Vereinbarung zum Datenschutz

zwischen

_____
_____
_____
_____

(im Folgenden Auftraggeberin genannt)

und der

HEUBECK AG
Gustav-Heinemann-Ufer 72a
50968 Köln,

(im Folgenden Auftragnehmerin genannt)

Präambel

Die Auftragnehmerin erbringt für die Auftraggeberin auf Grundlage eines Dienstleistungsvertrages oder einzelner Beauftragungen Beratungs- und Dienstleistungen in Zusammenhang mit der betrieblichen Altersversorgung bzw. Altersvorsorge der Auftraggeberin. Um ihre Dienstleistungen erbringen zu können, benötigt die Auftragnehmerin personenbezogene Daten, die ihr von der Auftraggeberin im Rahmen einer Auftragsverarbeitung zur Verfügung gestellt werden.

Diese Vereinbarung konkretisiert die aus dieser Auftragsverarbeitung resultierenden datenschutzrechtlichen Rechte und Pflichten der Auftraggeberin und der Auftragnehmerin.

§ 1
Datenschutzrechtliche Stellung der Vertragsparteien

(1) Die Auftraggeberin ist im Rahmen dieser Auftragsverarbeitung Verantwortliche im Sinne des Art. 24 EU-DS-GVO.

(2) Die Auftragnehmerin ist im Rahmen dieser Auftragsverarbeitung Auftragsverarbeiter im Sinne des Art. 28 EU-DS-GVO.

§ 2
Konkretisierung des Auftragsdatenverhältnisses

(1) Die Daten werden ausschließlich zur Erstellung der im Hauptvertrag oder in der jeweiligen Beauftragung aufgeführten Dienstleistungen genutzt bzw. verarbeitet.

(2) Die von der Auftragsverarbeitung betroffenen Daten, der betroffene Personenkreis sowie die Empfänger der Daten werden in der Anlage zu diesem Vertrag aufgeführt.

(3) Die Dauer der Auftragsverarbeitung richtet sich nach der Dauer des Hauptvertrages bzw. der jeweiligen Beauftragung.

(4) Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung der Auftraggeberin und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. EU-DS-GVO erfüllt sind.

§ 3
Technisch-organisatorische Maßnahmen

(1) Die Auftragnehmerin gestaltet in ihrem Verantwortungsbereich die innerbetriebliche Organisation so aus, dass sie den besonderen Anforderungen des Datenschutzes, insbesondere der Art. 28 bis Art. 32 EU-DS-GVO gerecht wird. Sie trifft und dokumentiert die hinsichtlich der konkreten Auftragsdurchführung erforderlichen technischen und organisatorischen Maßnahmen und wird die Dokumentationen der Auftraggeberin vor Beginn der Verarbeitung zur Prüfung zur Verfügung stellen. Bei Akzeptanz durch die Auftraggeberin werden die in der Anlage zu diesem Vertrag dokumentierten Maßnahmen Grundlage des Auftrags. Bei

einem festgestellten Anpassungsbedarf werden die Parteien diesen einvernehmlich umsetzen.

(2) Bei den zu treffenden Maßnahmen handelt es sich um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit der Daten sowie der Belastbarkeit der Systeme. Dabei berücksichtigt die Auftragnehmerin den Stand der Technik, die Implementierungskosten und die Art, den Umfang und den Zweck der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen im Sinne des Art. 32 Abs. 1 EU-DS-GVO.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmerin ist es insoweit gestattet, alternative, adäquate Maßnahmen umzusetzen, soweit das vereinbarte Schutzniveau hierdurch nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

(4) Die Auftragnehmerin stellt der Auftraggeberin die für die Erstellung der Verfahrensverzeichnisse erforderlichen Angaben zur Verfügung und führt selbst ein solches Verzeichnis.

§ 4
Pflichten der Auftragnehmerin

(1) Die Auftragnehmerin und die der Auftragnehmerin unterstellten Personen dürfen die Daten nur im Rahmen der Weisungen der Auftraggeberin erheben, nutzen oder verarbeiten. Die Auftragnehmerin verwendet die Daten nicht für andere als in dem Vertrag vereinbarte Zwecke und ist insbesondere nicht berechtigt, die Daten an Dritte weiterzugeben, es sei denn, sie ist gesetzlich hierzu verpflichtet.

(2) Die Auftragnehmerin stellt sicher, dass die mit der Verarbeitung der Daten befassten Mitarbeiter auf die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 Buchst. b), 29, 32 Abs. 4 EU-DS-GVO verpflichtet sind und in die Schutzbestimmungen der relevanten Datenschutzbestimmungen eingewiesen sind.

(3) Auf Anforderung unterstützt die Auftragnehmerin die Auftraggeberin bei der Einhaltung der in Art. 12 bis 23 EU-DS-GVO enthaltenen Pflichten. Die Auftraggeberin erstattet der Auftragnehmerin die hieraus entstehenden Kosten.

(4) Die Auftragnehmerin stellt sicher, dass die in diesem Vertrage festgelegten technisch-organisatorischen Maßnahmen gemäß Art. 32 bis 36 EU-DS-GVO umgesetzt werden.

(5) Die Auftragnehmerin hat einen betrieblichen Datenschutzbeauftragten bestellt, der seine Tätigkeit gemäß der Art. 38 und 39 EU-DS-GVO ausübt. Die Kontaktdaten des Datenschutzbeauftragten werden der Auftraggeberin zum Zweck der direkten Kontaktaufnahme benannt.

(6) Die Auftragnehmerin kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen im Hinblick darauf, dass diese im Einklang mit den Anforderungen des geltenden Datenschutzrechtes erfolgen und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

(7) Die Auftragnehmerin unterrichtet die Auftraggeberin unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder bei anderen Unregelmäßigkeiten bei der Verarbeitung der Daten der Auftraggeberin oder bei Verstößen gegen die in diesem Auftrag getroffenen Bestimmungen. Sie informiert die Auftraggeberin über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf den Auftrag beziehen.

§ 5
Pflichten der Auftraggeberin

(1) Die Auftraggeberin ist bezüglich der zu verarbeitenden Daten für die Einhaltung der für sie einschlägigen Datenschutzgesetze verantwortlich im Sinne des Art. 24 EU-DS-GVO.

(2) Die Auftraggeberin informiert die Auftragnehmerin unverzüglich über Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen, die sie bei der Prüfung der Auftragsergebnisse feststellt.

(3) Der Auftraggeberin obliegen die sich aus Art. 12 bis 23 EU-DS-GVO und Art. 32 bis 36 EU-DS-GVO resultierenden Pflichten.

(4) Die Auftraggeberin behandelt alle im Rahmen des Auftragsverhältnisses erlangten Kenntnisse von Datensicherungsmaßnahmen der Auftragnehmerin vertraulich.

(5) Die Auftraggeberin trägt die Verantwortung für das Löschen der nicht mehr benötigten Daten und erteilt entsprechende Weisungen.

§ 6
Weisungsbefugnis der Auftraggeberin

(1) Die Auftraggeberin kann das ihr im Rahmen dieses Auftragsverhältnisses zustehende Weisungsrecht durch Einzelweisungen konkretisieren. Verfahrensänderungen sind mit der Auftragnehmerin abzustimmen und zu dokumentieren.

(2) Auskünfte an Dritte oder Betroffene darf die Auftragnehmerin nur mit vorheriger Zustimmung der Auftraggeberin erteilen.

(3) Mündliche Weisungen bestätigt die Auftraggeberin auf Wunsch der Auftragnehmerin schriftlich oder per E-Mail.

(4) Die Auftragnehmerin informiert die Auftraggeberin unverzüglich, wenn sie der Meinung ist, dass eine Weisung gegen Datenschutzvorschriften verstößt. Die Auftragnehmerin ist berechtigt, die Umsetzung der Weisung so lange auszusetzen, bis sie durch die Auftraggeberin bestätigt oder geändert wird.

§ 7
Kontrollrechte der Auftraggeberin

(1) Die Auftraggeberin hat das Recht, die nach Art. 28 EU-DS-GVO vorgesehene Auftragskontrolle im Benehmen mit der Auftragnehmerin durchzuführen oder durch einen von ihr zu benennenden Prüfer durchführen zu lassen. Die Auftraggeberin kann sich daher vor Beginn und sodann regelmäßig von der Angemessenheit der getroffenen technischen und organisatorischen Maßnahmen zur Einhaltung der datenschutzrechtlichen Bestimmungen überzeugen. Hierzu weist die Auftragnehmerin der Auftraggeberin die getroffenen Maßnahmen nach. Die Auftraggeberin kann sich, in der Regel nach Anmeldung, während der üblichen Geschäftszeiten und ohne Störung der Betriebsabläufe von den getroffenen Maßnahmen persönlich überzeugen. Sie kann für diese Prüfung auch Dritte einschalten. Die Auftragnehmerin kann für die Ermöglichung von Kontrollen durch die Auftraggeberin einen Vergütungsanspruch geltend machen.

(2) Die Auftragnehmerin erteilt der Auftraggeberin alle zur Durchführung einer Auftragskontrolle nach Art. 28 EU-DS-GVO erforderlichen Informationen und Auskünfte.

§ 8
Subunternehmer

(1) Die Auftragnehmerin ist nur mit Zustimmung der Auftraggeberin berechtigt, zur Erfüllung ihrer vereinbarten Leistungen Subunternehmer zu beauftragen. Die Zustimmung zu den in der Anlage zu diesem Vertrag aufgeführten Subunternehmen gilt als erteilt.

(2) Die Auftragnehmerin ist verpflichtet, bei Auftragserteilung an Subunternehmer ihre Pflichten aus diesen Auftragsverhältnis, insbesondere die Anforderungen an die Vertraulichkeit, den Datenschutz und die Datensicherheit dem Subunternehmer zu übertragen und dies der Auftraggeberin nachzuweisen.

(3) Keine Unterauftragsverhältnisse im Sinne der Absätze 1 bis 3 sind solche Dienstleistungen, die Dritte als Nebenleistungen zur Unterstützung der Auftragsdurchführung bei der Auftragnehmerin erbringen. Hierzu zählen z.B. Telekommunikationsdienstleistungen, Wartung und Benutzerservice, Reinigungskräfte oder die Entsorgung von Datenträgern. Die Auftragnehmerin ist jedoch verpflichtet, auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

§ 9
Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate personenbezogener Daten werden nur dann hergestellt, wenn sie zu Auftragsdurchführung oder zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung (z.B. Erstellung von Sicherheitskopien) erforderlich sind.

(2) Die Auftragnehmerin wird personenbezogene Daten nur nach Weisung der Auftraggeberin löschen bzw. deren Verarbeitung einschränken. Nach Beendigung des Hauptvertrages hat die Auftragnehmerin sämtliche in ihrem Besitz befindliche personenbezogenen Daten herauszugeben, deren Verarbeitung einzuschränken oder datenschutzgerecht zu löschen, soweit keine gesetzlichen Aufbewahrungspflichten bestehen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch die Auftragnehmerin entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 10
Haftung

(1) Für Schäden, die ein Betroffener durch eine Verletzung datenschutzrechtlicher Bestimmungen durch eine der Vertragsparteien erleidet, haften die Vertragsparteien dem Betroffenen gegenüber gesamtschuldnerisch.

(2) Im Innenverhältnis zueinander ersetzt diejenige Partei, die die Verletzung der datenschutzrechtlichen Bestimmungen zu vertreten hat, der anderen Partei den durch die Inanspruchnahme entstandenen Schaden.

(3) Im Übrigen gelten im Rahmen dieses Vertrages die Haftungsbestimmungen des dieser Auftragsverarbeitung zugrundeliegenden Hauptvertrages bzw. des jeweiligen Auftrages.

§ 11
Schlussbestimmungen

(1) Dieser Vertrag beginnt und endet mit dem Hauptvertrag, bzw. mit der Mitteilung der Auftraggeberin, dass keine weiteren Beauftragungen mehr erfolgen.

(2) Änderungen und Ergänzungen dieser Vereinbarung können nur einvernehmlich vorgenommen werden und bedürfen der Schriftform.

(3) Falls einzelne Regelungen dieser Vereinbarung unwirksam sein oder werden sollten, wird die Wirksamkeit der übrigen Regelungen hierdurch nicht berührt. Die unwirksame Regelung ist durch eine gültige zu ersetzen, die dem ursprünglich Gewollten möglichst nahekommt.

(4) Erfüllungsort ist Köln. Ausschließlicher Gerichtsstand für alle Auseinandersetzungen aus und im Zusammenhang mit der Vereinbarung ist das Landgericht Köln, sofern gesetzlich nicht zwingend ein anderer ausschließlicher Gerichtsstand angeordnet wird.

	Köln,
Ort, Datum	Ort, Datum
(Firma)	HEUBECK AG

Anhang: Technische und organisatorische Maßnahmen