A Planon Company

AVV AUFTRAGSVERARBEITUNGS-VEREINBARUNG NACH ART. 28 ABS. 3 DSGVO

Gültig ab:	1.11.2024
Version:	v21.12
Vertragsgebiet:	Deutschland
Typ:	Auftragsverarbeitungsvereinbarung

AUFTRAGSVERARBEITUNGSVEREINBARUNG

nach Art. 28 Abs. 3 DSGVO

zwischen

COOR GmbH
Altlaufstraße 38
85635 Höhenkirchen-Siegertsbrunn
Deutschland
eingetragen beim Amtsgericht Frankfurt am Main unter HRB 194229 ("**COOR**")

und

eingetragen beim Amtsgericht unter HRB und/oder mit der D-U-N-S Nummer ("**Kunde**")

nachfolgend jeweils als "**Partei**" und zusammen als die "**Parteien**" bezeichnet

Die Parteien vereinbaren wie folgt:

Der Auftragnehmer verarbeitet personenbezogene Daten im Sinne von Art. 4 Nr. 2 DSGVO im Auftrag des Auftraggebers gemäß Art. 28 DSGVO auf Grundlage dieser Vereinbarung zur Auftragsverarbeitung („**Vereinbarung**").

Diese Vereinbarung gilt als Rahmenvertrag und findet auf alle Tätigkeiten Anwendung, die gemäß Leistungsbeschreibung mit dem Kunden eine Auftragsverarbeitung darstellen ("Auftragstätigkeiten"). Dies gilt auch, wenn die Leistungsbeschreibungen und/oder sonstigen vertraglichen Vereinbarungen nicht ausdrücklich auf diese Vereinbarung Bezug nehmen.

Die folgenden Anlagen sind Bestandteil dieser Vereinbarung:

I Bedingungen für die Auftragsverarbeitung
II TOM Technische und organisatorisch Maßnahmen zur Datensicherheit
III Beschreibung der betroffenen Personen, Kategorien von Daten und Verarbeitungstätigkeiten/ Verarbeitungsgegenstand, Dauer, Art und Zweck der Verarbeitung der personenbezogenen Daten
IV Vom Kunden genehmigte Unterauftragnehmer

Diese Vereinbarung tritt zum (i) , oder (ii) mit dem Datum der letzten Unterschrift (je nachdem, was früher der Fall ist) in Kraft ("**Inkrafttreten**").

COOR GmbH:		:	
Unterschrift:	_____	Unterschrift:	_____
Name & Titel:	_____	Name & Titel:	_____
Datum:	_____	Datum:	_____

ANLAGE I: AUFTRAGSVERARBEITUNGSVEREINBARUNG

Diese Vereinbarung zur Auftragsverarbeitung („**Vereinbarung**") regelt die Verarbeitung von Personenbezogenen Daten im Zusammenhang mit dem zwischen dem Kunden und COOR bestehenden Vertrag über die Nutzung der COOR-Software und/oder den Zugriff darauf und/oder damit im Zusammenhang stehende Leistungen sowie zu den sich darauf ggf. beziehenden Änderungsvereinbarungen.

1. BEGRIFFSBESTIMMUNGEN

Sofern in dieser Vereinbarung nicht anders bestimmt ist, haben die in dieser Vereinbarung verwendeten und ggf. mit großen Anfangsbuchstaben verstehenden Begriffe die folgende Bedeutung:

„Anlassfall" der Kunde hat auf Basis tatsächlicher Anhaltspunkte berechtigte Zweifel, dass Prüfberichte bzw. Zertifizierungen unzureichend oder unzutreffend sind oder es gibt besondere Vorfälle im Sinne von Art. 33 Abs. 1 DSGVO im Zusammenhang mit der Durchführung der Auftragsverarbeitung;

„COOR-Sicherheitsstandards" bezeichnet die Sicherheitsstandards in Anhang 1 zu dieser Vereinbarung;

„DSGVO" bezeichnet die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung Personenbezogener Daten und zum freien Datenverkehr);

„EWR" bezeichnet den Europäischen Wirtschaftsraum;

„Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (gemäß Art. 4 Nr. 1 DSGVO);

„Rechenzentrum" Zur Erfüllung der SaaS Leistungen nimmt COOR für Rechenzentrumsleistungen Unterauftragsverarbeiter im Sinne des Art. 28 DSGVO in Anspruch.

„Standardvertragsklauseln" bezeichnet die Standardvertragsklauseln des Beschlusses der Europäischen Kommission vom 04. Juni 2021 über Standardvertragsklauseln für die Übermittlung Personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.

„Verarbeitung" hat die in Art. 4 Nr. 2 DSGVO definierte Bedeutung;

2. AUFTRAGSVERARBEITUNG

2.1 Umfang und Funktionen der Parteien. Diese Vereinbarung gilt für die Verarbeitung Personenbezogener Daten durch COOR im Auftrag des Kunden. Der Kunde ist hierbei in Bezug auf die Personenbezogenen Daten der für die Verarbeitung **„Verantwortliche**" und COOR der „**Auftragsverarbeiter**" (Art. 4 Nr. 7 und 8 DSGVO).

2.2 Einhaltung gesetzlicher Vorschriften. Jede der Parteien hält im Rahmen der Durchführung dieser Vereinbarung die für sie geltenden und verbindlichen gesetzlichen Vorschriften, Bestimmungen und Regelungen ein, einschließlich aller gesetzlichen Vorgaben in Bezug auf den Datenschutz einschließlich DSGVO.

2.3 Weisungen für die Auftragsverarbeitung. COOR wird die Personenbezogenen Daten nach Maßgabe der dokumentierten, schriftlichen Weisungen des Kunden verarbeiten, wobei diese Verpflichtung auch im Hinblick auf die Übermittlung Personenbezogener Daten in ein Drittland gilt, sofern nach anwendbarem Recht nicht etwas anderes vorgeschrieben ist; in letzterem Fall teilt COOR dies dem Kunden vorher mit, sofern COOR dies rechtlich nicht untersagt ist. COOR teilt dem Kunden unverzüglich mit, falls COOR der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbe-stimmungen der Europäischen Union oder der EU-Mitgliedstaaten verstößt. In diesem Fall ist COOR berechtigt, die Verarbeitung einzustellen, bis der Kunde seine Weisung bestätigt hat. Der Kunde weist COOR hiermit an, die Personenbezogenen Daten so zu verarbeiten, wie dies für die Erbringung der Leistungen nach Maßgabe der Bestimmungen des Vertrags und dieser Vereinbarung erforderlich ist. Eine Verarbeitung außerhalb des Rahmens dieser Vereinbarung bedarf der vorherigen schriftlichen Vereinbarung zwischen COOR und dem Kunden über zusätzliche Anweisungen für die Verarbeitungstätigkeit einschließlich der Vereinbarung etwaiger weiterer Gebühren, die vom Kunden an COOR für die Durchführung der Anweisungen zu zahlen sind.

2.4 Zugang oder Nutzung. COOR wird die Personenbezogenen Daten im Rahmen der Auftragsverarbeitung nicht verarbeiten, soweit dies nicht für die Erbringung der Leistungen gegenüber dem Kunden erforderlich ist, es sei denn, COOR ist nach EU-Recht oder dem Recht eines EU-Mitgliedstaats, das auf COOR anwendbar ist, verpflichtet, Personenbezogene Daten anderweitig zu verarbeiten – auch in Bezug auf die Übermittlung an ein Drittland oder eine internationale Organisation; in letzterem Fall teilt COOR diese rechtlichen Anforderungen vor der Verarbeitung dem Kunden mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2.5 Vertragsgegenstand und Dauer der Verarbeitung. Vertragsgegenstand und Dauer der Verarbeitung der Personenbezogenen Daten ergeben sich aus Anhang 2 zu dieser Vereinbarung.

2.6 Art und Zweck der Verarbeitung. Art und Zweck der Verarbeitung der Personenbezogenen Daten ergeben sich aus Anhang 2 zu dieser Vereinbarung.

2.7 Beschreibung der betroffenen Personen, Kategorien von Daten und Verarbeitungstätigkeiten. Die betroffenen Personen, Kategorien von Personenbezogenen Daten und Verarbeitungstätigkeiten ergeben sich aus Anhang 2 zu dieser Vereinbarung. Die folgenden Arten von sensiblen Personenbezogenen Daten (einschließlich Bildern oder anderen Informationen, die solche sensiblen Daten enthalten oder offenbaren) dürfen nicht in der COOR Software verarbeitet werden:

- Informationen, die sich auf die körperliche oder geistige Gesundheit einer Person beziehen sowie Informationen, die sich auf die Bereitstellung oder Bezahlung von Gesundheitsleistungen beziehen;
- Personenbezogene Daten, die als besondere Kategorien im Sinne von Artikel 9 und Artikel 10 der DSGVO eingestuft sind.

2.8 Weitergabe. COOR wird keine Personenbezogenen Daten an Dritte weitergeben, soweit dies nicht zur Einhaltung dieser Vereinbarung, von EU-Recht oder dem Recht eines EU-Mitgliedstaats, das auf COOR anwendbar ist, erforderlich ist. Verlangen Vollstreckungsbehörden oder sonstige staatliche Dritte von COOR Personenbezogene Daten, so wird COOR versuchen, diese Stellen an den Kunden zu verweisen, damit diese die Daten unmittelbar beim Kunden anfordern. In diesem Rahmen ist COOR berechtigt, den Vollstreckungs-behörden bzw. sonstigen staatlichen Dritten die wesentlichen Kontaktdaten des Kunden zu übergeben. Ist die Weitergabe Personenbezogener Daten an einen Dritten (insbesondere auch an eine Vollstreckungsbehörde) rechtlich zwingend, so benachrichtigt COOR den Kunden über die rechtlichen Anforderungen vor der Weitergabe, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2.9 COOR-Mitarbeiter. COOR setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß Art. 28 Abs. 3 S. 3 lit. b) DSGVO auf die Vertraulichkeit verpflichtet worden sind und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. COOR und jede COOR unterstellte Person, die Zugang zu Personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Kunden und gemäß den COOR-Sicherheitsstandards verarbeiten. COOR legt den Mitarbeiten angemessene vertragliche Pflichten auf, einschließlich entsprechender Pflichten in Bezug auf die Vertraulichkeit. Die Verpflichtungen auf die Vertraulichkeit gelten auch nach Beendigung dieser Vereinbarung fort.

2.10 Standort vom Rechenzentren. Der Kunde erteilt COOR die allgemeine Genehmigung zur Erfüllung der SaaS Leistungen Unterauftragsverarbeiter im Sinne des im Sinne des Art. 28 DSGVO in Anspruch zu nehmen. Die jeweils aktuell eingesetzten Unterauftragsverarbeiter kann der Verantwortliche unter Anhang 2 einsehen. Der Standort des Rechenzentrums befindet sich im Gebiet der Bundesrepublik Deutschland, in Österreich, in einem anderen Mitgliedstaat der Europäischen Union, in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) oder in einem legitimierten Drittland gemäß Art. 44 ff. DSGVO.

2.11 Datenübermittlung in Drittländer ohne Angemessenheitsbeschluss. COOR verpflichtet sich mit Unterauftragsverarbeitern Standardvertragsklauseln abzuschließen in Fällen, in denen Verarbeitungstätigkeiten im Auftrag des Kunden eine Übermittlung Personenbezogener Daten in ein Land außerhalb des EWR beinhalten, für das kein gültiger Angemessenheitsbeschluss der Europäischen Kommission (Art. 45 DSGVO) besteht.

3. SICHERHEITSBEZOGENE VERANTWORTUNGSBEREICHE VON COOR

3.1 COOR trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der Personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Die Parteien vereinbaren die in Anlage 1 „Technische und organisatorische Maßnahmen" zu dieser Vereinbarung niedergelegten Datensicherheitsmaßnahmen (die COOR-Sicherheitsstandards).

3.2 COOR hat die sich aus den COOR-Sicherheitsstandards ergebenden Maßnahmen zur Aufrechterhaltung der Sicherheit der Leistungen durchgeführt und wird diese aufrechterhalten. COOR ist berechtigt, die COOR-

Sicherheitsstandards anzupassen, soweit das Schutzniveau der zum Vertragsschluss bestehenden COOR-Sicherheitsstandards nicht unterschritten wird.

3.3 COOR führt gemäß Artikel 30 Absatz 2 DSGVO ein Verzeichnis zu allen Kategorien der im Auftrag des Kunden vorgenommenen Verarbeitungstätigkeiten.

4. RECHTE UND PFLICHTEN DES KUNDEN

4.1 Der Kunde ist dafür verantwortlich, die COOR-Sicherheitsstandards in Bezug auf die Datensicherheit zu überprüfen und für sich selbst festzustellen, ob diese Leistungen seine Anforderungen erfüllen und einen angemessenen Schutz der Personenbezogenen Daten gewährleisten.

4.2 Der Kunde ist Verantwortlicher gemäß anwendbarem Datenschutzrecht und insbesondere dafür verantwortlich, die Betroffenen Personen über die Verarbeitung ihrer Daten nach dem Vertrag zu informieren, sowie geltend gemachte Betroffenenrechte zu erfüllen.

5. ZERTIFIZIERUNGEN

COOR's Unterauftragsverarbeiter (Anlage 2 / „Rechenzentrum") sind im Besitz eines gültigen ISO 27001 Zertifikats bzw. eines anderen Standards, der im Wesentlichen ISO 27001 entspricht und verpflichten sich zwecks Einführung, Durchführung, Kontrolle und Verbesserung der Sicherheitsstandards, ein Informationssicherheitsprogramm aufrecht zu erhalten, das die Anforderungen nach ISO 27001 bzw. eines anderen Standards erfüllt, der im Wesentlichen ISO 27001 entspricht.

6. AUDIT

Die Rechenzentren setzen zum Nachweis der Angemessenheit der Sicherheitsstandards und dieser Vereinbarung externe Prüfer ein. Diese Prüfung a) wird mindestens jährlich durchgeführt; b) wird nach ISO 27001 Standards oder diesen im Wesentlichen entsprechenden Standards durchgeführt; c) wird durch unabhängige Dritte im Sinne von Prüfungshandlung bei Zertifizierungsverfahren/-nachweisen durch Auditoren die keine technische Auditoren darstellen durchgeführt und d) ergibt einen vertraulichen Prüfbericht (**„Bericht"**); dieser stellt Vertrauliche Informationen des Rechenzentrum dar. Auf Verlangen und gegen Kostenersatz kann der Kunde in Mitwirkung von COOR die vollständigen Prüfunterlagen und Auditberichte im Rahmen einer Prüfhandlung einsehen. Die Einsichtnahme ist Vor-Ort oder per Zoom möglich, wobei keine Kopien angefertigt werden dürfen.

6.1 Eine Datenschutzkontrolle hat das Ziel, die Einhaltung der obliegenden Pflichten gemäß der DSGVO auf Grundlage dieses Vertrages zu überprüfen. Der Nachweis soll primär durch unabhängige Prüfberichte und Zertifizierungen erbracht werden. Im Anlassfall kann der Kunde Vor-Ort-Kontrollen durchführen. Sofern solche Vor-Ort-Kontrollen durchgeführt werden, sind diese als Stichprobenkontrollen der für die Durchführung der Auftragsverarbeitung relevanten Bereiche (vorbehaltlich der Mandantentrennung) auszugestalten.

6.2 COOR räumt dem Kunden das Recht ein, sich zu den üblichen Geschäftszeiten persönlich von der Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang alle 12 Monate oder im Anlassfall selbst zu überzeugen.

6.3 Der Kunde übt sein Prüfrecht aus, indem er COOR anweist, die Prüfung in der in dieser Ziffer beschriebenen Weise durchzuführen. Diese ist mindestens 30 Tage im Voraus abzustimmen, während der regulären Geschäftszeiten von COOR so durchzuführen, dass sie den Betriebsablauf nicht stört und bedingt die vorherige Unterzeichnung einer Geheimhaltungsvereinbarung des Prüfers.

6.4 COOR wird den Kunden bei der Durchführung von Kontrollen unterstützen und nach eigenem Ermessen an der vollständigen und zügigen Abwicklung mitwirken. Eine Unterstützung bei den Kontrollen durch COOR im Ausmaß von 4 Stunden ist eingerechnet. Für den Aufwand, der COOR für seine Mitwirkung an Kontrollen darüber hinaus entsteht, ist COOR berechtigt eine zusätzliche angemessene Vergütung zu verlangen. Der Kunde ist zur Zahlung dieser zusätzlichen Vergütung nur und erst dann verpflichtet, wenn er sich nach eigenem Ermessen schriftlich mit der Übernahme dieser Zahlungsverpflichtungen einverstanden erklärt hat. COOR ist erst dann verpflichtet, bei der Durchführung dieser zusätzlichen Prüfungen entsprechend mitzuwirken, wenn eine Einigung über etwaige zusätzliche Zahlungen erreicht wurde und COOR diese Zahlungen erhalten hat.

7. UNTERSTÜTZUNGSLEISTUNGEN

7.1 COOR wird den Kunden gegen Zahlung einer angemessenen Vergütung angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Pflicht zur Beantwortung von Anfragen in Ausübung der Betroffenenrechte betreffend Information, Auskunft, Berichtigung und Löschung, Einschränkung der Verarbeitung, Benachrichtigung, Datenübertragbarkeit, Widerspruch und automatisierte Entscheidungen unterstützen und unter Berücksichtigung der Art der Verarbeitung und der COOR zur Verfügung stehenden Informationen den Kunden bei der Einhaltung seiner Pflichten aus Artikel 32 bis 36 DSGVO in Bezug auf die Datensicherheit, die Meldung von Verletzungen des Schutzes von Personenbezogenen Daten, Datenschutz-Folgenabschätzungen und vorherige Konsultation von Aufsichtsbehörden, unterstützen, soweit dies jeweils für die von COOR durchgeführte Verarbeitungstätigkeit von Bedeutung ist.

7.2 Insbesondere meldet COOR entsprechend Artikel 33 Absatz 2 DSGVO dem Kunden Verletzungen des Schutzes Personenbezogener Daten unverzüglich nach Bekanntwerden. Die Pflicht zur Mitteilung gilt nicht als Anerkennung eines Verschuldens oder einer Haftung durch COOR.

7.3. Meldungen über etwaige Verletzungen des Schutzes Personenbezogener Daten werden an die in Anhang 2 zu dieser Vereinbarung genannten Ansprechpartner des Kunden auf die durch COOR gewählte Weise übermittelt, was auch E-Mail umfasst. Der Kunde ist allein dafür verantwortlich, dass die von ihm übergebenen Kontaktdaten richtig und aktuell sind.

8. UNTERAUFTRAGSVERARBEITER

8.1 **Genehmigte Unterauftragsverarbeiter.** COOR kann zur Erfüllung der vertraglichen Pflichten weitere Auftragsverarbeiter (**„Unterauftragsverarbeiter"**) einsetzen. Der Kunde erteilt hiermit seine Zustimmung zum Einsatz der in Anhang 3 aufgeführten Unterauftragsverarbeiter in der in dieser Ziffer beschriebenen Weise. Erweiterungen oder Änderungen an der Liste der Unterauftragsverarbeiter teilt COOR dem Kunden mit einer Frist von vier (4) Wochen vor der jeweiligen Änderung mit. Soweit der Kunde der Erweiterung oder Änderung innerhalb dieser Frist nicht widerspricht, gilt die aktualisierte Liste der Unterauftragsverarbeiter als vom Kunden genehmigt.

8.2 **Pflichten der Unterauftragsverarbeiter.** Beauftragt COOR einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten im Auftrag des Kunden, so sind dem Unterauftragsverarbeiter Datenschutzverpflichtungen entsprechend denen dieser Vereinbarung schriftlich aufzuerlegen. Die Verantwortung für die Einhaltung der Pflichten aus dieser Vereinbarung sowie für etwaige Handlungen oder Unterlassungen eines Unterauftragsverarbeiter, aufgrund derer Pflichten aus dieser Vereinbarung verletzt werden, verbleibt bei COOR.

9. VERTRAULICHE INFORMATIONEN

9.1 Die Parteien verpflichten sich, über alle ihnen im Rahmen der Vorbereitung, Durchführung und Erfüllung dieser Vereinbarung oder einer Leistungsvereinbarung zur Kenntnis gelangten, geschützten oder vertraulichen Informationen und Daten, insbesondere der Betriebs- und Geschäftsgeheimnisse der jeweils anderen Partei Stillschweigen zu bewahren.

9.2 Geschützte oder vertrauliche Informationen im Sinne dieser Vereinbarung oder einer COF sind sämtliche Informationen, die

a. seitens einer Partei ausdrücklich und schriftlich als vertraulich bezeichnet wurden;

b. zu den nach dem GeschGehG geschützten Informationen gehören, insbesondere Know-how;

c. durch gewerbliche und andere Schutzrechte geschützt sind, z.B. Entwurfsmaterial für Software (vgl. § 69a Abs. 1 UrhG); oder

d. bei denen sich das Geheimhaltungsinteresse der offenbarenden Partei aus der Natur der Information ergibt, namentlich Konzepte, Geschäftspläne, Muster, Verfahren, Formeln, Prozesse, Methoden, Techniken und Ideen, Produkt- und Programmspezifikationen, Software Dokumentation, Zeichnungen, Verkaufs- und Marketingdaten bzw. Marketingpläne, Informationen über Preisgestaltung und Kosten, Informationen über Lieferanten und Geschäftsbeziehungen sowie sonstige Betriebs- und Geschäftsgeheimnisse.

9.3 Die Einbeziehung von Informationen unter die geschützten oder vertraulichen Informationen nach Ziffer 9.2 endet, wenn in Bezug auf die geschützten oder vertraulichen Informationen ganz oder zum Teil nachweislich Folgendes gilt:

a. sie waren der sie empfangenden Partei vor der Übermittlung bereits bekannt oder

b. sie waren vor der Mitteilung bereits öffentlich bekannt oder

c. sie wurden nach Mitteilung ohne Mitwirkung der empfangenden Partei sowie unabhängig von einem etwaigen Versäumnis der empfangenden Partei öffentlich bekannt oder

d. sie sind der empfangenden Partei durch einen Dritten bekannt gemacht worden, der keiner direkten oder indirekten Geheimhaltungsverpflichtung gegenüber der jeweils anderen Vertragspartei unterliegt.

9.4 Der Nachweis des Vorliegens einer dieser Ausnahmen ist von derjenigen Partei zu führen, die sich auf die Ausnahme beruft.

9.5 Die Parteien verpflichten sich, die geschützten oder vertraulichen Informationen vor dem unberechtigten Zugriff Dritter zu schützen und nicht ohne vorherige schriftliche Zustimmung des offenbarenden Vertragspartners Dritten mittelbar oder unmittelbar zugänglich zu machen, es sei denn es besteht eine Verpflichtung zur gerichtlichen Offenlegung. Die Parteien verpflichten sich darüber hinaus, die ihnen überlassenen geschützten oder vertraulichen Informationen ausschließlich zu dem vereinbarten Zweck zu nutzen.

9.6 Die Parteien werden die geschützten oder vertraulichen Informationen der jeweils anderen Partei nur denjenigen Mitarbeitern zugänglich machen, die von ihnen Kenntnis nehmen müssen, um diese Vereinbarung oder eine Leistungsvereinbarung zu erfüllen. Dies gilt auch, wenn diese Mitarbeiter bei einem Verbundenen Unternehmen der Parteien angestellt sind. Die Parteien werden den sachlich begrenzten Personenkreis, der im Rahmen der Zusammenarbeit mit den geschützten oder vertraulichen Informationen in Berührung kommt, vor der Weitergabe dieser Informationen an diesen Personenkreis zu Bedingungen zur Geheimhaltung verpflichten.

9.7 Die Geheimhaltungsverpflichtung gilt auch für 3 Jahre über die Beendigung dieser Vereinbarung hinaus.

10. HAFTUNG

10.1 COOR haftet unbeschränkt bei Vorsatz, grober Fahrlässigkeit, bei der Verletzung des Lebens, des Körpers, der Gesundheit oder soweit das Produkthaftungsgesetz zur Anwendung kommt.

10.2 Im Übrigen haften COOR und der Kunde einander für von ihnen zu vertretende Schäden wie folgt: Bei einer leicht fahrlässig verursachten Verletzung wesentlicher Vertragspflichten haftet COOR außer in den Fällen der Ziffer 10.1 der Höhe nach begrenzt auf den vertragstypisch vorhersehbaren Schaden, wobei sich COOR´s maximale Haftung auf einen Betrag in Höhe der in den zwölf Monaten vor dem betreffenden Vorfall gezahlten Gebühren beschränkt ist. Wesentliche Vertragspflichten sind abstrakt solche Pflichten, deren Erfüllung die ordnungsgemäße Durchführung eines Vertrages überhaupt erst ermöglicht und auf deren Einhaltung die Vertragsparteien regelmäßig vertrauen dürfen, wobei eine Verletzung einer wesentlichen Vertragspflicht nicht vorliegt, soweit der Schaden durch die korrekte Umsetzung der beauftragten Leistung oder einer vom Kunden erteilten Weisung entstanden ist.

10.3 Im Übrigen ist eine Haftung COORs ausgeschlossen.

10.4 COOR haftet nicht für Ansprüche aus entgangenem Gewinn.

10.5 Ferner übernimmt COOR keine Haftung für Schäden, die aus dem Verfälschen oder unbefugtem Gebrauch der Software durch den Kunden oder durch Dritte entstehen, die für den Kunden die Software nutzen, es sei denn, diese Schäden beruhen auf Vorsatz oder grober Fahrlässigkeit von Personen, deren Verhalten sich COOR zurechnen lassen muss.

10.6 Insbesondere haftet der Kunde nach Art. 82 DSGVO für diejenigen Schäden, die aus einer nicht den Bestimmungen der DSGVO entsprechenden Verarbeitung resultieren.

11. WIDERSPRÜCHE

11.1 Soweit nicht durch diese Vereinbarung geändert oder ergänzt, bleibt der Vertrag unverändert wirksam. Im Falle eines Widerspruchs zwischen dem Vertrag und dieser Vereinbarung in Bezug auf den Gegenstand dieser Vereinbarung haben die Bestimmungen dieser Vereinbarung Vorrang.

12. DAUER DER VEREINBARUNG

12.1 Die Parteien können die Vereinbarung jederzeit ohne Einhaltung einer Frist außerordentlich kündigen, insbesondere wenn ein schwerwiegender Verstoß der anderen Partei gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, COOR eine Weisung des Kunden nicht ausführen kann oder will oder COOR die Kontrollrechte des Kunden vertragswidrig verweigert.

13. LÖSCHUNG VON DATEN

13.1 Sofern COOR im Rahmen dieser Vereinbarung Personenbezogene Daten des Kunden erhalten hat, wird COOR nach Wahl des Kunden, alle Personenbezogenen Daten des Kunden nach dem Ende der Diensterbringung oder auf schriftliches Verlangen des Kunden jederzeit löschen oder an den Kunden zurückgeben, soweit nicht EU-Recht oder das Recht eines EU-Mitgliedstaats COOR dazu verpflichtet oder berechtigt, solche Personenbezogenen Daten aufzubewahren.

13.2 Sofern der Kunde keine anderweitige Weisung erteilt, stellt COOR dem Kunden mit Ablauf oder Beendigung des Vertrages eine maschinenlesbare Sicherungskopie als verschlüsselten Download zur Verfügung. Der Kunde hat 2 Monate nach Beendigung des Vertrages Zeit, diese Sicherungskopie herunterzuladen. Nach Ablauf der 2 Monate, wird COOR die Sicherungskopie vernichten und auf Wunsch eine Löschungsbestätigung senden.

ANHANG 1 ZU ANLAGE IV:
COOR TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUR DATENSICHERHEIT

Die in diesem Anhang 1 und unter dem folgenden Link detailliert beschriebenen TOM = Technischen und Organisatorischen Maßnahmen werden als verbindlich festgelegt, um die Verarbeitung der Personenbezogenen Daten im Einklang mit Anforderungen der gesetzlichen Datenschutzvorschriften vorzunehmen und den Schutz der Rechte der Betroffenen zu gewährleisten:

https://www.coor.info/datensicherheit > TOM

Die Technischen und Organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es COOR gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

1. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

COOR sorgt für Technische und Organisatorische Maßnahmen (einschließlich interner Richtlinien) zur a) Absicherung Personenbezogener Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem unberechtigten Zugang oder der unberechtigten Weitergabe, b) Feststellung vernünftigerweise vorhersehbarer interner Sicherheitsrisiken und unberechtigter Versuche des Zugangs zu Personenbezogenen Daten und c) Eingrenzung von Sicherheitsrisiken, insbesondere auch durch Risikoeinschätzung und regelmäßige Überprüfungen. Die Maßnahmen gliedern sich wie folgt:

1.1 Zugangskontrolle. Die Mitarbeiter und Auftragnehmer von COOR sowie sonstige zur Durchführung der Leistungen berechtigte Personen können auf die Personenbezogenen Daten nur im Rahmen und Umfang ihrer Zugriffsberechtigung (Erlaubnis) zugreifen. Alle Dienste sind mit einem Login und einem Passwort gesichert.

1.2 Netzwerksicherheit. Die Infrastruktur von COOR wird den Mitarbeitern und Auftragnehmern von COOR sowie sonstigen Personen insoweit zugänglich sein, wie dies für die Durchführung der Leistungen erforderlich ist. COOR sorgt für die Zugangskontrolle sowie Zugangsregelungen zur Steuerung, welcher Zugriff auf die Infrastruktur von der jeweiligen Netzwerkanbindung und dem jeweiligen Nutzer zulässig ist, insbesondere auch durch Einsatz von Firewalls oder funktional gleichwertiger Technologien. COOR sorgt für Korrekturmaßnahmen und Reaktionspläne zur Reaktion auf mögliche Sicherheitsbedrohungen.

1.3 Personal. Mitarbeiter von COOR, die Zugang zu den Personenbezogenen Daten haben, müssen eine Vertraulichkeitsvereinbarung unterzeichnen; die Teilnahme an regelmäßigen Themenschulungen ist für sie Pflicht.

1.4 Zuliefererbeziehungen. COOR kontrolliert relevante Zulieferer durch Überprüfung der von ihnen bereitgestellten Prüfberichte. Wenn COOR dies für erforderlich hält, werden auch andere Methoden zur Kontrolle eingesetzt. Bei Nichteinhaltung wird der Zulieferer von COOR angesprochen, damit das Problem aufgegriffen und eine Lösung gefunden wird.

1.5 Notfallwiederherstellung. COOR sorgt für die bereitgestellte Cloud-Lösung für einen Notfallwiederherstellungsplan in der Weise, dass mögliche Ausfallzeiten für den Kunden eingeschränkt werden.

2. LAUFENDE EVALUIERUNG

COOR führt regelmäßige Überprüfungen der Sicherheit seiner Infrastruktur durch, die für die Datenkategorie angemessen ist.

3. AUFGABEN DES KUNDEN

Der Kunde ist für die Nutzung der von COOR bereitgestellten Anwendung(en) verantwortlich. Dies umfasst insbesondere auch die Nutzung der Cloud-Geräte, mit denen der Kunde die Anwendung(en) wiederherstellen, neu starten oder aufrüsten kann, sowie den Zugang zu Anwendungen unter Verwendung der von COOR bereitgestellten Zugriffsarten.

4. DATENGEHEIMNIS

COOR hat die mit der Verarbeitung von Personenbezogenen Daten betrauten Mitarbeiter schriftlich dazu zu verpflichten, Personenbezogene Daten streng vertraulich zu behandeln und diese für keine anderen Zwecke als die Erbringung der Leistungen gegenüber dem Kunden zu verwenden. COOR weist die Mitarbeiter außerdem in die entsprechenden Datenschutzvorschriften ein.

5. MELDUNG VON DATENSCHUTZVERLETZUNGEN

Der Auftragsverarbeiter informiert den für die Verantwortlichen über Verstöße gegen den Schutz Personenbezogener Daten und stellt mindestens die folgenden Informationen zur Verfügung:

- Eine Beschreibung der Art der Verletzung, der betroffenen Kategorien und wenn möglich die ungefähren Anzahl der betroffenen Personen und Datensätze;
- Name und Kontaktdaten eines Ansprechpartners für weitere Informationen;
- Eine Beschreibung der wahrscheinlichen Folgen des Verstoßes;
- Eine Beschreibung der Maßnahmen, die ergriffen wurden, um den Verstoß zu beheben oder abzumildern.

ANHANG 2 ZU ANLAGE IV
BESCHREIBUNG DER BETROFFENEN PERSONEN, KATEGORIEN VON DATEN UND VERARBEITUNGSTÄTIGKEITEN / VERARBEITUNGSGEGENSTAND, DAUER, ART UND ZWECK DER VERARBEITUNG DER PERSONENBEZOGENEN DATEN

BETROFFENE PERSONEN

Betroffene Personen sind

▪ Kunden und Interessenten des Verantwortlichen (Kunden) sowie deren Mitarbeiter
▪ Lieferanten, Subunternehmer, Dienstleister und Kooperationspartner des Verantwortlichen (Kunden) sowie deren Mitarbeiter
▪ COOR User
▪ Beschäftigte des Verantwortlichen (Kunden)

Gegebenenfalls sind weitere Betroffene Personen vom Verantwortlichen (Kunden) zusätzlich vorzugeben und zwischen COOR und dem Kunden schriftlich zu vereinbaren.

KATEGORIEN VON DATEN

Die Personenbezogenen Daten von Personen, die vom Kunden zu dem Dienst hochgeladen werden und/oder von COOR und/oder einem Unterauftragsverarbeiter nach dem Vertrag verarbeitet werden:

▪ Personenstammdaten (Vorname, Nachname, Geschlecht, …)
▪ Adressdaten
▪ Kommunikationsdaten (Telefon, E-Mail Adresse, …)
▪ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
▪ Vertragsabrechnungs- und Zahlungsdaten
▪ Planungs- und Steuerungsdaten

Gegebenenfalls sind weitere Kategorien vom Kunden zusätzlich vorzugeben und zwischen COOR und dem Kunden schriftlich zu vereinbaren.

VERARBEITUNG

Verarbeitung gemäß der in dem Vertrag vereinbarten Leistungen.

VERARBEITUNGSGENSTAND, DAUER, ART UND ZWECK DER VERARBEITUNG DER PERSONENBEZOGENEN DATEN

Verarbeitungsgegenstand:
Der Verarbeitungsgegenstand ergibt sich aus dem Vertrag samt seinen Anlagen.

Dauer, Art und Zweck der Verarbeitung der Personenbezogenen Daten:
Die Dauer der Verarbeitung ergibt sich aus der COF, dem Vertrag und seinen Anlagen. Art und Zweck der Verarbeitung bestehen in der Bereitstellung der Software-as-a-Service-Plattform und ergeben sich detaillierter aus der COF, dem Vertrag und seinen Anlagen, inklusive den entsprechenden Leistungsbeschreibungen.

Kontaktdaten des Auftragsverarbeiters (COOR):

Kontakt für datenschutzrelevante Themen:

Zertifizierte Datenschutzbeauftragte:	Anita Obermair
E-Mail:	datenschutz@coor.info
Telefon:	+43 (0)662 452277

Kontaktdaten beim Verantwortlichen (Kunden)

Zuständiger:	
(Sofern vorhanden) Datenschutzbeauftragte:	
E-Mail:	
Telefon:	

Meldung von Datenschutzverstößen geht an:

Telefon:	
E-Mail: *)	

***) Sofern die E-Mail Adresse nicht ausgefüllt ist, gilt die E-Mail Adresse auf dem Bestellformular / OF.**

Weisungsberechtigte Personen des Verantwortlichen (Kunden):

Weisungsberechtigte Person	Funktion im Unternehmen	Anschrift/Kontakt

ANHANG 3 ZUR ANLAGE IV
VOM KUNDEN GENEHMIGTE UNTERAUFTRAGSVERARBEITER

Als vorab genehmigte Unterauftragsverarbeiter gelten die zum Zeitpunkt des Vertragsschlusses unter
https://www.coor.info/datensicherheit > WEITERE AUFTRAGSVERARBEITER
gelisteten Unternehmen.