

AUFTRAGSVERARBEITUNGSVERTRAG

Dieser Auftragsverarbeitungsvertrag ("AVV") gilt für die Verarbeitung Personenbezogener Daten von Kunden (wie nachstehend definiert) durch die Vertragsparteien im Zusammenhang mit Produkten und Leistungen (die "**Leistungen**"), die im Rahmen des Vertrags erbracht werden.

1. Definitionen

1.1. In diesem AVV haben in Großbuchstaben geschriebenen Begriffe die folgende Bedeutung:

- (a) „**Vertrag**“ meint den bestehenden Software-Dienstleistungsvertrag, das Bestellformular oder sonstige schriftliche Verträge zwischen Magnet und dem Kunden, gemäß dem Magnet die Leistungen für den Kunden erbringt, einschließlich aller Anhänge, Arbeitsbeschreibungen, Ergänzungen und Änderungen dazu (einschließlich dieses AVV).
- (b) „**Personenbezogene Daten von Kunden**“ meint alle personenbezogenen Daten, die vom Kunden zur Verfügung gestellt und/oder von Magnet im Auftrag des Kunden verarbeitet werden und die im Zusammenhang mit der Erbringung der Leistungen durch Magnet im Rahmen des Vertrages stehen.
- (c) „**Datenschutzgesetze**“ meint alle Datenschutz-, Privatsphäre- oder IT-Sicherheitsgesetze, die auf Magnets Verarbeitung personenbezogener Daten von Kunden im Rahmen des Vertrags Anwendung finden können, einschließlich (a) Bundes- und Landesgesetze und -vorschriften der Vereinigten Staaten, die sich auf die Privatsphäre oder IT-Sicherheit beziehen, wie der *California Consumer Privacy Act* in seiner durch den *California Privacy Rights Act* („**CCPA**“) geänderten Fassung; (b) die Datenschutz-Grundverordnung (EU) 2016/679 „**DS-GVO**“; und (c) die *General Data Protection Regulation* des Vereinigten Königreichs.
- (d) „**Betroffene Person**“ meint eine identifizierte oder identifizierbare natürliche Person, auf die sich die personenbezogenen Daten von Kunden beziehen. Entsprechend der jeweiligen Definition der Datenschutzgesetze bedeutet „Betroffene Person“ auch „Verbraucher.“
- (e) „**Personenbezogene Daten**“ meint alle Informationen, die sich auf eine identifizierte oder identifizierbare lebende Person beziehen, einschließlich aller Informationen, die in den geltenden Datenschutzgesetzen als „personenbezogene Daten“, „persönliche Informationen“ („*personal information*“) oder durch einen entsprechenden Begriff definiert sind.
- (f) „**Unterauftragsverarbeiter**“ meint einen weiteren Auftragsverarbeiter, der von Magnet unterbeauftragte wurde, um Leistungen gegenüber dem Kunden zu erbringen und der dabei Personenbezogene Daten von Kunden im Auftrag von Magnet verarbeitet.
- (g) „**Drittland**“ meint ein Land oder Gebiet, das (a) außerhalb des EWR liegt (für Kunden, die in einem EWR-Mitgliedsland ihren gewöhnlichen Aufenthaltsort haben); oder (b) außerhalb des Vereinigten Königreichs (für Kunden, die im Vereinigten Königreich ihren gewöhnlichen Aufenthaltsort haben).

1.2. Die Begriffe „**Unternehmen**“, „**Verantwortlicher**“, „**internationale Organisation**“, „**verarbeiten**“ (und ihre Ableitungen), „**Auftragsverarbeiter**“, „**verkaufen**“, „**teilen**“ und „**Dienstleister**“ haben jeweils die in den einschlägigen Datenschutzgesetzen definierte Bedeutung.

1.3. Großgeschriebene Begriffe, die in diesem AVV verwendet aber nicht anders definiert werden, haben die im Vertrag festgelegte Bedeutung.

2. Verarbeitung personenbezogener Daten von Kunden

2.1. Sofern im Folgenden nicht anderweitig bestimmt, ist das gemeinsame Verständnis der Parteien, dass der Kunde der Verantwortliche (und das Unternehmen) und Magnet der Auftragsverarbeiter (und Dienstleister) in Bezug auf die Verarbeitung der personenbezogenen Daten von Kunden zur Erbringung der Leistungen ist. **Anhang A** zu diesem AVV legt den Gegenstand und die Dauer der Verarbeitung, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten von Kunden und die Kategorien der betroffenen Personen fest. Der Kunde ist verantwortlich für die Richtigkeit, Qualität und Rechtmäßigkeit der personenbezogenen Daten von Kunden, die er Magnet im Zusammenhang mit den Leistungen zur Verfügung stellt, und für die Zwecke, für die er Personenbezogene Daten von Kunden erhält und verwendet.

- 2.2. Jede Partei wird ihre jeweiligen Verpflichtungen gemäß den geltenden Datenschutzgesetzen einhalten. Der Kunde wird Magnet zusätzlich Vorgaben machen, so dass Personenbezogene Daten von Kunden in Übereinstimmung mit den Datenschutzgesetzen verarbeitet werden.
- 2.3. Der Kunde sichert zu und hat dafür einzustehen, dass (a) er die Leistungen nur so benutzen wird, wie es der Vertrag vorsieht; (b) er dazu berechtigt ist, diesen AVV abzuschließen; und (c) er dazu berechtigt ist und alle erforderlichen gesetzlichen Genehmigungen besitzt, sämtliche Verarbeitungsgeräte, die sich im Besitz, im Gewahrsam oder unter der Kontrolle des Kunden befinden, zu entsperren; auf die Personenbezogenen Daten von Kunden zuzugreifen und sie anderweitig zu verarbeiten, die auf den vorgenannten Verarbeitungsgeräten gespeichert sind oder die auf anderem Wege über diese Verarbeitungsgeräte zugegriffen werden kann; und diese Personenbezogenen Daten des Kunden für die Erbringung der Leistungen im eigenen Namen zur Verfügung zu stellen und Magnet zu gestatten, die vorgenannten Handlungen vorzunehmen. Der Kunde wird keine geltenden Datenschutzgesetze verletzen, indem er rechtswidrig Verarbeitungsgeräte entsperren oder darauf zugreifen wird oder Magnet anweisen wird, rechtswidrig Personenbezogene Daten von Kunden zu verarbeiten. Der Kunde sichert ferner zu und hat dafür einzustehen, dass er alle erforderlichen Erlaubnisse für den Zugriff und die Verarbeitung von Personenbezogenen Daten des Kunden erhalten hat und die Zustimmung erteilt wurde, dass Magnet die Daten sammeln, darauf zugreifen, diese verwenden, speichern, übertragen und anderweitig verarbeiten darf, wie es im Vertrag und in diesem AVV festgelegt ist, insbesondere zur Erfüllung von gerichtlichen Anordnungen, rechtmäßigen behördlichen oder strafverfolgungsbehördlichen Ersuchen oder der Erfüllung rechtmäßiger strafverfolgungsbehördlicher Ermittlungsbefugnisse, jeweils in Bezug auf jede Betroffene Person, auf deren Personenbezogene Daten der Kunde und/oder Magnet in Verbindung mit dem Produkt oder den Leistungen zugreift oder diese anderweitig verarbeitet. Der Kunde wird Magnet auf dessen Verlangen eine schriftliche Bestätigung dieser Zustimmung geben.
- 2.4. Magnet wird Personenbezogene Daten von Kunden nur für die in **Anhang A** angegebenen Zwecke und entsprechend den dokumentierten Anweisungen des Kunden verarbeiten. Der Kunde weist Magnet hiermit an, Personenbezogene Daten von Kunden (a) für die in Anhang A angegebenen Zwecke zu verarbeiten, was insbesondere die Verarbeitung zum Zweck der Erbringung der Leistungen umfasst; (b) entsprechend den Vorgaben der anwendbaren Datenschutzgesetze zu verarbeiten; (c) so anzuzeigen, dass die Einstellungen und Konfigurationen, die vom Kunden oder seinen autorisierten Benutzern innerhalb des Produkts oder der Leistungen angewandt wurden, entsprechend berücksichtigt werden; (d) Unterauftragsverarbeiter nur unter den in diesem AVV bestimmten Voraussetzungen zu beauftragen; und (e) sonstige schriftliche Anweisungen des Kunden schriftlich einzuhalten. Der Kunde ist dafür verantwortlich, dass der Magnet keine Anweisung für ein Tun oder Unterlassen in Bezug auf die Verarbeitung von Personenbezogener Daten von Kunden gibt, die gegen die anwendbaren Datenschutzgesetze verstößt.
- 2.5. Für Personenbezogene Daten von Kunden, die dem CCPA unterliegen, wird Magnet nicht (a) Personenbezogene Daten von Kunden verkaufen oder weitergeben; (b) Personenbezogene Daten von Kunden außerhalb von Magnets direkter Geschäftsbeziehung mit dem Kunden aufbewahren, benutzen oder offenlegen; oder (c) Personenbezogene Daten von Kunden mit personenbezogenen Daten aus anderen Quellen kombinieren. Für den Fall, dass Magnet nach eigener Auffassung nicht in der Lage ist, dass die Anforderungen des CCPA eingehalten werden wird es den Kunden informieren, jede nicht autorisierte Verarbeitung Personenbezogener Daten von Kunden unterlassen und mit dem Kunden zusammenarbeiten, um die nicht autorisierte Verarbeitung Personenbezogener Daten von Kunden zu beheben und die Einhaltung der Anforderungen des CCPA sicherzustellen.

3. **Grenzüberschreitende Übermittlung personenbezogener Daten**

- 3.1. Die Parteien erkennen an und vereinbaren, dass ab Vertragsbeginn Personenbezogene Daten von Kunden aus dem Europäischen Wirtschaftsraum („EWR“) oder dem Vereinigten Königreich („UK“), die von Magnet außerhalb des EWR und/oder UK in ein Drittland oder an eine internationale Organisation übermittelt werden und für die jeweils kein Angemessenheitsbeschluss der Europäischen Kommission besteht, den Standardvertragsklauseln Modul 2 (für Verantwortliche und Auftragsverarbeiter) (*EU Standard Contractual Clauses*, „EU-SCCs“) unterliegen, die hiermit Vertragsinhalt werden.
- a) **Eingeschränkte Übermittlung.** Der Kunde wird als Verantwortlicher und Magnet als Auftragsverarbeiter tätig und dabei Personenbezogene Daten von Kunden nur in einem solchen Umfang verarbeiten, wie es für die im Vertrag genannten Zwecke erforderlich ist wobei das gleiche Schutzniveau, das nach den geltenden Datenschutzgesetzen gilt, eingehalten werden muss. Soweit Magnet im Rahmen des Vertrags Personenbezogene Daten von Kunden verarbeitet, die dem Anwendungsbereich der DS-GVO oder der UK-GDPR unterliegen, unterfällt die Übermittlung den EU-SCCs bzw. dem UK-IDTA (*UK-International Data Transfer Agreement*, „UK-IDTA“), wie in Abschnitt 3(b) und 3(c) unten näher dargestellt. Soweit solche grenzüberschreitenden Übermittlungen zur Vertragserfüllung notwendig sind, ermächtigt der Kunde Magnet und seine Unterauftragsverarbeiter, grenzüberschreitenden Übermittlungen Personenbezogener Daten von Kunden in Übereinstimmung mit diesem AVV vorzunehmen, wenn die anwendbaren

Datenschutzgesetze zugleich eingehalten werden. Der Kunde wird Magnet vor der Weitergabe personenbezogener Daten darüber informieren, ob der DS-GVO oder der UK-GDPR unterfallende personenbezogene Daten von Magnet verarbeitet werden.

- b) Übermittlungen aus dem EWR. In Bezug auf Personenbezogene Daten von Kunden, die aus dem Europäischen Wirtschaftsraum („EWR“) übermittelt werden, gelten die genannten EU-SCCs, die Teil dieses AVV sind, und haben entsprechend den Bestimmungen der EU-SCCs Vorrang vor dem Rest dieses AVV. Die EU-SCCs werden gemäß den nachfolgenden Bestimmungen abgeschlossen:
- i) Soweit der Kunde Datenexporteur und Verantwortlicher und Magnet Datenimporteur und Auftragsverarbeiter ist, findet Modul 2 Anwendung.
 - ii) Klausel 7, die "Kopplungsklausel (fakultativ)", findet keine Anwendung.
 - iii) Bei Klausel 9 (Einsatz von Unterauftragsverarbeitern) wählen die Parteien die Option 2 (Allgemeine schriftliche Genehmigung), und die Frist für die vorherige Mitteilung der Beauftragung oder des Wechsel von Unterauftragsverarbeitern wird in Ziffer 6 dieses AVV festgelegt.
 - iv) Bei Klausel 11 (Rechtsbehelfe) entfällt die fakultative Bestimmung, dass Betroffene Personen die Möglichkeit haben müssen, eine Beschwerde bei einer unabhängigen Streitbeilegungsstelle einzureichen.
 - v) Bei Klausel 17 (Anwendbares Recht) wählen die Parteien Option 1 (das Recht eines EU-Mitgliedstaates, das Rechte von Drittbegünstigten zulässt). Die Parteien wählen das Recht von Frankreich.
 - vi) Bei Klausel 18 (Gerichtsstands und Zuständigkeit) wählen die Parteien die Gerichte von Frankreich.
 - vii) Die Anhänge I und II sind diesem AVV beigelegt.
 - viii) Mit dem Abschluss dieses AVV wird davon ausgegangen, dass die Parteien die EU-SSCs und ihre geltenden Anhänge unterzeichnen. Die aktuellste Fassung der EU-SSCs ist unter dem nachfolgenden Link auffindbar <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32021D0914>.
- c) Übermittlungen aus dem UK. In Bezug auf personenbezogene Daten, die aus dem Vereinigten Königreich übermittelt werden und für die das Recht des Vereinigten Königreichs (und nicht das Recht eines EWR-Mitgliedstaats) die Anforderungen an eine grenzüberschreitende Übermittlung bestimmt, ist das geltende UK-IDTA Teil dieses AVV und hat entsprechend den Bestimmungen der UK-IDTA Vorrang vor dem Rest dieses AVV, es sei denn, das Vereinigte Königreich gibt Aktualisierungen der UK-IDTA heraus, die nach Kenntnisnahme des Kunden vorrangig gelten. Für die in dieser Ziffer verwendeten undefinierten Begriffe in Großbuchstaben gelten die Definitionen des UK-IDTA.
- i) Für Übermittlungen aus dem UK findet das UK Addendum, *template Addendum B.1.0 issued 2 February 2022*, Anwendung. Das UK Addendum wird gemäß den nachfolgenden Bestimmungen abgeschlossen:
 - (1) Tabelle 1 des UK Addendum: (1) Die Angaben zu den Parteien sind die Parteien und ihre verbundenen Unternehmen, soweit eine von ihnen an einer solchen Übermittlung beteiligt ist, einschließlich der in Annex 1 genannten Übermittlungen; (2) der Hauptansprechpartner ist die in Anhang 1 genannte Kontaktperson.
 - (2) Tabelle 2 des UK-Addendum: Es gilt die Fassung der vereinbarten EU-SCCs, die hiermit Vertragsinhalt werden.
 - (3) Tabelle 3 des UK-Addendum: (1) Die Liste der Parteien (IDTA Annex 1.A) findet sich in Anhang 1; (2) Beschreibung des Transfers (IDTA Annex 1.B) befindet sich in Anhang 1; (3) Technische und

organisatorische Maßnahmen (IDTA Annex II) befinden sich in Anhang B; die Liste der Unterauftragsverarbeiter (IDTA Annex III) findet sich in Anhang A. .

- (4) Tabelle 4 des UK-Addendum: Keine der Parteien kann diesen AVV gemäß Abschnitt 19 des UK-Addendum beenden.
 - (5) Mit dem Abschluss dieses AVV unterzeichnen die Parteien das UK-Addendum und die dazugehörigen Tabellen und Annexe.
- d) Gesetzliche Überarbeitungen der EU-SCCs oder UK-IDTA. Für den Fall, dass die DS-GVO oder UK-GDPR die Verwendung geänderter Standardvertragsklauseln, die auf diesen AVV anwendbar sind, erfordern, finden diese geänderten Standardvertragsklauseln je nach Anwendungsbereich automatisch als Ersatz für die EU-SCCs und/oder UK-IDTA, Anwendung, ohne dass weitere Maßnahmen erforderlich sind; dies gilt nur dann nicht, wenn Magnet den Kunden anderweitig darüber in Kenntnis setzt. Übermittlung aus der Schweiz. In Bezug auf aus der Schweiz übermittelte personenbezogene Daten, für die das schweizerische Recht (und nicht das Recht eines EWR-Mitgliedstaats) den internationalen Charakter der Übermittlung regelt, werden die Verweise auf die DSGVO in Klausel 4 der EU-SCCs, soweit rechtlich zulässig dahingehend geändert, dass sie sich stattdessen auf das schweizerische Bundesgesetz über den Datenschutz (DSG) oder dessen Nachfolger beziehen, und der Begriff der Aufsichtsbehörde den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten mit umfasst..
- e) Übermittlungen aus dem Dubai International Financial Centre („DIFC“). Für personenbezogene Daten, die den DIFC-Datenschutzgesetzen unterliegen („DIFC-Daten“), gelten diese Standardvertragsklauseln. Für exportierte personenbezogene Daten, die den DIFC-Datenschutzgesetzen unterliegen, gilt das DIFC-Datenschutzgesetz Nr. 5 von 2020 in seiner geänderten Fassung für SCCs soweit diese DIFC-Daten betreffen. Der Datenschutzbeauftragte des DIFC ist die Aufsichtsbehörde für personenbezogene Daten im DIFC (*DIFC Commissioner of Data Protection*).
- 3.2. Soweit Personenbezogene Daten von Kunden übermittelt werden müssen, die nicht unter die Pflichten der Ziffer 3.1 fallen und anderen spezifischen Übermittlungsanforderungen oder -mechanismen unterliegen, wird der Kunde Magnet über etwaige Einschränkungen und Pflichten informieren. Die Parteien werden nach Treu und Glauben zusammenarbeiten, um diesen AVV zu ändern oder zusätzliche Klauseln zu vereinbaren, die erforderlich sind, um eine konforme Übermittlung Personenbezogener Daten von Kunden an Magnet zu ermöglichen.
- 3.3. Magnet kann Personenbezogene Daten von Kunden vorbehaltlich angemessener Schutzmaßnahmen und/oder Übermittlungsmechanismen, die den Datenschutzgesetzen entsprechen, an eine andere Partei weiterleiten.
4. **Mitarbeiter**. Magnet stellt sicher, dass alle zur Verarbeitung Personenbezogener Daten von Kunden befugten Mitarbeiter von Magnet eine Vertraulichkeitsverpflichtung in angemessenen Umfang abgegeben haben oder einer angemessenen gesetzlichen Geheimhaltungspflicht unterliegen.
5. **Sicherheit**. Magnet wird in Bezug auf die Personenbezogenen Daten von Kunden angemessene technische und organisatorische Maßnahmen ergreifen, wie in Anhang B dieses AVV dargelegt, die dazu bestimmt sind, ein Sicherheitsniveau zu gewährleisten, das den Risiken angemessen ist, die sich aus der Verarbeitung der Personenbezogenen Daten von Kunden durch Magnet ergeben. Im Falle eines Sicherheitsvorfalls, der Personenbezogene Daten von Kunden betrifft, wird Magnet unverzüglich Schritte unternehmen, um den Sicherheitsvorfall zu beheben, und den Kunden unverzüglich, auf jeden Fall aber innerhalb von zweiundsiebzig (72) Stunden nach Bekanntwerden eines solchen Sicherheitsvorfalls benachrichtigen. Magnet wird dem Kunden ausreichende Informationen zur Verfügung stellen, damit der Kunden seinen Mitteilungspflichten gegenüber den betroffenen Personen und/oder den Aufsichtsbehörden nachkommen zu kann und wird den Kunden im angemessenen Umfang unterstützen, wenn dieser bei der Reaktion auf den Sicherheitsvorfall Unterstützung benötigt.
6. **Verarbeitung durch Unterauftragsverarbeiter**. Der Kunde erklärt sich ausdrücklich damit einverstanden, dass Magnet Unterauftragsverarbeiter einsetzt. Abhängig vom Standort des Kunden und dem/den gekauften und/oder lizenzierten Produkt(en) werden unterschiedliche Unterauftragsverarbeiter eingesetzt. Diese sind in Anhang A des AVV aufgeführt. Der Kunde erklärt sich damit einverstanden, dass Magnet weitere Unterauftragsverarbeiter unter den folgenden Voraussetzungen beauftragen darf:
- 6.1. Magnet wird den Kunden über einen neuen Unterauftragsverarbeiter, der Personenbezogene Daten von Kunden verarbeitet, unterrichten. Nach Erhalt einer solchen Mitteilung kann der Kunde der Beauftragung des neuen Unterauftragsverarbeiters innerhalb von fünfzehn (15) Kalendertagen unter Nennung eines sachlichen Grundes widersprechen. Etwaige Differenzen werden die Parteien nach Treu und Glauben lösen.

- 6.2. Magnet wird mit den Unterauftragsverarbeitern einen schriftlichen Vertrag abschließen, die ein dieses AVV gleichwertiges Schutzniveau für Personenbezogene Daten von Kunden bestimmt; Magnet bleibt gegenüber dem Kunden für die Durchführung der Verarbeitung Personenbezogener Daten von Kunden durch jeden Unterauftragsverarbeiter bei der Erbringung der Leistungen verantwortlich.
7. **Angemessene Unterstützung.** Auf Anfordern des Kunden hin wird Magnet den Kunden dabei angemessen unterstützen die Bestimmungen der Datenschutzgesetzte einzuhalten, Rechte von betroffenen Personen zu erfüllen, sowie datenschutzrechtliche Prüfungen und Konsultationen mit Behörden durchzuführen; dies gilt nicht, wenn Magnet dafür auf Personenbezogene Daten von Kunden zugreifen muss, auf die es nicht bei der regulären Erbringen der Leistungen zugreifen muss.
8. **Löschung oder Rückgabe von Personenbezogenen Daten von Kunden.** Während der Erbringung der Leistungen können der Kunde und/oder die autorisierten Nutzer des Kunden Personenbezogene Daten von Kunden im Rahmen der erbrachten Leistungen löschen. Nach Ablauf oder Beendigung des Vertrages oder nach vollständiger Erbringung der Leistungen hat der Kunde sechzig (60) Kalendertage Zeit, um Personenbezogene Daten von Kunden aus den erbrachten Leistungen abzurufen; danach wird Magnet die Personenbezogenen Daten des Kunden löschen. Auf Verlangen des Kunden wird Magnet schriftlich bestätigen, dass die Personenbezogenen Daten von Kunden gelöscht worden sind. Dieser AVV bleibt wirksam, bis alle Personenbezogenen Daten von Kunden vernichtet worden sind.
9. **Audit-Rechte** . Auf schriftliches Anfordern des Kunden und nicht öfter als einmal im Jahr wird Magnet dem Kunden (oder dem unabhängigen, vom Kundenbeauftragten Prüfer, der kein Wettbewerber von Magnet ist) Informationen zur Verfügung stellen, um Magnet den Nachweis über die Einhaltung seiner Verpflichtungen unter diesem AVV und/oder den Datenschutzgesetzen zu ermöglichen . Alternativ und nach eigenem Ermessen kann Magnet (i) einen qualifizierten und unabhängigen Dritten als Prüfer beauftragen, Magnets technische und organisatorische Sicherheitsmaßnahmen zu bewerten, wobei der Kunde eine Zusammenfassung dieses Prüfberichts als ausreichend anerkennt, sofern nicht detailliertere Informationen erforderlich sind, um Datenschutzgesetze einzuhalten; oder (ii) eine Zusammenfassung einer Bewertung durch einen unabhängigen Dritten als Prüfer zur Verfügung stellen, die in den zwölf (12) Monaten vor der Anfordern des Kunden erhoben wurde, wobei der Kunde diese als ausreichend anerkennt, sofern nicht detailliertere Informationen erforderlich sind, um Datenschutzgesetze einzuhalten. Alle Informationen, die dem Kunden gemäß dieser Ziffer 9 zur Verfügung gestellt werden, sind vertrauliche Informationen von Magnet.
10. **Änderungen der Datenschutzgesetze.** Wenn eine Änderung dieses AVV infolge einer Änderung oder Aktualisierung der Datenschutzgesetze erforderlich ist, wird Magnet diesen AVV entsprechend aktualisieren. Die Änderungen müssen mit den exakten Anforderungen der Datenschutzgesetze entsprechen.

ANHANG A
zum Auftragsverarbeitungsvertrag

Einzelheiten der Verarbeitung Personenbezogener Daten von Kunden

1. Zwecke der Verarbeitung; Verarbeitungsvorgänge

Die Art und der Zweck der Verarbeitung Personenbezogener Daten von Kunden umfassen:

Die Erbringung der Leistungen in Übereinstimmung mit dem Vertrag und diesem AVV.

2. Personenbezogene Daten von Kunden

a. Arten von personenbezogenen Daten

Wir erheben eine begrenzte Anzahl personenbezogener Daten im Zusammenhang mit unseren Software- und Supportleistungen. Die folgenden Kategorien personenbezogener Daten werden erfasst:

- Kontakt- und Zahlungsinformationen für Unternehmen
- Technische Informationen oder Internet-Informationen für die Lizenzaktivierung (z. B. UUID (*Universally Unique Identifier*), Benutzername, Computer- und Informationen zum Domainnamen sowie dem Server)
- Informationen entsprechend unserer Cookie-Richtlinie;
- Andere Informationen, die Sie bei der Inanspruchnahme von Support-Leistungen freiwillig angeben.

Weitere Informationen finden Sie in unserer Datenschutzrichtlinie. Unsere Cookie-Richtlinie und Datenschutzrichtlinie finden Sie unter www.magnetforensics.com/legal.

b. Betroffene Personen

Zu den Kategorien der betroffenen Personen, auf die sich Personenbezogene Daten von Kunden beziehen, gehören:

- Mitarbeiter des Kunden
- Andere Betroffene Personen, deren Personenbezogene Daten der Kunde im Rahmen der Leistungen erhebt und verarbeitet

3. Dauer der Verarbeitung

Fortlaufend für die Dauer des Vertrages, zuzüglich des Zeitraums vom Vertragsende bis zur Rückgabe oder Löschung aller Personenbezogenen Daten von Kunden durch Magnet entsprechend dem Vertrag (einschließlich dieses AVV), den Anweisungen des Kunden und dem anwendbaren Recht.

4. Zugelassene Unterauftragsverarbeiter

Welche Unterauftragsverarbeiter für Personenbezogene Daten von Kunden zuständig sind, kann vom Standort des Kunden und dem Produkt bzw. den Produkten abhängen, die der Kunde erworben und/oder lizenziert hat. Bitte sprechen Sie mit Ihrem Kundenbetreuer oder kontaktieren Sie uns wie nachfolgend beschrieben, um weitere Informationen zu erhalten.

- a. **Amazon Web Leistungen, Inc.**
Erbrachte Leistungen: Cloud-Hosting für Personenbezogene Daten von Kunden und Infrastruktur für Leistungen
- b. **SalesForce**
Erbrachte Leistungen: Kundenmanagement, Produktdokumentation, Projektmanagement, Feedback zur Dokumentation und Produktschulung.

- c. **Gainsight PX**
Erbrachte Leistungen: Produktnutzungsdaten für bestimmte Produkte.
- d. **Gainsight CS**
Erbrachte Leistungen: Kundenmanagement für bestimmte Produkte.
- e. **Flexera**
Erbrachte Leistungen: Produktlizenzierung.
- f. **Skilljar**
Erbrachte Leistungen: Produktschulung.
- g. **Smartsheet**
Erbrachte Leistungen: Projektmanagement.
- h. **Slack**
Erbrachte Leistungen: Projektmanagement.
- i. **JIRA**
Erbrachte Leistungen: Fallmanagement.
- j. **SharePoint**
Erbrachte Leistungen: Projektmanagement.
- k. **Mailchimp**
Erbrachte Leistungen: Marketing, lizenzierte Funktion für eine Anwendung.
- l. **MailGun**
Erbrachte Leistungen: Marketing, lizenzierte Funktion für eine Anwendung.
- m. **SendGrid**
Erbrachte Leistungen: Marketing, lizenzierte Funktion für eine Anwendung.
- n. **Okta**
Erbrachte Leistungen: SSO, Marketing- und Produktplanungszwecke, Sign-on-Funktionalität.
- o. **Zoho Formulare**
Erbrachte Leistungen: Umfragen, Anfragen für Produktfeedback
- p. **Aha!**
Leistungen: Roadmap-Management, Ideen-Portal.

ANHANG B

zum Auftragsverarbeitungsvertrag

Technische und organisatorische Maßnahmen (TOM)

1. Magnet hat ein umfassendes, schriftliches Informationssicherheitsprogramm eingeführt und wird es beibehalten. Eine oder mehrere benannte qualifizierte Personen ist/sind für die Pflege des Informationssicherheitsprogramms von Magnet verantwortlich. Magnet wird das Informationssicherheitsprogramm regelmäßig überprüfen, um vorhersehbare interne und externe Risiken für die Privatsphäre, die Sicherheit und/oder die Integrität elektronischer, physischer oder sonstiger Aufzeichnungen, die Personenbezogene Daten von Kunden enthalten, zu identifizieren und zu bewerten und um sicherzustellen, dass Magnets Informationssicherheitsprogramm weiterhin den geltenden Datenschutzgesetzen entspricht.
2. Magnets Informationssicherheitsprogramm (in Bezug auf die Personenbezogenen Daten von Kunden) entspricht im Wesentlichen der Norm ISO/IEC 27001:2013 Informationstechnologie - Sicherheitstechniken - Managementsysteme für Informationssicherheit - Anforderungen. Darüber hinaus wird Magnet einen SOC 2, Typ II Bericht über die Kontrollen in Bezug auf Sicherheit, Verfügbarkeit, Datenintegrität der Verarbeitung, Vertraulichkeit und Datenschutz seiner relevanten Systeme und Verarbeitungen von einer qualifizierten, unabhängigen, professionellen Wirtschaftsprüfungsgesellschaft durchführen lassen. Auf Anfordern den Kunden hin wird Magnet dem Kunden gestatten, die Ergebnisse solcher Prüfberichte oder Bewertungen (die Magnets vertrauliche Informationen sind) einzusehen, soweit sie für die Personenbezogenen Daten von Kunden relevant sind.
3. Jegliche Verarbeitung Personenbezogener Daten von Kunden erfolgt über Informationsverarbeitungssysteme, für die wirtschaftlich angemessene technische und organisatorische Maßnahmen zum Schutz Personenbezogener Daten von Kunden getroffen wurden. Magnet wird angemessene und geeignete technische, physische und administrative Maßnahmen ergreifen, um die Personenbezogenen Daten von Kunden, die sich in seinem Besitz oder unter seiner Kontrolle befinden, gegen unbefugte oder unrechtmäßige Verarbeitung oder zufälligen Verlust, Zerstörung oder Beschädigung in Übereinstimmung mit den anwendbaren Datenschutzgesetzen zu schützen, wobei der Schaden, der sich aus einer unbefugten oder unrechtmäßigen Verarbeitung oder einem zufälligen Verlust, einer zufälligen Zerstörung oder Beschädigung ergeben könnte, und die Sensibilität der Personenbezogenen Daten des Kunden berücksichtigt werden.
4. Magnet wird (a) angemessene Schritte unternehmen, um die Zuverlässigkeit von Angestellten, Zeitarbeitern, Auftragnehmern und anderem Personal (zusammenfassend „**Personal**“), das Zugang zu Personenbezogenen Daten von Kunden hat, zu gewährleisten; (b) den Zugang zu Personenbezogenen Daten von Kunden auf diejenigen Mitarbeiter beschränken, für die eine betriebliche Notwendigkeit besteht, Zugang zu solchen Personenbezogenen Daten von Kunden zu haben, und die eine angemessene Schulung zum Schutz der Privatsphäre und zur Sicherheit erhalten haben; und (c) Hintergrundüberprüfungen für Mitarbeiter und Auftragnehmer im Rahmen des gesetzlich zulässigen durchführen, die für Personenbezogene Daten von Kunden verantwortlich sind oder Zugang zu ihnen haben.
5. **Mindestmaß an Kontrollen.** Ohne Einschränkung sonstiger Verpflichtungen des AVV werden die folgenden Sicherheitskontrollen durchgeführt:
 - (a) die Richtlinien, Verfahren und Prozesse zur Verwaltung der Sicherheitsrisiken im Zusammenhang mit der Verarbeitung Personenbezogener Daten von Kunden werden dokumentiert, nachvollzogen, überprüft und regelmäßig aktualisiert werden;
 - (b) Geräte, Systeme, Einrichtungen und andere Verarbeitungsgeräte („**Verarbeitungsgeräte**“), die auf Personenbezogene Daten von Kunden zugreifen, diese speichern und verarbeiten, sowie diejenigen, die für die Erbringung der Leistungen für den Kunden gemäß dem AVV wesentlich sind, werden identifiziert und verwaltet;
 - (c) der physische Zugang zu den Verarbeitungsgeräten wird verwaltet und kontrolliert, einschließlich Maßnahmen zur Verhinderung und Aufdeckung von unbefugtem Zugang zu den Verarbeitungsgeräten (einschließlich dem Zugang zu den jeweiligen Räumlichkeiten), und der Zugang zu den Verarbeitungsgeräten wird auf autorisierte Benutzer beschränkt;
 - (d) Sicherheitsrisikobewertungen werden durchgeführt, um vorhersehbare interne und externe Sicherheitsrisiken zu ermitteln und zu bewerten;
 - (e) der Fernzugriff von Mitarbeitern und anderen Personen auf Verarbeitungsgeräte ist beschränkt und wird mit einer mehrstufigen Authentifizierung sicher verwaltet;

- (f) die Personenbezogenen Daten von Kunden und die zugehörigen Aufzeichnungen werden identifiziert, und der Zugriff wird so verwaltet, dass die Vertraulichkeit, Integrität und Verfügbarkeit dieser Daten geschützt ist;
 - (g) es werden technische Überwachungsmittel eingerichtet, die eine Überprüfung nicht autorisierter Aktivitäten ermöglichen;
 - (h) elektronische und physische Aufzeichnungen, die Personenbezogene Daten von Kunden enthalten, werden entsprechend den Richtlinien und Verfahren zur sicheren Vernichtung vernichtet;
 - (i) geeignete technische Sicherheitslösungen werden implementiert und verwaltet, um die Vertraulichkeit, Integrität und Verfügbarkeit der Personenbezogenen Daten von Kunden zu schützen;
 - (j) kritische Sicherheitspatches für Betriebssysteme und Software werden rechtzeitig auf allen Verarbeitungsgeräten installiert, die zur Verarbeitung Personenbezogener Daten von Kunden verwendet werden, und erkannte sicherheitsrelevante Fixes werden umgehend installiert;
 - (k) Anti-Malware-Software wird auf allen Verarbeitungsgeräten, die zur Verarbeitung Personenbezogener Daten von Kunden verwendet werden, installiert und so konfiguriert, dass sie regelmäßig nach Updates einspielen;
 - (l) die Wartung und Reparatur von Komponenten des Informationssystems wird auf kontrollierte und sichere Weise durchgeführt;
 - (m) das Netzwerk und die Verarbeitungsgeräte von Magnet werden überwacht, um Schwachstellen, Bedrohungen, irreguläre oder unautorisierte Aktivitäten und andere potenzielle Cybersicherheitsereignisse (zusammenfassend als „**sicherheitsrelevante Ereignisse**“ bezeichnet) rechtzeitig zu erkennen;
 - (n) die Personenbezogenen Daten von Kunden werden nicht auf tragbaren oder leicht zu entfernenden Speichermedien gespeichert;
 - (o) Personenbezogene Daten von Kunden werden nicht in Testumgebungen oder sonstigen Umgebungen gespeichert oder verwendet, die keine Produktionsumgebung darstellen;
 - (p) Prozesse und Verfahren zur Reaktion auf sicherheitsrelevante Ereignisse werden fortwährend weiterentwickelt und getestet, um eine rechtzeitige Reaktion zu gewährleisten und darüber hinaus finden folgende Maßnahmen statt: (i) Sicherheitsrelevante Ereignisse werden untersucht, nachvollzogen und kategorisiert; (ii) es werden Maßnahmen ergriffen, um die Folgen eines sicherheitsrelevanten Ereignisses zu begrenzen und verbleibende Bedrohungen oder Schwachstellen zu beseitigen; (iii) betroffene Verarbeitungsgeräte und Personenbezogene Daten von Kunden werden wiederhergestellt und andere geeignete Maßnahmen zur Schadensbegrenzung werden ergriffen; (iv) Reaktions- und Wiederherstellungsmaßnahmen werden dokumentiert; und (v) Richtlinien und Verfahren werden routinemäßig überprüft und aktualisiert, um gewonnene Erkenntnisse zu berücksichtigen und potenzielle Bedrohungen und Schwachstellen zu beseitigen.
6. **Verschlüsselung und Schutz der Infrastruktur.** Personenbezogene Daten von Kunden, einschließlich Personenbezogener Daten von Kunden auf tragbaren Geräten und Sicherungsmedien, werden bei der Übermittlung und im Ruhezustand verschlüsselt, wobei branchenübliche kryptografische Techniken und eine sichere Key-Management-Systeme zum Einsatz kommen.
7. **Systemauthentifizierung und -autorisierung.** Der Zugriff auf Personenbezogene Daten von Kunden ist auf Grundlage einer Benutzerauthentifizierung zu protokollieren; dies umfasst insbesondere die Kontrolle unter Einsatz von Benutzer-IDs und sonstigen Identifikationsmaßnahmen, Passwörtern, biometrischen Merkmalen, Authentifizierungs-Tokens, aktiven Account Log-in-Verfahren, Protokollaufzeichnungen, die Zugriffsversuche aufzeichnen, und Sperrung nach mehreren erfolglosen Anmeldeversuchen.
- (a) Die Zugriffsrechte der Benutzer auf Systeme, die Personenbezogene Daten von Kunden enthalten, werden regelmäßig überprüft.
 - (b) Magnet wird elektronische Protokolle von Personen führen, die auf Personenbezogene Daten von Kunden zugreifen, in denen die Details des Zugriffs und der vorgenommenen Transaktionsänderungen dargestellt werden. Solche elektronischen Protokolle müssen dem Kunden auf Anfordern zur Einsichtnahme zur Verfügung gestellt werden.

8. **Betriebskontinuität.** Magnet führt geeignete Verfahren für die Betriebskontinuität und die Wiederherstellung im Katastrophenfall (der "**Betriebskontinuitätsplan**") ein, um die kontinuierliche Erfüllung seiner Verpflichtungen im Rahmen des AVV und die betriebliche Widerstandsfähigkeit im Allgemeinen zu gewährleisten; Magnet wird den Betriebskontinuitätsplan nach den Maßstäben einer *best-practice* in dieser Branche regelmäßig weiterentwickeln, überprüfen und aktualisieren.

ANNEX I

A. LISTE DER PARTEIEN

Datenexporteur(e): [*Identität und Kontaktdaten des/der Datenexporteurs(e) und ggf. seines/ihres Datenschutzbeauftragten und/oder Vertreters in der Europäischen Union*].

1. Name: Kunde, wie im Vertrag angegeben

Anschrift: Die Adresse des Kunden, wie im Vertrag angegeben

Name, Position und Kontaktdaten der Kontaktperson: Kontaktperson des Kunden, wie im Vertrag angegeben

Tätigkeiten, die für die gemäß diesen Bestimmungen übermittelten Daten relevant sind: Bereitstellung personenbezogener Daten für die Inanspruchnahme der Leistungen

Rolle (Verantwortlicher/Auftragsverarbeiter): Verantwortlicher

Datenimporteur(e): [*Identität und Kontaktdaten des/der Datenimporteure(s), einschließlich einer Kontaktperson, die für den Datenschutz zuständig ist*]

1. Name: **Magnet Forensics USA Inc.**

Adresse: 2250, Corporate Park Dr #130, Herndon, VA 20171

Name, Position und Kontaktdaten der Kontaktperson: dpo@magnetforensics.com

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten relevant sind: Erbringung der Leistungen

Unterschrift und Datum:

Rolle (Verantwortlicher/Auftragsverarbeiter): Auftragsverarbeiter

B. BESCHREIBUNG DER ÜBERMITTLUNG

Kategorien von betroffenen Personen, deren personenbezogene Daten übermittelt werden

Siehe Annex I

Kategorien der übermittelten personenbezogenen Daten

Siehe Annex I

Übermittlung sensibler Daten (falls zutreffend) und Anwendung von Beschränkungen oder Schutzmaßnahmen, die der Art der Daten und den damit verbundenen Risiken in vollem Umfang Rechnung tragen, wie z. B. strikte Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnung des Zugangs zu den Daten, Beschränkungen für die Weiterübermittlung oder zusätzliche Sicherheitsmaßnahmen.

Siehe Annex I

Häufigkeit der Übermittlung (z. B. ob die Daten einmalig oder kontinuierlich übermittelt werden).

Regelmäßig

Art der Verarbeitung

Erhebung, Organisation, Speicherung, Gewährung des Zugangs, Einschränkung, Löschung und Vernichtung

Zweck(e) der Datenübermittlung und Weiterverarbeitung

Für die Erbringung der Leistungen

den Zeitraum, für den die personenbezogenen Daten aufbewahrt werden, oder, falls dies nicht möglich ist, die Kriterien, nach denen dieser Zeitraum festgelegt wird

Siehe Annex I

Bei Übermittlungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben

Unterauftragsverarbeiter verarbeiten personenbezogene Daten nach Maßgabe des Mittel und Zwecks sowie der Art und der Dauer der Verarbeitung durch den Verantwortlichen.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

Die Aufsichtsbehörde eines der Mitgliedstaaten, in dem die betroffenen Personen, deren personenbezogene Daten gemäß diesen Regelungen übermittelt werden, ihren gewöhnlichen Aufenthaltsort haben, ist die zuständige Aufsichtsbehörde.

ANNEX II

Technische und organisatorische Maßnahmen (TOM) einschließlich technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Daten

Die technischen und organisatorischen Maßnahmen sind im Anhang B aufgeführt.