BGHM
Berufsgenossenschaft
Holz und Metall

Ihre gesetzliche Unfallversicherung

Vereinbarung

über die Verarbeitung personenbezogener Daten im Auftrag

gem. § 80 Sozialgesetzbuch Zehntes Buch (SGB X)

i.V.m. Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen

der Berufsgenossenschaft Holz und Metall (BGHM),

Isaac-Fulda-Allee 18, 55124 Mainz,

- Auftraggeberin -

nachstehend Verantwortliche genannt

und

xxx

- Auftragnehmerin -

nachstehend Auftragsverarbeiter genannt

wird zur Gewährleistung des Datenschutzes und der Datensicherheit im Rahmen des § 80 Sozialgesetzbuch Zehntes Buch (SGB X) i.V. mit Art. 28 Datenschutz-Grundverordnung (DSGVO) Folgendes vereinbart:

Inhaltsverzeichnis

§ 1 Gegenstand und Dauer der Datenschutzvereinbarung 3

§ 2 Verantwortlichkeit 3

§ 3 Zweckbestimmung 3

§ 4 Leistungsort 3

§ 5 Unterweisung und Verpflichtung der Beschäftigten 4

§ 6 Technische und organisatorische Maßnahmen des Auftragsverarbeiters 4

§ 7 Weisungsbefugnis der Verantwortlichen 4

§ 8 Kontrollrechte der Verantwortlichen 5

§ 9 Anträge der Betroffenen, Berichtigen, Einschränken der Verarbeitung und Löschen von Daten 5

§ 10 Duplizieren, Löschen und Rückgabe von Daten 5

§ 11 Pflichten des Auftragsverarbeiters bei möglichen Datenschutzverstößen 6

§ 12 Sonstige Pflichten des Auftragsverarbeiters 6

§ 13 Unterauftragsverhältnisse 6

§ 14 Zurückbehaltungsrecht 7

§ 15 Haftung 7

§ 16 Schriftformklausel 7

§ 17 Salvatorische Klausel 7

...

§ 1 Gegenstand und Dauer der Datenschutzvereinbarung

(1) Gegenstand dieser Vereinbarung ist die datenschutzkonforme Ausführung der vertraglich beschriebenen Leistungen gegenüber der Verantwortlichen, d.h. die Bereitstellung und den Betrieb eines Callcenters als Beratungs-Hotline für die telefonische Betreuung von Kleinbetrieben im Rahmen der DGUV Vorschrift 2.

(2) Zu diesem Zweck erhält der Auftragsverarbeiter Zugang zu Sozialdaten und verarbeitet diese.

(3) Betroffen sind Versicherte und Mitgliedsbetriebe der Verantwortlichen.

(4) Diese Daten unterliegen während der Vertragsdauer und darüber hinaus dem Sozialdatenschutz nach § 35 Sozialgesetzbuch Erstes Buch (SGB I) in Verbindung mit §§ 67 bis 85 a SGB X und der DSGVO.

(5) Die hier vereinbarten bzw. gesetzlich geregelten Pflichten, insbesondere nach Art. 28 DSGVO, gelten für die Dauer der Ausführung des Vertrages und darüber hinaus, solange sich die Daten im Zugriffsbereich des Auftragsverarbeiters befinden.

§ 2 Verantwortlichkeit

(1) Die BGHM ist Verantwortliche gem. Art. 4 Nr. 7 DSGVO für die jeweils übermittelten Daten.

(2) Der Auftragsverarbeiter gewährleistet die Einhaltung des Datenschutzes nach Maßgabe des jeweils geltenden Rechts für die Auftragsverarbeitung und dieser Vereinbarung.

(3) Der Auftragsverarbeiter verantwortet außerdem, dass jedem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten vollumfänglich auferlegt werden, die in diesem Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des Sozialdatenschutzes und der DSGVO erfolgt (Art. 28 Abs. 4 DSGVO).

(4) Der Auftragsverarbeiter gilt unbeschadet der Artikel 82, 83 und 84 DSGVO als Verantwortlicher bezüglich Verarbeitungen, bei der er unter Verstoß gegen die DSGVO die Zwecke und Mittel der Verarbeitung bestimmt (Art. 28 Abs. 10 DSGVO).

§ 3 Zweckbestimmung

Der Auftragsverarbeiter verwendet die überlassenen Daten ausschließlich zum Zwecke der Vertragserfüllung.

§ 4 Leistungsort

(1) Der Auftragsverarbeiter stellt sicher, dass sämtliche Daten ausschließlich und nachweisbar in der Bundesrepublik Deutschland, der Europäischen Union (EU), im Europäischen Wirtschaftsraum (EWR) oder in der Schweiz verarbeitet werden.

(2) Die Verantwortliche wird rechtzeitig vor Verlagerung der Leistungserbringung / der Datenverarbeitung des Auftragsverarbeiters an einen anderen Ort informiert. Sie stimmt dieser

...

innerhalb von 4 Wochen zu, sofern die geplante Verlagerung des Ortes der geschuldeten Dienstleistung nach dem Recht der Sozialversicherung zulässig ist.

§ 5 Unterweisung und Verpflichtung der Beschäftigten

(1) Der Auftragsverarbeiter unterweist alle mit der Datenverarbeitung befassten Beschäftigten vor Beginn der Verarbeitung hinsichtlich der Anforderungen des Sozialdatenschutzes nach § 35 SGB I und §§ 67 bis 85a SGB X.

(2) Außerdem werden alle mit der Datenverarbeitung befassten Beschäftigten des Auftragsverarbeiters und alle Beschäftigten, die Zugang zu den Daten haben, vor Beginn der Verarbeitung entsprechend Art 28 Abs. 3 b DSGVO, § 78 Abs. 1 SGB X auf den Datenschutz verpflichtet und auf die Folgen von Verstößen hingewiesen.

§ 6 Technische und organisatorische Maßnahmen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter trifft alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes nach den Weisungen der Verantwortlichen und entsprechend Art. 32 DSGVO.

(2) Der Auftragsverarbeiter dokumentiert die von ihm ergriffenen technischen und organisatorischen Maßnahmen entsprechend dem Schutzbedarf der zu verarbeitenden Daten und stellt diese der Auftraggeberin vor Abschluss dieser Vereinbarung zur Verfügung. Diese Beschreibung ist nach Maßgabe einer möglichen Erstinspektion vor Vertragsbeginn und späterer Folgeinspektionen durch die Verantwortliche Vertragsgrundlage.

(3) Der Auftragsverarbeiter stellt der Verantwortlichen ergänzend sein aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsverarbeitung zur Verfügung. Das gilt auch für datenschutzspezifische Zertifizierungen oder Datenschutzsiegel und -prüfzeichen, Audits, Testate von Sachverständigen. Sie sind für die Verantwortliche jedoch nicht bindend. Diese behält sich vor, diese Nachweise auf Aktualität, Zuverlässigkeit des Ausstellers, inhaltliche Richtigkeit und Anwendbarkeit zu prüfen.

(4) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen, soweit keine anderweitigen Weisungen der Verantwortlichen vorliegen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und der Verantwortlichen mitzuteilen. Sollten anderweitige Prüfungen oder Audits einen Nachbesserungsbedarf ergeben, ist die Verantwortliche darüber zu informieren.

§ 7 Weisungsbefugnis der Verantwortlichen

(1) Die Verantwortliche behält sich ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der vertragsgegenständlichen Datenverarbeitung bei dem Auftragsverarbeiter vor, dass sie jederzeit durch Einzelweisungen konkretisieren kann.

(2) Der Auftragsverarbeiter wird die Verantwortliche unverzüglich darauf aufmerksam machen, wenn eine erteilte Weisung gegen gesetzliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch die Verantwortliche bestätigt oder geändert wird.

...

(3) Mündliche Weisungen wird die Verantwortliche unverzüglich schriftlich oder elektronisch (in Textform) bestätigen.

§ 8 Kontrollrechte der Verantwortlichen

(1) Der Auftragsverarbeiter räumt der Verantwortlichen das Recht ein, vor Aufnahme der Datenverarbeitung eine Erstinspektion und sodann ggfls. regelmäßige Inspektionen durch ihre Beauftragten in den Räumlichkeiten und am Ort der Auftragsverarbeitung durchzuführen. Den hierzu Beauftragten sind alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO bezeichneten Pflichten zur Verfügung zu stellen (Art. 28 Abs. 3h DSGVO, § 6 Abs. 3 dieser Vereinbarung).

(2) Die Inspektionen werden mindestens drei Tage vorher angekündigt. Bei Verstößen oder dem Verdacht auf Verstöße gegen den Datenschutz, diese Vereinbarung oder erteilte Weisungen, insbesondere bei konkreten Zweifeln an der ordnungsgemäßen Durchführung der technischen und organisatorischen Maßnahmen, kann die Verantwortliche eine Inspektion jederzeit unangekündigt während der Betriebs- und Geschäftszeiten vornehmen. Sie bemüht sich dabei, Störungen des Betriebsablaufs so weit als möglich zu vermeiden.

§ 9 Anträge der Betroffenen, Berichtigen, Einschränken der Verarbeitung und Löschen von Daten

Der Auftragsverarbeiter hat nur nach Weisung der Verantwortlichen Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken. Soweit Betroffene sich diesbezüglich unmittelbar an den Auftragsverarbeiter wenden, wird dieser das Ersuchen unverzüglich an die Verantwortliche weiterleiten. Die Prüfung der Anfrage obliegt ausschließlich der Verantwortlichen.

§ 10 Duplizieren, Löschen und Rückgabe von Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen der Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherungskopien, die erforderlich sind zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung, sowie Daten, die der gesetzlichen Aufbewahrungspflicht unterliegen.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch die Verantwortliche – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, der Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung entsprechend DIN 66399 Schutzklasse 3 Stufe 4 zu vernichten bzw. datenschutzgerecht zu löschen. Die Protokolle der Vernichtung bzw. der Löschung sind auf Anforderung vorzulegen.

(3) Evtl. Ausdrucke (Testdrucke, Ausschussmaterial, Listen etc.), sind unverzüglich entsprechend DIN 66399 Schutzklasse 3, Stufe P 4 zu vernichten.

(4) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende der Verantwortlichen übergeben.

...

§ 11 Pflichten des Auftragsverarbeiters bei möglichen Datenschutzverstößen

(1) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese der Verantwortlichen unverzüglich (Art. 33 Abs. 2 DSGVO). Das gilt auch, wenn die bloße Möglichkeit besteht, dass unbefugte Dritte Kenntnis von Daten erhalten haben.

(2) Die Prüfung, ob eine Datenschutzverletzung vorliegt und ob dies zu einem Risiko für die Rechte und Freiheiten der Betroffenen führt (Art. 33, 34 DSGVO i.V.m. § 83 a SGB X), obliegt der Verantwortlichen.

(3) Der Auftragsverarbeiter trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher Risiken und nachteiliger Folgen für die Betroffenen. Er stimmt sich hierzu mit der Verantwortlichen ab. Der Auftragsverarbeiter unterstützt die Verantwortliche bei der Erfüllung ihrer Informationspflichten gegenüber den zuständigen Aufsichtsbehörden bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Art. 33, 34 DSGVO, § 83 a SGB X.

(4) Die Meldungen an Behörden und Benachrichtigungen von Betroffenen nach den o.g. Vorschriften erfolgt ausschließlich durch die Verantwortliche. Bevor der Auftragsverarbeiter eine Meldung an eine Aufsichtsbehörde aus etwaigen unmittelbaren gesetzlichen Pflichten der Auftragsverarbeitung vornimmt, ist die Verantwortliche zum Zweck der Abstimmung darüber zu unterrichten.

§ 12 Sonstige Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter unterstützt bei Bedarf die Verantwortliche bei der Erfüllung ihrer datenschutzrechtlichen Pflichten (z.B. einer Datenschutzfolgenabschätzung oder der Konsultation der zuständigen Aufsichtsbehörde).

(2) Der Auftragsverarbeiter hat zu jeder Zeit der Vertragsdauer einen Datenschutzbeauftragten bestellt (Art. 37 bis 39 DSGVO bzw. §§ 5 bis 7 BDSG) und teilt der Verantwortlichen dessen Kontaktdaten mit. Ein Wechsel des Datenschutzbeauftragten ist der Verantwortlichen unverzüglich schriftlich mitzuteilen.

(3) Der Auftragsverarbeiter informiert die Verantwortliche unverzüglich über ihn oder einen Unterauftragnehmer betreffende Kontrollen, Maßnahmen und Ermittlungen durch Aufsichtsbehörden.

(4) Sollten die Daten der Verantwortlichen bei dem Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter die Verantwortlichen unverzüglich darüber zu informieren. Der Auftragsverarbeiter informiert unverzüglich alle in diesem Zusammenhang Verantwortlichen darüber, dass die Hoheit und das Eigentum an den Daten ausschließlich bei der Verantwortlichen liegen.

§ 13 Unterauftragsverhältnisse

(1) Für Unterauftragsverhältnisse gilt Art. 28 Abs. 2 DSGVO.

(2) Verträge zur Wartung von Datenverarbeitungsanlagen im Auftrag des Auftragsverarbeiters, bei deren Ausführung ein Zugriff auf Daten nicht ausgeschlossen werden kann, gelten ebenfalls

...

als Unterauftragsverhältnisse im Sinne dieser Vereinbarung (Art. 4 Nr. 2 DSGVO, § 80 Abs. 5 SGB X).

§ 14 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

§ 15 Haftung

Die Verantwortlichen und der Auftragsverarbeiter haften gegenüber betroffenen Personen gemäß den in der DSGVO getroffenen Regelungen.

§ 16 Schriftformklausel

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Regelungen handelt. Das Schriftformerfordernis gilt auch für den Verzicht auf dieses Formerfordernis.

§ 17 Salvatorische Klausel

(1) Sollte eine Bestimmung dieses Vertrages unwirksam oder undurchführbar sein oder künftig unwirksam oder undurchführbar werden, so werden die übrigen Regelungen dieses Vertrags davon nicht berührt.

(2) Anstelle der unwirksamen oder undurchführbaren Regelung verpflichten sich die Parteien schon jetzt, eine wirksame Regelung zu vereinbaren, die dem Sinn und Zweck der unwirksamen oder undurchführbaren Regelung möglichst nahekommt. Entsprechendes gilt für Lücken dieses Vertrags. Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Sozialdaten im Sinne dieses Vertrages am besten gewährleistet.

Auftraggeberin:	**Auftragnehmer:**
Mainz, ……...	……..., ……
……..…...	……..……