**Vereinbarung zur Auftragsverarbeitung**

**nach Art. 28 DS-GVO**

**zwischen**

xxxx

als Verantwortlicher

- nachstehend **„Auftraggeber“** genannt -

und

**SDK Systemdruck Köln GmbH & Co. KG**

Maarweg 233, 50825 Köln

vertreten durch die Geschäftsführung

Nicole Royar

als Auftragsverarbeiter

- nachstehend **„Auftragnehmer“** genannt –

- gemeinsam **„Vertragsparteien“** oder „**Parteien**“-

**Inhaltsübersicht**

[1. Generelles 3](#_Toc511309162)

[2. begriffsbestimmungen 3](#_Toc511309163)

[3. Bestandteile der Vereinbarung 3](#_Toc511309164)

[4. grundsätze zur Auftragsverarbeitung 4](#_Toc511309165)

[5. dauer der Auftragsverarbeitung 4](#_Toc511309166)

[6. Ort der Auftragsverarbeitung 4](#_Toc511309169)

[7. Weisungen des Auftraggebers 4](#_Toc511309178)

[8. Anpassungen und fortentwicklung 4](#_Toc511309179)

[9. Verschwiegenheitspflicht 5](#_Toc511309180)

[10. sicherheit der Verarbeitung 5](#_Toc511309181)

[11. Unterauftragnehmer 6](#_Toc511309183)

[12. rechte der betroffenen personen 6](#_Toc511309184)

[13. Meldung von Datenschutzvorfällen 7](#_Toc511309185)

[14. Mitwirkungspflichten des auftragnehmers 7](#_Toc511309188)

[15. Herausgabe von personenbezogenen Daten 8](#_Toc511309189)

[16. Kontrollrechte des Auftraggebers 9](#_Toc511309190)

[17. Pflichten des Auftraggebers 9](#_Toc511309191)

[18. Haftung 9](#_Toc511309192)

[19. Sonstige Pflichten und Bestimmungen 9](#_Toc511309193)

[Anlage Gegenstand der Auftragsverarbeitung 11](#_Toc511309194)

[Anlage sicherheit der verarbeitung 13](#_Toc511309195)

[anlage Unterauftragnehmer 16](#_Toc511309196)

# Generelles

## Die vorliegende Vereinbarung (nebst ihrer unten näher bezeichneten Anlagen) zur Auftragsverarbeitung nach Art. 28 DS-GVO (nachfolgend auch „**Vereinbarung**“) konkretisiert gesetzliche Rechte und Pflichten, die sich für die Parteien aus der Datenschutzgrundverordnung (VO (EU) 2016/679, nachfolgend auch „DS-GVO“) ergeben, wenn der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet oder Auftragswartung betreibt (nachfolgend auch „**Auftragsverarbeitung**“).

## Der Auftragnehmer erkennt an, dass die DS-GVO die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten schützt und diese Prinzipien auch für den Auftragnehmer gelten.

# begriffsbestimmungen

## Es gelten die Begriffsbestimmungen aus Art. 4 und Art. 9 DS-GVO sowie folgende zusätzlichen Begriffsbestimmungen:

## „**Auftragswartung**“ meint Leistungen des Auftragnehmers (z. B. Pflege-, Wartungs- oder sonstige Leistungen an Computerprogrammen oder technischen Gegenständen zur Informationsverarbeitung), bei deren Ausführung nicht auszuschließen ist, dass der Auftragnehmer Zugriff auf personenbezogenen Daten erhält, die der Auftraggeber verantwortet.

## „**Leistungsvertrag**“ meint das Rechtsverhältnis zwischen dem Auftraggeber und den Auftragnehmer, aufgrund dessen der Auftragnehmer für den Auftraggeber bestimmungsgemäß Auftragsverarbeitung oder Auftragswartung betreibt.

## „**Unterauftragnehmer**“ meint Dritte im Sinne des Art. 4 Nr. 10 DS-GVO, die der Auftragnehmer mit schriftlicher Gestattung des Auftraggebers zur Leistungserbringung im Rahmen des Leistungsvertrags einsetzt.

## Weitere Begriffsbestimmungen können kontextbezogen in der jeweiligen Ziffer dieser Vereinbarung getroffen werden.

# Bestandteile der Vereinbarung

## Die Auftragsverarbeitung oder -wartung durch den Auftragnehmer erfolgt stets auf der Grundlage eines Leistungsvertrags (Ziffer 2.3) zwischen dem Auftragnehmer und dem Auftraggeber. Der Leistungsvertrag ist maßgeblich für den Gegenstand, die Dauer, die Art und den Zweck der Auftragsverarbeitung, sowie für die Festlegung der Art der personenbezogenen Daten und der Kategorien der betroffenen Personen (nachfolgend auch „Auftragsgegenstand“). Zur Bestimmung des Auftragsgegenstands werden die Parteien die **Anlage „Auftragsgegenstand“**, welche dieser Vereinbarung beiliegt, verwenden, und diese dem entsprechenden Leistungsvertrag rechtsverbindlich hinzufügen.

## Die vorliegende Vereinbarung beinhaltet Regelungen zur Auftragsverarbeitung bzw. -wartung, die auf alle zwischen den Parteien geschlossenen Leistungsverträge anzuwenden sind. Verbindliche Vertragsbestandteile dieser Vereinbarung sind:

1. Anlage Auftragsgegenstand
2. Anlage Sicherheit der Verarbeitung

## Die Bestimmungen dieser Vereinbarung einschließlich ihrer Anlagen gehen etwaigen widersprüchlichen Regelungen eines Leistungsvertrags vor.

# grundsätze zur Auftragsverarbeitung

## Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich nach Maßgabe des Leistungsvertrags, nach Maßgabe dieser Vereinbarung sowie im Rahmen von Weisungen des Auftraggebers.

# dauer der Auftragsverarbeitung

## Diese Vereinbarung tritt am **01.06.2018** in Kraft.

## Die Vereinbarung endet automatisch und ohne dass es einer Kündigung bedarf, wenn der Auftragnehmer für den Auftraggeber insgesamt keine Auftragsverarbeitung oder -wartung mehr betreibt.

# Ort der Auftragsverarbeitung

## Die Auftragsverarbeitung darf ausschließlich - vorbehaltlich der nachfolgenden Bestimmungen - in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erfolgen.

## Jede Auftragsverarbeitung außerhalb eines Mitgliedsstaates der Europäischen Union oder außerhalb eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum (im folgenden „**Drittland**“) bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers.

# Weisungen des Auftraggebers

## Unbeschadet bindender Festlegungen i.S.d. Ziffer 3.2 dieser Vereinbarung erkennt der Auftragnehmer an, dass allein der Auftraggeber die Zwecke der Auftragsverarbeitung bestimmt und diese auch durch einzelfallbezogene Weisungen anordnen darf, und dass jede Verarbeitung durch den Auftragnehmer außerhalb der Zweckbestimmung oder einer Weisung rechtswidrig ist. Für Ausnahmen hiervon ist Art. 28 Abs. 3 lit. a DS-GVO maßgeblich.

## Jede Weisung des Auftraggebers verpflichtet den Auftragnehmer dazu, jeden in der Weisung bezeichneten Vorgang (z. B. Erheben, Speichern, Übermitteln, Löschen oder Vernichten von personenbezogenen Daten) weisungsgemäß vorzunehmen, zu dulden oder zu unterlassen („Handlungen“). Das Weisungsrecht des Auftraggebers beinhaltet insbesondere, dass der Auftraggeber gegenüber dem Auftragnehmer bestimmen darf, wie der Leistungsvertrag in datenschutzrechtlicher Hinsicht durchzuführen ist, sowie auftragskontrollbezogene Informationen verlangen zu dürfen, als auch Handlungen zu verlangen, die zur Erfüllung einer gesetzlichen, hoheitlichen oder behördlichen Anforderung, welcher der Auftraggeber unterliegt, dienen kann.

## Weisungen bedürfen grundsätzlich der Schrift- oder Textform (§ 126b BGB). Mündliche Weisungen sind nur in Ausnahmefällen zulässig; sie sind vom Auftragnehmer in Schrift- oder Textform (§ 126b BGB) zu dokumentieren.

## Der Auftragnehmer hat Weisungen vorbehaltslos und unverzüglich umzusetzen;

# Anpassungen und fortentwicklung

## Die Parteien sind sich einig, die vorliegende Vereinbarung einschließlich Anlagen im Fall von Änderungen, Anpassungen und/oder Ergänzungen datenschutzrechtlicher Bestimmungen – insbesondere der DS-GVO und/oder der jeweils anwendbaren nationalen Umsetzungsgesetze einvernehmlich anzupassen und zu ändern.

# Verschwiegenheitspflicht

## Der Auftragnehmer garantiert, dass er die bei ihm mit der Verarbeitung beschäftigten Personen zur Vertraulichkeit verpflichtet hat, und er diese Verpflichtung durch organisatorische Vorkehrungen auch nachhält, insbesondere dass personenbezogene Daten nicht unbefugt, nur auftragsgemäß bzw. nach Weisungen verarbeitet werden, und dass diese Verpflichtung auch nach Beendigung ihrer Tätigkeit fortbesteht (Art. 28 Abs. 3 lit b); Art. 29; Art. 32 Abs. 4 DS-GVO). Entsprechendes gilt für weitere datenschutzrechtliche Vertraulichkeits- und/oder Schutzbestimmungen, soweit diese für die Verarbeitung einschlägig sind.

## Dem Auftraggeber sind auf Verlangen entsprechende Nachweise unentgeltlich zur Verfügung zu stellen. Dem Auftragnehmer bleibt es nachgelassen, den Nachweis durch die Einhaltung genehmigter Verhaltensregeln (Art. 40 DS-GVO) oder die Einhaltung eines genehmigten Zertifizierungsverfahrens (Art. 42 DS-GVO) zu erbringen, soweit hieraus hervorgeht, dass die bei der Verarbeitung eingesetzten Personen nach Ziffer 9.1 zur Vertraulichkeit verpflichtet sind.

# sicherheit der Verarbeitung

## Der Auftragnehmer bestätigt, die in seinem Verantwortungsbereich nach Art. 32 DS-GVO erforderlichen Maßnahmen ergriffen zu haben. Der Auftragnehmer verpflichtet sich, seine innerbetriebliche Organisation unter Berücksichtigung des jeweiligen Stands der Technik, der Implementierungskosten und der Art, des Umfangs sowie der Umstände und Zwecke der Verarbeitung und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen entsprechend auszugestalten und zu aktualisieren, so dass diese den besonderen Anforderungen des Datenschutzes nach der DS-GVO entsprechen und den Schutz der Rechte der betroffenen Personen gewährleisten. Generell umfassen die zu ergreifenden technisch-organisatorischen Maßnahmen (TOM) insbesondere

### die dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der Daten;

### die Verschlüsselung personenbezogener Daten und – nach Möglichkeit – deren Pseudonymisierung;

### die Möglichkeit zur raschen Wiederherstellung der Verfügbarkeit personenbezogener Daten und den Zugang zu Ihnen im Fall eines physischen oder technischen Zwischenfalls; und

### die Einführung und das Vorhalten von Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

## Die dokumentierten Maßnahmen des Auftragnehmers werden Grundlage der jeweiligen Auftragsverarbeitung und als **ANLAGE Sicherheit der Verarbeitung** zu diesem Vertrag genommen.

## Dem Auftragnehmer bleibt es nachgelassen, die Geeignetheit der - insbesondere nach Art. 32 DS-GVO zu treffenden - technisch-organisatorischen Maßnahmen durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DS-GVO, oder die Einhaltung eines genehmigten Zertifizierungsverfahrens nach Art. 42 DS-GVO nachzuweisen. Der Nachweis kann nur (und nur solange) dadurch erfolgen, dass der Auftragnehmer dem Auftraggeber ein gültiges Zertifikat vorweist, welches von einer akkreditierten Zertifizierungsstelle nach Art. 43 DS-GVO für diejenigen Verarbeitungsverfahren und -orte erteilt ist, die für die Verarbeitungen unter dieser Vereinbarung beziehungsweise den entsprechenden Leistungsvertrag relevant sind. Veränderungen am Zertifikat oder dessen Ablauf hat der Auftragnehmer dem Auftraggeber unverzüglich mitzuteilen.

## Es ist dem Auftragnehmer gestattet, eine andere als eine ausdrücklich beschriebene technische Maßnahme zu ergreifen und umzusetzen, wenn das Sicherheitsniveau der Verarbeitung dadurch erhöht, die Maßnahme dokumentiert und dem Auftraggeber mitgeteilt wird.

# Unterauftragnehmer

## Die Unterbeauftragung der Verarbeitung durch den Auftragnehmer an einen Unterauftragnehmer ist unzulässig, es sei denn folgende Voraussetzungen sind erfüllt:

* Der Auftraggeber hat die Unterbeauftragung schriftlich (in dieser Vereinbarung, oder in einem Leistungsvertrag) nicht ausdrücklich ausgeschlossen,
* Der Auftragnehmer hat den Unterauftragnehmer sorgfältig ausgewählt,
* Der Auftragnehmer hat durch entsprechende Vereinbarungen mit dem Unterauftragnehmer sichergestellt, dass der Auftraggeber während der Laufzeit der Unterbeauftragung alle Rechte, die ihm gegenüber dem Auftragnehmer zustehen, auch gegenüber dem Unterauftragnehmer ausüben kann; dies beinhaltet auch Einsichtsrechte in datenschutzrelevante Unterlagen und Verträge und Auskunft über datenschutzrechtlich relevante Vorgänge.

## Die Verarbeitung, insbesondere auch die Übermittlung von personenbezogenen Daten an bzw. durch den Unterauftragnehmer sind nur (und nur solange) zulässig, als die in Ziffer 11.1 genannten Voraussetzungen nachweislich erfüllt sind und der Auftraggeber seine Zustimmung nicht nach Maßgabe von Ziffer 11.4 widerrufen hat.

## Bei Abschluss dieser Vereinbarung zwischen Auftraggeber und Auftragnehmer eingesetzte Unterauftragnehmer sind in der **Anlage Unterauftragnehmer** abschließend aufgezählt; etwaige Nachträge dazu sind schriftlich auszufertigen. Es bleibt unbenommen, Unterauftragnehmer im Leistungsvertrag zu gestatten.

# rechte der betroffenen personen

## Der Auftraggeber ist für die Wahrung der Rechte der betroffenen Personen nach dem 3. Kapitel DS-GVO verantwortlich. Dem Auftragnehmer ist eine Umsetzung der Rechte betroffener Personen nur nach Weisung des Auftraggebers gestattet. Der Auftragnehmer ist jedoch verpflichtet, den Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen nach dem 3. Kapitel der DS-GVO vollumfänglich zu unterstützen.

## Werden Betroffenenrechte unmittelbar gegenüber dem Auftragnehmer geltend gemacht, hat der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterzuleiten. Ist dem Auftragnehmer eine Zuordnung des Ersuchens zu einer Person nicht möglich, weist er die fehlende Identifizierbarkeit gegenüber dem Auftraggeber entsprechend Art. 11 Abs. 2 DS-GVO nach. Werden Ersuchen nicht unverzüglich weitergeleitet, haftet der Auftragnehmer dem Auftraggeber für etwaige Verzögerungen bei der Bearbeitung von Anfragen von betroffenen Personen unter Berücksichtigung der in Art. 12 Abs. 3 DS-GVO genannten Bearbeitungsfristen, es sei denn, er hat die Verzögerung nicht zu vertreten.

# Meldung von Datenschutzvorfällen

## Der Auftragnehmer erstattet in jedem Fall dem Auftraggeber Meldung, in dem er (i) von einer Verletzung des Schutzes personenbezogener Daten durch ihn oder die bei ihm beschäftigten Personen, (ii) von einem Verstoß gegen Vorschriften zum Schutz personenbezogener Daten oder (iii) von einem Verstoß gegen die in dieser Vereinbarung getroffenen Festlegungen Kenntnis erlangt (im folgenden „Datenschutzvorfall“).

## Die Meldung hat unverzüglich, spätestens innerhalb von achtundvierzig (48) Stunden ab Kenntniserlangung zu erfolgen.

## Nach Kenntniserlangung eines Datenschutzvorfalls trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Abmilderung nachteiliger Auswirkungen für die betroffenen Personen und den Auftraggeber.

# Mitwirkungspflichten des auftragnehmers

## Bezogen auf seinen Verantwortungsbereich ist der Auftragnehmer verpflichtet, die für das Verfahrensregister des Auftraggebers nach Art. 30 Abs. 1 DS-GVO erforderlichen Angaben und Informationen bereitzustellen.

## Der Auftragnehmer wird - bezogen auf seinen Verantwortungsbereich - den Auftraggeber bei der Einhaltung der Pflichten nach Art. 32 DS-GVO vollumfänglich unterstützen. Hierzu wird der Auftragnehmer dem Auftraggeber sämtliche für Art. 32 DS-GVO erforderlichen Unterlagen, Dokumente und Nachweise zur Verfügung stellen.

## Der Auftragnehmer ist verpflichtet, die Durchführung der Verarbeitung regelmäßig auf ihre Vertragskonformität hin selbst zu überprüfen. Werden im Rahmen der Prüfung Fehler oder Unregelmäßigkeiten bekannt, ist der Auftraggeber unverzüglich zu informieren.

## Der Auftragnehmer ist verpflichtet, soweit gesetzlich vorgeschrieben, einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 37, 38 DS-GVO ausüben kann, zu bestellen. Die Kontaktdaten des Datenschutzbeauftragten oder eines anderen Ansprechpartners für Datenschutzfragen - soweit ein Datenschutzbeauftragter nicht zu bestellen ist - werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

# Herausgabe von personenbezogenen Daten

## Der Auftragnehmer erkennt an, dass der Auftraggeber infolge seiner Rolle als Verantwortlicher jederzeit dazu berechtigt sein muss, vom Auftragnehmer die Herausgabe von personenbezogenen Daten zu verlangen. Der Auftragnehmer garantiert dem Auftraggeber daher, technische und organisatorische Maßnahmen getroffen zu haben, um den Herausgabeanspruch unverzüglich erfüllen zu können, und verzichtet darauf, etwaige Einwendungen und Einreden gegen den Herausgabeanspruch zu erheben.

## Der Herausgabeanspruch umfasst sämtliche personenbezogenen Daten, die der Auftragnehmer unter der Verantwortung des Auftraggebers verarbeitet, insbesondere vom Auftraggeber übermittelte personenbezogene Daten sowie personenbezogene Daten, die im Rahmen der Durchführung eines Leistungsvertrages verändert, entstanden oder geschaffen worden sind.

## Nach vom Auftraggeber in Schrift- oder Textform bestätigter erfolgreicher Herausgabe der personenbezogenen Daten sind diese unverzüglich von den Speichermedien des Auftragnehmers derart zu löschen, sodass diese nicht mehr reproduziert werden können. Der Auftragnehmer übernimmt die Garantie für eine entsprechende Löschung dieser personenbezogenen Daten auf Speichermedien seiner etwaigen Unterauftragnehmer. Der Auftragnehmer hat dem Auftraggeber auf Verlangen die Durchführung dieser Löschung durch geeignete Dokumente oder einer entsprechenden Versicherung nachzuweisen. Vorstehendes gilt entsprechend, wenn die Verarbeitung personenbezogener Daten durch den Auftragnehmer endet, der Auftraggeber gegenüber dem Auftragnehmer jedoch ausdrücklich auf die Herausgabe verzichtet, und keine einer Löschung entgegenstehende Vereinbarung getroffen wurde.

## Der Auftragnehmer darf bestimmte personenbezogene Daten anstelle ihrer Löschung in gesperrter Form speichern, solange und soweit der Auftragnehmer zwingenden gesetzlichen Bestimmungen unterliegt, die ihn zu einer Aufbewahrung verpflichten. Die Rechtmäßigkeit eines Zugriffs auf gesperrte Daten beurteilt sich nach der gesetzlichen Bestimmung, aufgrund derer die personenbezogenen Daten gesperrt werden mussten.

## Im Fall der Wegnahme oder der Pfändung eines Speichermediums durch einen Dritten, auf dem personenbezogene Daten des Auftraggebers gespeichert sind, oder bei Betreibung der Zwangsvollstreckung in ein solches Speichermedium durch einen Dritten, hat der Auftragnehmer sowohl den Dritten über den Umstand, dass sich personenbezogene Daten des Auftraggebers auf dem betroffenen Datenträger befinden, als auch den Auftraggeber über die entsprechende Maßnahme unverzüglich zu informieren. Etwaige Rechtsmittel des Auftraggebers gegen die Maßnahmen des Dritten bleiben unberührt.

# Kontrollrechte des Auftraggebers

## Der Auftraggeber hat während der Laufzeit dieser Vereinbarung bis zum Eintritt der allgemeinen Verjährung von Ansprüchen aus dieser Vereinbarung das Recht, Überprüfungen durchzuführen, oder im Einzelfall durch zur Verschwiegenheit verpflichtete Dritte bzw. Prüfer durchführen zu lassen. Der Auftraggeber hat insbesondere das Recht, sich durch Stichprobenkontrollen von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in seinem Geschäftsbetrieb zu den üblichen Geschäftszeiten zu überzeugen.

## Dies umfasst das Recht, das Grundstück, die Geschäftsräume und die Standorte der informationstechnischen Anlagen des Auftragnehmers zu betreten und dort Besichtigungen und Prüfungen vorzunehmen oder vornehmen zu lassen, sowie geschäftliche Unterlagen und gespeicherte Daten und Datenverarbeitungsprogramme einzusehen, soweit dies zur Auftragskontrolle erforderlich ist.

## Kontrollen sind in der Regel mit einer Vorlaufzeit von vierzehn (14) Tagen anzukündigen. In dringenden Fällen kann der Auftraggeber die Ankündigungsfrist auf 24 Stunden verkürzen; ein dringender Fall liegt insbesondere bei Inspektionen durch Datenschutzaufsichtsbehörden, sonstigen hoheitlichen Aufsichtsbehörden, oder bei eventuell meldepflichtigen Vorfällen vor.

# Pflichten des Auftraggebers

## Der Auftraggeber ist für die Einhaltung der auf ihn anwendbaren gesetzlichen Bestimmungen zum Schutz personenbezogener Daten verantwortlich.

## Der Auftraggeber wird den Auftragnehmer unverzüglich und vollständig informieren, wenn er bei Prüfung der Verarbeitungsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

## Dem Auftraggeber obliegt die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DS-GVO; die Verpflichtung des Auftragnehmers zur Führung eines eigenen Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO bleibt hiervon unberührt.

# Haftung

## Der Auftraggeber haftet dem Auftragnehmer unbeschränkt für die Verletzung datenschutzrechtlicher Pflichten eines Verantwortlichen i.S.d. Art. 4 Nr. 7 DS-GVO. Dies gilt nicht, wenn der Auftraggeber die Verletzungshandlung nicht zu vertreten hat.

## Gegenüber einer betroffenen Person haften Auftraggeber und Auftragnehmer nach Maßgabe des Art. 82 DS-GVO als Gesamtschuldner.

# Sonstige Bestimmungen

## Jede Änderung dieser Vereinbarung bedarf zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für einen Verzicht auf das Schriftformerfordernis selbst.

## Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

## Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung und datenschutzrelevanter Streitigkeiten aus Leistungsverträgen ist Köln.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Köln, 22.05.2018

Ort, Datum Ort, Datum

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 

Auftraggeber Auftragnehmer

# Anlage Gegenstand der Auftragsverarbeitung

**1. Gegenstand der Auftragsverarbeitung**

Versand von Printprodukten an Kunden

**2. Art und Zweck der Verarbeitung**

Versand

**3. Art der personenbezogenen Daten**

Folgende Datenarten / -kategorien sind Gegenstand der Auftragsverarbeitung:

* + Personenstammdaten

**4. Kategorien betroffener Personen**

Folgende Kategorien von Betroffenen sind von der Auftragsverarbeitung betroffen:

* + Kunden
	+ Abonnenten

...

#

# Anlage sicherheit der verarbeitung

1. **Pseudonymisierung und Verschlüsselung pers. Daten (Art. 32 Abs. 1 lit. a DS-GVO)**

**Pseudonymisierung**

Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen.

* Standardmäßig ist keine Pseudonymisierung vorgesehen oder erforderlich. Soweit erforderlich, werden Maßnahmen zur Pseudonymisierung mit dem Auftraggeber vereinbart.

**Verschlüsselung**

Einsatz von Verfahren und Algorithmen, die personenbezogene Daten mittels digitaler bzw. elektronischer Codes oder Schlüssel inhaltlich in eine nicht lesbare Form umwandeln. Es kommen symmetrische und asymmetrische Verschlüsselungstechniken in Betracht:

* Es werden Dienste bereitgestellt (sftp), die eine gesicherte und verschlüsselte Übermittlung von Kundendaten an SDK ermöglichen.
1. **Maßnahmen zur Sicherstellung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)**

**Zutrittskontrolle**

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere zur Legitimation der Berechtigten:

**Gebäudesicherung**

* Das Gebäude ist mit einer elektronischen Zutrittskontrolle mit Sicherheitsschlössern gesichert. Die Schließberechtigungen sind für verschiedene Mitarbeitergruppen ihren Tätigkeiten entsprechend festgelegt.
* Die Schließanlage zeichnet mittels Protokolldateien die Öffnung bzw. Schließung in jedem Schließzylinder der Zugangstüren auf. Die Schlüsselausgabe ist protokolliert.
* Die Außentür des Gebäudes ist Video überwacht.
* Die Alarmanlage ist an einen Wachdienst angebunden.
* Betriebsfremde Personen dürfen nur nach vorheriger Anmeldung die Firmenräumlichkeiten betreten und werden während ihres Aufenthalts von Mitarbeitern von SDK begleitet.
* Der Zutritt der Mitarbeiter wird außerdem durch ein Zeiterfassungssystem mit Chipkartenleser erfasst.

**Raumsicherung**

Zutritt IT-Administration

* Zutritt zur IT-Administration haben nur Mitarbeiter der Geschäfts- bzw. Betriebsleitung sowie Mitarbeiter des IT-Bereiches.

Zutritt Serverraum

* Die physischen Zutritte werden durch eine Remote-Administration reduziert.
* Der Serverraum ist verschlossen. Jeder Zutritt wird mittels der Protokolldateien der Schließanlage aufgezeichnet.
* Zutritt zum Serverraum haben nur definierte Mitarbeiter des IT-Bereiches.
* Nichtfirmenzugehörige Personen dürfen die Räume des Rechenzentrums nur in Begleitung eines berechtigten Mitarbeiters betreten.
* Die Server befinden sich in einem abgeschlossenen Serverschrank.

Zutritt Ausfallrechenzentrum

* Zur Datensicherung wird die virtuelle Serverarchitektur komplett an einen anderen, räumlich getrennten, Standort (Ausfallrechenzentrum) repliziert. Das Ausfallrechenzentrum befindet sich in einem Container auf dem Betriebsgelände Stolberger Str. 84, der räumlich vom Betriebsgebäude getrennt ist.
* Das Ausfallrechenzentrum ist als geschlossener Sicherheitsbereich konzipiert. Der Zutritt erfolgt über zwei hintereinander liegende Eisentüren, die jeweils mit einer elektronischen

Zutrittskontrolle mit Sicherheitsschlössern versehen sind. Beide sind mit der Alarmanlage gekoppelt.

* Die Unversehrtheit des Containers wird im Rahmen der Kontrollgänge des Sicherheitsdienstes kontrolliert.

**Zugangskontrolle**

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstamm­daten­satz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

**Zugang zu den Arbeitsplätzen**

Benutzer

* Mitarbeiter sind verpflichtet, sämtliche Informationen, IT-Systeme, Datenträger ausschließlich für geschäftliche Zwecke zu nutzen. Insbesondere ist den Mitarbeitern die Nutzung von Internet und E-Mail für private Zwecke nicht erlaubt.
* Jeder Arbeitsplatz wird durch einen zentral verwalteten On-Access-Virenscanner geschützt. Dadurch wird jeglicher Dateizugriff auf dem PC vom Virenscanner geprüft und überwacht.

Handhabung Passwörter

* Die Mitarbeiter sind dazu angehalten, verantwortungsbewusst mit Berechtigungen und Passwörtern umzugehen.
* Die Passwortlänge ist vorgeschrieben. Jeder Mitarbeiter benötigt ein 8-stelliges Kennwort.
* Das Passwort muss alle 90 Tage geändert werden.
* Nach sechs Fehlversuchen bei der Eingabe des Passwortes wird der betreffende Account gesperrt.

Zugang zur Serverstruktur

* Alle Serveradministrator-Kennwörter wurden nach den "Microsoft Kennwort-Komplexitätsvoraussetzungen" angelegt. Auf den Fileservern wurde ein zentral verwalteter Virenscanner installiert. Dadurch wird jeglicher Dateizugriff vom Virenscanner geprüft und überwacht.

Absicherung von Kunden-Zugängen

* Nichtfirmenangehörige (Kunden) stellen SDK Daten ausschließlich über gesicherte Verbindungen zur Verfügung.
* Diese Kundenzugänge sind passwortgeschützt.

Absicherung von Internet-Zugängen

* Der Zugang erfolgt ausschließlich über demilitarisierte Zonen (DMZ).
* Das gesamte Rechenzentrum - und damit das dahinterliegende Netzwerk - wird durch eine Firewall-Topologie geschützt.
* Der Gesamte E-Mail-Verkehr von SDK durchläuft ein zweistufiges Sicherheits-Konzept, wobei jede Stufe von einem anderen Hersteller kommt, um die Sicherheit zu erhöhen. Erst nach dieser zweistufigen Prüfung werden E-Mails an den Empfänger übertragen.
* Alle Fernzugriffe auf die Firmenserver werden nur über Virtual Private Network (VPN) zugelassen.

**Zugriffskontrolle**

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

* Mit den Regelungen eines restriktiven Berechtigungssystems wird sichergestellt, dass jeder Mitarbeiter ausschließlich aufgabenbezogen den Zugang zu Produktionssystemen und Daten erhält.
* Zugriffe auf Dateien in Filesystemen werden durch entsprechende Gruppenrechte eingeschränkt. Die Daten werden auf dem Fileserver Abteilungs- oder Arbeitsgruppenbezogen abgelegt bzw. organisiert, so dass die Nutzer in Abhängigkeit mit ihrem Tätigkeitsfeld eingeschränkte Benutzerrechte haben.
* Zugriffe sind über die Passwortregelungen (siehe Ziffer 2 Zugangskontrolle) gesichert.
* Bei serverbasierenden Anwendungen sind interne Berechtigungsschemata implementiert. Für diese Anwendungen vergeben definierte "Anwendungsadministratoren" die Berechtigungen.

**Trennungskontrolle**

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

* Die Daten verschiedener Auftraggeber werden getrennt aufbewahrt bzw. verarbeitet. Dies wird vor allem durch die aufgeführten Maßnahmen zur Zugriffskontrolle gewährleistet.
1. **Maßnahmen zur Sicherstellung der Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**

**Weitergabekontrolle**

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

* Alle Verfahren zur automatisierten Verarbeitung und Übermittlung personenbezogener Daten an Dritte werden in der Verfahrensübersicht erfasst.
* Abruf- und Übermittlungsprogramme (z. B. FTP, Firewall, Remote Access) werden dokumentiert.
* Weitere Maßnahmen wie VPN, Firewall siehe Ziffer 2 Zugangskontrolle.

**Eingabekontrolle**

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

* Im Rahmen einzelner Anwendungen, bei (außergewöhnlichen) Aktivitäten der Betriebssysteme sowie bei Überwachungseinrichtungen im Internet (Firewall, Content-Filter) erfolgt eine Protokollierung.

**4. Maßnahmen zur IT-Sicherheit**

Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 lit. b DS-GVO)

Maßnahmen zur Wiederherstellung der Verfügbarkeit und dem Zugang zu pers. Daten bei einem technischen Zwischenfall (Art. 32 lit. c DS-GVO)

**Verfügbarkeitskontrolle:**

**Wasserschutz und Brandschutz**

* Das Rechenzentrum liegt oberhalb des Grundwasserbereiches.
* Es existieren Feuerlöschgeräte im Gebäude (gemäß der Brandschutz-VO).

**Sichere Versorgung**

* Alle produktiven Server werden über eine unterbrechungsfreie Stromversorgung (USV) netzunabhängig versorgt. Die USV versorgt alle Server bei Stromausfall für ca. 30 Minuten mit Strom. Kehrt die reguläre Stromversorgung in dieser Zeit nicht zurück, werden die Server automatisch heruntergefahren.
* Der Serverraum ist klimatisiert. Eine 15KW Klimaanlage hält die Temperatur im Rechenzentrum konstant bei 21 Grad Celsius.
* Zu Maßnahmen zur Bestandssicherung siehe Ziffer 3 Zugriffskontrolle. Auf allen Servern werden täglich Veränderungsdaten gesichert. Am Wochenende wird eine Vollsicherung durchgeführt. Die Datensicherungsbänder werden in einem feuerfesten Tresor aufbewahrt, der in einem anderen Gebäudekomplex steht. Für eine Datenrücksicherung steht eine Bänderhistorie von ca. 6 Monaten zur Verfügung. Einmal pro Woche erfolgt zusätzlich ein Disk-to-Disk-Backup für virtualisierte Systeme.

**Ausfallrechenzentrum**

* Zur Datensicherung wird mehrmals täglich die virtuelle Serverarchitektur komplett an einen anderen, räumlich getrennten, Standort (Ausfallrechenzentrum) repliziert.
* Das Ausfallrechenzentrum ist klimatisiert. Jeder Raum ist mit einem Brandmelder ausgestattet, der an die Brandmeldezentrale angeschlossen ist.
* Das Ausfallrechenzentrum verfügt über einen eigenen Stromkreis. Bei Stromausfall erfolgt eine automatische Umschaltung auf ein Notstromaggregat, welches sich in einem separaten, abgeschlossenen Raum befindet.
* Der Innenraum des Containers, in dem sich das Ausfallsicherheitszentrum befindet, hat die Feuerschutzklasse F30.

**Virtualisierte Desktops**

* Die Mitarbeiterdesktops sind überwiegend virtualisiert.

**5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der technisch-organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d DS-GVO; Art 25. Abs. 1 DS-GVO)**

**Datenschutzmanagement**

* Mitarbeiter sind auf die Grundsätze der EU DS-GVO verpflichtet und über ihre Pflichten als Auftragnehmer unterrichtet.
* Es wird ein Datenschutz-Management-System eingesetzt.
* Es werden regelmäßig interne Audits durchgeführt.

**Datenschutzfreundliche Voreinstellungen (Privacy by Default)**

* Die Implementierung von Verfahren oder Systemen mit personenbezogenen Daten richtet sich grundsätzlich am Prinzip der Datensparsamkeit aus und wird durch den betrieblichen Datenschutzbeauftragten geprüft.

**Auftragskontrolle**

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

* Es werden Vereinbarungen zur Auftragsverarbeitung gem. den Anforderungen von Art. 28 EU DS-GVO ageschlossen.
* Wartungs- und Fernwartungsaktivitäten werden durch geeignetes Personal überwacht.