuteilen, mindestens mit einer Frist von einem Monat. Weitere Kontrollen sind innerhalb einer Zeitspanne von 12 Monaten nur dann möglich, wenn seitens des Auftraggebers hierzu ein diese zusätzliche/n Kontrolle/n rechtfertigender wichtiger Grund besteht. Jede Kontrolle bei dem Auftragnehmer wird seitens des Auftragnehmers durch eine fachkundige Person – fachkundiger Mitarbeiter, Datenschutzbeauftragter o.ä. nach Ermessen des Auftragnehmers - pro kontrollierender Person seitens des Auftraggebers, begleitet.

9.4 Lässt der Auftraggeber durch oder begleitet durch eine fachkundige Person (internen oder externen Datenschutzbeauftragter, Wirtschaftsprüfer o.ä.) eine Kontrolle im Sinne von Ziffer 9.2 bei dem Auftragnehmer durchführen, ist der Auftraggeber verpflichtet, auf seine Kosten durch diesen unabhängigen Dritten ein Protokoll dieser Kontrolle erstellen zu lassen (nachfolgend „Prüfprotokoll“). Der Auftraggeber wird das durch diese fachkundige Person erstellte Prüfprotokoll dem Auftragnehmer als gut lesbare und einsetzbare digitale Datei unverzüglich nach Erstellung zur freien Verwendung zur Verfügung stellen. Der Auftragnehmer ist insbesondere berechtigt, diese Datei nach Schwärzung des Namens des Auftraggebers und – sofern der Ersteller der interne Datenschutzbeauftragte des Auftraggebers ist – des Erstellernamens Dritten / anderen Auftraggebern zu übermitteln und so die Ordnungsgemäßheit der Datenverarbeitung bei dem Auftragnehmer diesen gegenüber zu dokumentieren.

9.5 Fragt der Auftraggeber einen Termin für eine Kontrolle im Sinne von Ziffer 9.2 bei dem Auftragnehmer an, kann der Auftragnehmer eine Kontrolle abwenden, indem er dem Auftraggeber ein aktuelles – maximal 12 Monate altes – Prüfprotokoll elektronisch zur Verfügung stellt, das eine fachkundige Person für einen anderen Auftraggeber oder für den Auftragnehmer bei dem Auftragnehmer erstellt hat. Zugleich hat der Auftragnehmer dann dem Auftraggeber zu versichern, dass das übermittelte Protokoll die aktuelle Situation bei dem Auftragnehmer weiterhin richtig wiedergibt und kein jüngeres Protokoll vorliegt, das die Verhältnisse bei dem Auftragnehmer als nicht datenschutzkonform oder kritisch bewertet. Dieser Substituierung einer unmittelbaren Überprüfung durch den Auftraggeber kann der Auftraggeber entgegenhalten, dass er aufgrund eines berechtigten und nachweisbaren Interesses – was in der Anforderung so zu nennen ist – trotz vorgelegter Prüfberichte eine Kontrolle durchführen muss. Macht der Auftraggeber von diesem Recht Gebrauch, ist er verpflichtet, die Kontrolle an einem abgestimmten Termin nicht selber durchzuführen, sondern eine fachkundige Person damit zu betrauen und diese zudem mit der Erstellung eines Prüfprotokolls zu beauftragen.

9.6 Sämtliche bei dem Auftragnehmer im Zusammenhang mit der Durchführung einer oder mehrerer Kontrollen durch den Auftraggeber oder eine durch den Auftraggeber beauftragte fachkundige Person

Sitz der Gesellschaft: Köln
Amtsgericht Köln, HRB 70598
UST-ID NR: DE274568548

Bankverbindung:
Sparkasse KölnBonn
IBAN: DE60 3705 0198 1929 7712 67
BIC: COLSDE33XXX
Gläubiger ID: DE23ZZZ00000112172

Geschäftsführung:
Axel von Leitner

42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln

+49 221 - 291997 86
crm@42he.com

entstehenden Kosten sind durch den Auftraggeber zu erstatten. Erfasst sind hiervon insbesondere die Kosten des die Kontrollen begleitenden Mitarbeiters und / oder Datenschutzbeauftragten von dem Auftragnehmer und eventuelle ergänzende Dienstleistungen wie Kosten von Wirtschaftsprüfer, Rechtsanwalt etc. Der Auftragnehmer kann die Durchführung einer Kontrolle von der Zahlung eines Vorschusses auf die zu erwartenden zu erstattenden Kosten der Kontrolle abhängig machen.

9.7 Werden durch Behörden Kontrollen bei dem Auftragnehmer durchgeführt, die mit der Verarbeitung im Auftrag des Auftraggebers zusammenhängen, so gilt die Bestimmung zur Kostentragung der Ziffer 9.6 entsprechend.

9.8 Jeder, der für den Auftraggeber eine Kontrolle bei dem Auftragnehmer durchführt, hat vorab eine Geheimhaltungsvereinbarung zu unterzeichnen, die zu einer umfassenden Geheimhaltung hinsichtlich aller Details der Sicherungsmaßnahmen sowie sämtlicher Umstände, von denen die kontrollierende Person im Rahmen der Kontrolle mehr oder weniger beiläufig Kenntnis erlangt, gegen Verwirkung einer empfindlichen Vertragsstrafe verpflichtet.

9.9 Bei der Einbindung von Unterauftragnehmern gelten die hier formulierten Bestimmungen entsprechend. Auf Anfrage hat der Auftragnehmer an den Auftraggeber beim Auftragnehmer vorliegende Prüfprotokolle zu dem jeweiligen Unterauftragnehmer elektronisch zur Verfügung zu stellen. Die Kosten sind durch den Auftraggeber zu tragen.

10. Herausgabe- und Löschungspflichten bei Beendigung des Auftrags

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des zugrundeliegenden Vertrags – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, gegen Erstattung der Kosten dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung auf Kosten des Auftraggebers datenschutzgerecht zu vernichten.

10.3 Bei dem Auftragnehmer vorhandene Backups sind im üblichen Turnus zu löschen. Von vorliegenden Backups dürfen bis zu dieser Löschung keine im operativen System gelöschten Daten wieder hergestellt

Sitz der Gesellschaft: Köln
Amtsgericht Köln, HRB 70598
UST-ID NR: DE274568548

Bankverbindung:
Sparkasse KölnBonn
IBAN: DE60 3705 0198 1929 7712 67
BIC: COLSDE33XXX
Gläubiger ID: DE23ZZZ00000112172

Geschäftsführung:
Axel von Leitner

42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln

+49 221 - 291997 86
crm@42he.com

werden. Sollte ein Backup wieder aufgespielt werden müssen, ist der Auftragnehmer verpflichtet, anhand einer gesondert durch den Auftragnehmer zu führenden Löschhistorie Daten, die zuvor aus dem operativen System gelöscht worden waren, umgehend neuerlich vollständig aus dem neu durch Backup aufgespielten System zu löschen.

10.4 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren und dem Auftraggeber auf Verlangen gegen Erstattung damit zusammenhängender Kosten zu übergeben. Der Auftragnehmer kann sie zu seiner Entlastung bei Ende des zugrundeliegenden Vertrags oder dieser Vereinbarung dem Auftraggeber übergeben.

11. Mitteilung bei Datenschutzverstößen

11.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Hierzu gehören u.a.
11.1.1 die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,
11.1.2 die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
11.1.3 die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen,
11.1.4 die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung und
11.1.5 die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

11.2 Für Unterstützungsleistungen, die nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen. Das Vorliegen eines Fehlverhaltens des Auftragnehmers ist im Zweifel durch den Auftraggeber nachzuweisen.

12. Haftung

12.1 Bei Vorsatz oder grober Fahrlässigkeit haftet der Auftragnehmer gegenüber dem Auftraggeber für alle von dem Auftragnehmer sowie dessen gesetzlichen Vertretern oder Erfüllungsgehilfen verursachten Schäden unbeschränkt.

Sitz der Gesellschaft: Köln
Amtsgericht Köln, HRB 70598
UST-ID NR: DE274568548

Bankverbindung:
Sparkasse KölnBonn
IBAN: DE60 3705 0198 1929 7712 67
BIC: COLSDE33XXX
Gläubiger ID: DE23ZZZ00000112172

Geschäftsführung:
Axel von Leitner

42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln

+49 221 - 291997 86
crm@42he.com

12.2 Bei einfacher Fahrlässigkeit haftet der Auftragnehmer nur für Schäden aus der Verletzung des Lebens, des Körpers und der Gesundheit oder einer sog. „Kardinalpflicht“, d.h. einer Vertragspflicht, auf deren Einhaltung der Auftraggeber vertrauen durfte und deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht. Schadenersatzansprüche sind in diesem Fall der Höhe nach auf sog. „vertragstypisch vorhersehbare Schäden“ beschränkt, d.h. solche Schäden, mit deren Entstehung im Rahmen des vorliegenden Vertragsverhältnisses typischerweise gerechnet werden muss.

12.3 Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

12.4 Der Auftraggeber trägt die Beweislast dafür, dass etwaige Schäden nicht auf einem von ihm zu vertretenden Umstand beruhen, soweit die Schadensursache in der Erhebung, Verarbeitung oder Nutzung von Daten nach dieser Vereinbarung besteht.

13. Schlussbestimmungen

13.1 Jede Partei trägt die bei ihr im Zusammenhang mit der Umsetzung dieses Auftrags und der Erfüllung der in diesem Auftrag und der DSGVO aus datenschutzrechtlichen Gesichtspunkten vorzunehmenden Handlungen entstehenden Kosten selber, es sei denn, in dieser Vereinbarung ist eine abweichende Regelung hierzu getroffen.

13.2 Änderungen, Ergänzungen oder eine Aufhebung dieser Vereinbarung bedürfen - soweit hierin nichts anderes bestimmt ist - zu ihrer Rechtswirksamkeit der elektronischen Form oder der Schriftform. Dies gilt auch für eine Aufhebung des vorgenannten Formerfordernisses.

13.3 Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam sein oder werden, wird hierdurch die Wirksamkeit der Vereinbarung im Übrigen nicht berührt. Die Parteien werden die unwirksame Bestimmung durch eine dieser nach Sinn und Zweck möglichst nahekommende wirksame Bestimmung ersetzen. Die vorstehende Regelung gilt im Falle unbeabsichtigter Vertragslücken entsprechend.

13.4 Im Fall von Widersprüchen zwischen dieser Vereinbarung und sonstigen Vereinbarungen zwischen den Parteien mit Bezug zum Datenschutz, insbesondere datenschutzrelevante Regelungen im zugrundeliegenden Vertrag, gehen die Regelungen dieses Auftrags vor.

13.5 Für Streitigkeiten aus oder im Zusammenhang mit diesem Auftrag sind – sofern dies zulässig vereinbart werden kann – die Gerichte am Sitz des Auftraggebers ausschließlich zuständig. Der

Sitz der Gesellschaft: Köln
Amtsgericht Köln, HRB 70598
UST-ID NR: DE274568548

Bankverbindung:
Sparkasse KölnBonn
IBAN: DE60 3705 0198 1929 7712 67
BIC: COLSDE33XXX
Gläubiger ID: DE23ZZZ00000112172

Geschäftsführung:
Axel von Leitner

42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln

+49 221 - 291997 86
crm@42he.com

Auftraggeber hat aber das Recht, den Auftragnehmer auch an dem für dessen Sitz zuständigen Gericht zu verklagen.

13.6 Folgende Anlagen sind diesem Auftrag angefügt und stellen ausdrücklich einen Teil dieses Auftrags dar:

Anlage 1 – Spezifikationen zu dem Vertragsgegenstand – Datenkategorien und Betroffene
Anlage 2 – Technische-Organisatorische Maßnahmen
Anlage 3 – Liste der genehmigten Unterauftragnehmer
Anlage 4 – Liste Berechtigter zum Empfang von Weisungen

Unterschriften

Taufkirchen, den 23.05.2018

Markus Stigler, Geschäftsführer SpotVision GmbH

_____

Auftraggeber

Köln, den 22.05.2018

Axel von Leitner, Geschäftsführer 42he GmbH

_____

Auftragnehmer

Sitz der Gesellschaft: Köln
Amtsgericht Köln, HRB 70598
UST-ID NR: DE274568548

Bankverbindung:
Sparkasse KölnBonn
IBAN: DE60 3705 0198 1929 7712 67
BIC: COLSDE33XXX
Gläubiger ID: DE23ZZZ00000112172

Geschäftsführung:
Axel von Leitner

42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln

+49 221 - 291997 86
crm@42he.com

Anlage 1 - Spezifikationen zum Vertragsgegenstand

1. Art und Zweck der Verarbeitung

Als Auftragnehmer verarbeitet die Firma 42he im Rahmen des Auftrags personenbezogene Daten des Auftraggebers. Der Auftragnehmer stellt dem Auftraggeber eine softwarebasierte Lösung zur Verwaltung von Kunden- und Kontaktdaten zur Verfügung, die der Auftraggeber gegen Zahlung eines monatlichen Entgelts nutzen kann. Die Lösung wird auf einer Plattform/Oberfläche des Auftragnehmers betrieben; der Auftraggeber kann über den Internetbrowser mit E-Mail Adresse und Passwort die für ihn eingerichtete Oberfläche der Lösung aufrufen. Die weiteren Einzelheiten ergeben sich aus den Allgemeinen Geschäftsbedingungen zu CentralStationCRM.

2. Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

Personenstammdaten, Kommunikationsdaten (E-Mail, Telefon, Anschrift) und Vertragsstammdaten

3. Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

Kunden, Mitarbeiter, Lieferanten und Dienstleister

Sitz der Gesellschaft: Köln
Amtsgericht Köln, HRB 70598
UST-ID NR: DE274568548

Bankverbindung:
Sparkasse KölnBonn
IBAN: DE60 3705 0198 1929 7712 67
BIC: COLSDE33XXX
Gläubiger ID: DE23ZZZ00000112172

Geschäftsführung:
Axel von Leitner

42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln

+49 221 - 291997 86
crm@42he.com

Anlage 2 - Technische-Organisatorische Maßnahmen

Der Auftragnehmer setzt die folgenden technischen und organisatorischen Maßnahmen ein:

1. Zutrittskontrolle

Gemeint sind Maßnahmen um zu verhindern, dass Unbefugte Zutritt (räumlich zu verstehen) zu Datenverarbeitungsanlagen erhalten, mit welchen personenbezogene Daten verarbeitet werden.

- Zutrittskontrollsystem
- dokumentierte Schlüsselvergabe
- Schlüsselvergabe/Zutrittsberechtigung nur für berechtigte Personen
- Türsicherung (elektrische Türöffner)
- Überwachungseinrichtung: Video-/Fernsehmonitor
- Server in abschließbaren Serverschränken

2. Zugangskontrolle

Gemeint sind Maßnahmen um zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können.

- Server sind nur nach einem individuellen Login nutzbar
- Clients sind nur nach einem individuellen Login nutzbar
- Server Login mit digitalen Zertifikaten

3. Zugriffskontrolle

Es muss gewährleistet werden, dass die zur Benutzung von DV-Anlagen berechtigten Nutzer ausschließlich auf Inhalte zugreifen können für welche sie berechtigt sind und das personenbezogene Daten bei der Verarbeitung und Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können.

- Anzahl der Administratoren weitgehend reduziert
- zertifikatsbasierte Zugriffsberechtigung

4. Weitergabekontrolle

Es muss verhindert werden, dass personenbezogenen Daten bei der elektronischen Übertragung oder beim Transport oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können und das festgestellt werden kann an welchen Stellen eine Übermittlung solcher Daten im DV-System vorgesehen ist.

- Verschlüsselte Leitungen
- Zugriff von extern nur über verschlüsselte Verbindung
- Elektronische Signatur

Sitz der Gesellschaft: Köln
Amtsgericht Köln, HRB 70598
UST-ID NR: DE274568548

Bankverbindung:
Sparkasse KölnBonn
IBAN: DE60 3705 0198 1929 7712 67
BIC: COLSDE33XXX
Gläubiger ID: DE23ZZZ00000112172

Geschäftsführung:
Axel von Leitner

42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln

+49 221 - 291997 86
crm@42he.com

5. Eingabekontrolle

Es muss sichergestellt werden, dass in gewissem Maße nachträglich überprüft werden kann ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht worden sind. Diese Rolle übernehmen die Verlaufsansichten innerhalb der Software ein.

- Protokollierung
- Benutzeridentifikation
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

6. Auftragskontrolle

Es muss sichergestellt werden, dass personenbezogene Daten die im Auftrag verarbeitet werden, gemäß den Weisungen des Auftraggebers verarbeitet werden. Der Auftrag findet ausschließlich in Form von Eingaben innerhalb der CRM Software statt.

- Eindeutige Vertragsgestaltung, Weisungsbefugnisse festlegen
- Datenschutzvertrag
- Kontrollrechte

7. Verfügbarkeitskontrolle

Es muss sichergestellt werden, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden. Die Zerstörung von personenbezogenen Daten kann im Rahmen der jeweiligen Nutzerrechte über die Nutzeroberfläche durchgeführt werden. Die Verwaltung der Nutzerrechte obligt dem Auftraggeber.

- Backup- und Recovery-Verfahren
- Spiegeln von Festplatten (RAID)
- Einsatz von Unterbrechungsfreier Stromversorgung (USV)
- getrennte Aufbewahrung der Backups

8. Trennungskontrolle

Es ist sicher zu stellen, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden getrennt verarbeitet werden können.

- Interne Mandantenfähigkeit (z.B.: Daten von unterschiedlichen Kunden logisch voneinander getrennt)
- Trennung von Produktiv- und Testsystemen

Sitz der Gesellschaft: Köln
Amtsgericht Köln, HRB 70598
UST-ID NR: DE274568548

Bankverbindung:
Sparkasse KölnBonn
IBAN: DE60 3705 0198 1929 7712 67
BIC: COLSDE33XXX
Gläubiger ID: DE23ZZZ00000112172

Geschäftsführung:
Axel von Leitner

42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln

+49 221 - 291997 86
crm@42he.com

Anlage 3 - Liste der genehmigten Unterauftragnehmer

Für die Erbringung unserer Dienstleistung arbeiten wir mit verschiedenen Unterauftragnehmern zusammen. Für den Betrieb unserer eigenen IT-Infrastruktur nutzen wir die Dienste der Core-Backbone GmbH. Dort werden alle Daten gespeichert außer Dateianhänge (z.B. Word oder PDF-Dokumente). Für die Speicherung von Dateianhängen arbeiten wir mit den Diensten der Telekom Deutschland GmbH sowie mit dem EU-Rechenzentrum der Amazon Web Services, Inc..

Core-Backbone GmbH
Hans-Sachs-Str. 14
93138 Lappersdorf

Telekom Deutschland GmbH
Landgrabenweg 151
53227 Bonn

Amazon Web Services, Inc.
410 Terry Avenue North
Seattle, WA 98109-5210

Anlage 4 – Liste Berechtigter zum Empfang von Weisungen

Jeweils nach Schichtplan zuständige Mitarbeiterin/zuständiger Mitarbeiter im Kundensupport bzw. in der technischen Abteilung.

42he GmbH
Marktstraße 10 - Gebäude E8
50968 Köln
+49 (0)221 - 291997 86
info@42he.com

Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers:
Dennis Busch
stacktrace GmbH
Querstraße 3
96237 Ebersdorf

Sitz der Gesellschaft: Köln
Amtsgericht Köln, HRB 70598
UST-ID NR: DE274568548

Bankverbindung:
Sparkasse KölnBonn
IBAN: DE60 3705 0198 1929 7712 67
BIC: COLSDE33XXX
Gläubiger ID: DE23ZZZ00000112172

Geschäftsführung:
Axel von Leitner