Vertrag

über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DS-GVO

zwischen

Firmenname
Straße Hausnummer
PLZ Ort

– nachfolgend Auftraggeber“ genannt –

und

Bornemann AG
Im Fliegerhorst 10
38642 Goslar

– nachfolgend „Auftragnehmer“ genannt –

§1
Vertragsgegenstand

Im Rahmen der Leistungserbringung nach den in der Anlage 1 im Einzelnen benannten Verträgen (nachfolgend „Vertrag“ genannt) ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „Auftraggeber-Daten“ genannt).

Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit „Auftraggeber-Daten“ zur Durchführung des „Vertrags“.

Verweise auf die Datenschutz-Grundverordnung (DS-GVO [1]) und das Bundesdatenschutzgesetz 2018 (BDSG 2018 [2]) sind bis zum 24.05.2018 als Verweise auf das Bundesdatenschutzgesetz (BDSG [3]) auszulegen. Sofern sich diese Vereinbarung auf Regelungen der DS-GVO bezieht, die über die Regelungen des BDSG hinausgehen oder den Regelungen des BDSG widersprechen, findet die jeweilige Vertragsregelung bis zum 24.05.2018 keine Anwendung.

§2
Art, Umfang, Zweck und Laufzeit der Auftragsverarbeitung

1) Der Auftragnehmer verarbeitet die „Auftraggeber-Daten“ im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DS-GVO (Auftragsverarbeitung). Der Auftraggeber bleibt im datenschutzrechtlichen Sinn Verantwortlicher („Herr der Daten“).
2) Die Verarbeitung der „Auftraggeber-Daten“ im Rahmen der Auftragsverarbeitung erfolgt entsprechend den in Anlage 1 zu diesem Vertrag enthaltenen Festlegungen zu Art, Umfang und Zweck der Datenverarbeitung. Sie bezieht sich auf die in Anlage 1 festgelegte Art der „Auftraggeber-Daten“ und die dort bestimmten Kategorien betroffener Personen.
3) Der Auftragnehmer darf die „Auftraggeber-Daten“ im Rahmen des datenschutzrechtlich Zulässigen für eigene Zwecke auf eigene Verantwortung verarbeiten, wenn eine gesetzliche Erlaubnisvorschrift oder eine Einwilligungserklärung der betroffenen Person das gestattet. Auf solche Datenverarbeitungen findet dieser Vertrag keine Anwendung. In jedem Fall darf der Auftragnehmer die „Auftraggeber-Daten“ anonymisieren und in anonymisierter Form für eigene Zwecke verarbeiten und nutzen, insbesondere für statistische Zwecke.

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
[2] Bundesdatenschutzgesetz in der Fassung des Art. 1 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU, DSAnpUG-EU)
[3] Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 mit den zuletzt in Kraft getretenen Änderungen

4) Die Verarbeitung der „Auftraggeber-Daten“ findet grundsätzlich im Gebiet der Bundesrepublik Deutschland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.
5) Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zur Laufzeit und Kündigung des „Vertrags“. Eine Kündigung des „Vertrags“ bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

§3
Weisungsbefugnisse des Auftraggebers

1) Der Auftragnehmer verwendet die „Auftraggeber-Daten“ ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers, wie sie abschließend in den Bestimmungen dieses Vertrags Ausdruck finden.
2) Einzelweisungen des Auftraggebers sind grundsätzlich schriftlich oder zumindest in Textform durch die hierzu befugten Personen des Auftraggebers zu erteilen (Siehe Anlage 4). Etwaige Änderungen sind der anderen Vertragspartei unverzüglich schriftlich mitzuteilen. Mündliche Einzelweisungen bedürfen zu ihrer Wirksamkeit der unverzüglichen schriftlichen oder in Textform erteilten Bestätigung durch den Auftraggeber.
3) Unbeschadet dessen werden mündliche Einzelweisungen vom Auftragnehmer zur Sicherstellung der Identität des Erteilenden nur nach Nennung eines Kennworts angenommen; das Kennwort wird dem Auftraggeber unverzüglich nach Abschluss der vorliegenden Vereinbarung mitgeteilt. Der Auftraggeber ist selbst dafür verantwortlich dafür zu sorgen, dass das Kennwort lediglich solchen Personen bekannt ist, die zur Erteilung von Einzelweisungen gegenüber dem Auftragnehmer befugt sind.
4) Ist der Auftragnehmer der Ansicht, dass eine zulässige Einzelweisung gegen geltendes Datenschutzrecht verstößt, wird er den Auftraggeber möglichst zeitnah darauf hinweisen. Außerdem ist der Auftragnehmer berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen.

§4
Pflichten des Auftraggebers

1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der „Auftraggeber-Daten“ sowie für sie Wahrung der Rechte der betroffenen Personen verantwortlich. Sollten Dritte oder betroffene Personen gegen den Auftragnehmer aufgrund der Verarbeitung von „Auftraggeber-Daten“ Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen, wenn und soweit den Auftragnehmer nicht gemäß Art. 82 DS-GVO eine eigene Haftung trifft.

2) Der Auftraggeber ist Eigentümer der „Auftraggeber-Daten“ und Inhaber aller etwaigen Rechte, die die „Auftraggeber-Daten“ betreffen.
3) Dem Auftraggeber obliegt es, dem Auftragnehmer die „Auftraggeber-Daten“ rechtzeitig zur Leistungserbringung nach dem „Vertrag“ zur Verfügung zu stellen, und er ist verantwortlich für die Qualität der „Auftraggeber-Daten“. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

§5
Pflichten des Auftragnehmers

1) Der Auftragnehmer stellt sicher und kontrolliert regelmäßig, dass die Datenverarbeitung im Rahmen der Leistungserbringung nach dem „Vertrag“ in seinem Verantwortungsbereich, der Unterauftragnehmer nach § 9 dieses Vertrags einschließt, in Übereinstimmung mit den Bestimmungen dieses Vertrags erfolgt.
2) Der Auftragnehmer darf ohne vorherige Zustimmung durch den Auftraggeber im Rahmen der Auftragsverarbeitung keine Kopien oder Duplikate der „Auftraggeber-Daten“ anfertigen. Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß des „Vertrages“ (einschließlich der Datensicherung) erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
3) Der Auftragnehmer unterstützt den Auftraggeber bei Kontrollen durch die Aufsichtsbehörde im Rahmen des Zumutbaren und Erforderlichen, soweit diese Kontrollen die Datenverarbeitung durch den Auftragnehmer betreffen.
4) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung von dessen Verpflichtungen gemäß Artt. 32 bis 36 DS-GVO, insbesondere bei einer Datenschutz-Folgenabschätzung des Auftraggebers inklusive einer etwa notwendigen vorherigen Konsultation der zuständigen Aufsichtsbehörde. Hierzu wird der Auftragnehmer dem Auftraggeber im Rahmen des Zumutbaren proaktiv Informationen zu den technischen und organisatorischen Maßnahmen sowie den von der Auftragsverarbeitung umfassten Datenverarbeitungsvorgängen zur Verfügung stellen. Weitere Unterstützungsleistungen bedürfen der ausdrücklichen Vereinbarung der Parteien.
5) Der Auftragnehmer hat die bei der Verarbeitung von „Auftraggeber-Daten“ beschäftigten Personen gemäß Art. 28 Abs. 3 lit. b) DS-GVO schriftlich zur Vertraulichkeit zu verpflichten.
6) Der Auftragnehmer hat einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten benannt, dessen Kontaktdaten leicht zugänglich auf der Webseite des Auftraggebers abrufbar sind. Der Auftragnehmer verpflichtet sich zur Benennung eines Datenschutzbeauftragten, solange die gesetzlichen Voraussetzungen für eine Benennungspflicht gegeben sind.
7) Der Auftragnehmer unterliegt der behördlichen Aufsicht sowie den Bußgeld- und Strafvorschriften in Artt. 82 bis 84 DS-GVO sowie in §§ 41 bis 43 BDSG.

§6
Technische und organisatorische Maßnahmen

1) Der Auftragnehmer hat vor Beginn der Verarbeitung der „Auftraggeber-Daten“ die in Anlage 2 dieses Vertrags aufgelisteten technischen und organisatorischen Maßnahmen zu implementieren und während des Vertrags aufrechtzuerhalten. Hierbei handelt es sich um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.
2) Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der technologischen Weiterentwicklung unterliegen, ist es dem Auftragnehmer gestattet, alternative und adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der in Anlage 2 festgelegten Maßnahmen nicht unterschritten wird. Der Auftragnehmer wird solche Änderungen dokumentieren. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers und sind vom Auftragnehmer zu dokumentieren und dem Auftraggeber auf Anforderung zur Verfügung zu stellen.
3) Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des nachfolgend beschriebenen Verfahrens, wenn nicht die Parteien im „Vertrag“ eine abweichende Regelung für ein Änderungsverfahren getroffen haben; in solchen Fällen geht die Regelung im „Vertrag“ in Abweichung von § 12 dieses Vertrags den nachfolgenden Bestimmungen vor.

a. Der Auftraggeber kann jederzeit mittels konkreter Einzelweisungen Änderungen und Ergänzungen der Auftragsverarbeitung durch den Auftragnehmer, insbesondere Änderungen und Ergänzungen der technischen und organisatorischen Maßnahmen verlangen, wenn diese für den Auftragnehmer technisch umsetzbar und zumutbar sind. Der Auftragnehmer prüft solche Änderungsverlangen innerhalb von fünf Arbeitstagen nach Eingang und teilt dem Auftraggeber das Ergebnis zusammen mit den sich ggf. ergebenden einmaligen oder laufenden Mehrkosten und Umsetzungszeiträumen in Form eines verbindlichen Angebots mit.
b. Der Auftraggeber wird das Angebot innerhalb von fünf Werktagen ab Zugang des Angebots prüfen. Nimmt der Auftraggeber das Angebot an, so werden die Änderungen Vertragsbestandteil. Der Auftragnehmer wird ggf. die in Anlage 2 festgelegten technischen und organisatorischen Maßnahmen ergänzen. Nimmt der Auftraggeber das Angebot nicht an, werden die Parteien die Auftragsverarbeitung unverändert fortsetzen, wenn nicht dem Auftraggeber eine Fortsetzung unzumutbar ist.
c. Der Auftragnehmer wird während eines laufenden Änderungsverfahrens die Leistungen im Rahmen der Auftragsverarbeitung planmäßig weiterführen, es sei denn, der Auftraggeber weist

ihn schriftlich an, dass die Auftragsverarbeitung bis zur Entscheidung über die Einzelweisung eingestellt oder eingeschränkt werden soll.

§7
Mitzuteilende Verstöße des Auftragnehmers

1) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er eine Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit diesem Vertrag feststellt.
2) Soweit den Auftraggeber aufgrund eines Vorkommnisses nach § 7 Abs. 1 gesetzliche Informationspflichten wegen eines Risikos für die Rechte und Freiheiten natürlicher Personen (insbesondere nach Art. 33 DS-GVO) treffen, hat der Auftragnehmer den Auftraggeber bei der Erfüllung der Informationspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden, nachzuweisenden Aufwände und Kosten zu unterstützen.

§8
Kontrollrechte des Auftraggebers

1) Der Auftraggeber ist berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 8.00 bis 17.00 Uhr) auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers, die Geschäftsräume des Auftragnehmers, in denen „Auftraggeber-Daten“ verarbeitet werden, zu betreten, um sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 2 zu diesem Vertrag zu überzeugen.
2) Der Auftragnehmer gewährt dem Auftraggeber die zur Durchführung der Kontrollen nach § 8 Abs. 1 erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.
3) Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten - es sei denn, dass diese die Basis des erstattungsfähigen oder durchlaufenden Aufwandes darstellen - zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Kontrollzwecke sind, zu erhalten.

4) Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren; insbesondere ist der Termin der Kontrolle mit dem Auftragnehmer abzustimmen. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Auftraggebers, weitere Kontrollen auch unangekündigt im Fall von besonderen Vorkommnissen durchzuführen.

5) Im Falle von mehrfachen anlasslosen Kontrollen erhält der Auftragnehmer vom Auftraggeber eine Aufwandsentschädigung für seinen im Rahmen dieser Kontrollen anfallenden Aufwand in Höhe von 600,00 EUR netto (8 Stunden zu einem Stundensatz von 75,00 EUR netto) pro Kontrolle/pro Arbeitstag.

6) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von § 8 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen.

7) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 2 anstatt durch eine Vor-Ort-Kontrolle auch durch die Einhaltung genehmig ter Verhaltensregeln gemäß Art. 40 DS-GVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO sowie die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit - z.B. nach BSI-Grundschutz - („Prüfungsbericht“) erbracht werden, wenn und soweit der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 2 zu diesem Vertrag zu überzeugen.

§9
Unterauftragsverhältnisse

1) Der Auftragnehmer darf Unterauftragsverhältnisse hinsichtlich der Verarbeitung von „Auftraggeber-Daten“ begründen. Der Auftragsverarbeiter wird den Verantwortlichen über jede beabsichtigte Unterbeauftragung sowie jede Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern informieren, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Einen solchen Einspruch darf der Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden, Grund erheben. Im Fall der Einschaltung eines nach §§ 15 ff. AktG mit dem Auftragnehmer verbundenen Unternehmens als Unterauftragnehmer erteilt der Auftraggeber hiermit ausdrücklich seine Zustimmung; dasselbe gilt für die Anlage 3 bezeichneten Unterauftragnehmer

des Auftragnehmers zum Zeitpunkt des Vertragsschlusses.

2) Keiner Zustimmung bedarf die Einschaltung von Subunternehmern, bei denen der Subunternehmer lediglich eine Nebenleistung zur Unterstützung bei der Leistungserbringung nach dem „Vertrag“ in Anspruch nimmt, auch wenn dabei ein Zugriff auf die „Auftraggeber-Daten“ nicht ausgeschlossen werden kann; dazu zählen insbesondere Transportleistungen von Post- oder Kurierdiensten sowie Geldtransportdienstleistungen, Telekommunikationsdienste, Bewachungsdienste und Reinigungsdienste. Der Auftragnehmer wird mit solchen Subunternehmern branchenübliche Geheimhaltungsvereinbarungen treffen.

3) Zur Prüfung eines nach § 9 Abs. 1 möglichen Einspruchs hat der Auftragnehmer dem Auftraggeber auf Verlangen eine Kopie der Vereinbarung zur Unterauftragsverarbeitung zur Verfügung zu stellen. Der Unterauftragsverarbeitungsvertrag muss ein adäquates Schutzniveau aufweisen, welches demjenigen dieses Vertrags vergleichbar ist. Dem Auftraggeber sind in dem Unterauftragsverarbeitungsvertrag gegenüber dem Unterauftragnehmer eigene Kontrollrechte nach § 8 dieses Vertrags einzuräumen.

4) Die Regelungen in § 9 gelten auch, wenn ein Unterauftragnehmer in einem Drittstaat eingeschaltet wird. Eine Beauftragung von Subunternehmern in Drittstaaten erfolgt nur dann, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln). Der Auftraggeber erklärt sich bereit, an der Erfüllung der Voraussetzungen nach Art. 46 DS-GVO im erforderlichen Maße mitzuwirken.

§10
Rechte der betroffenen Personen

1) Die Rechte der durch die Datenverarbeitung betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen.

2) Soweit eine betroffene Person sich zwecks Ausübung der ihr nach den Artt. 15 ff. DS-GVO zukommenden Rechte unmittelbar an den Auftragnehmer wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

3) Für den Fall, dass eine betroffene Person die ihr nach den Artt. 15 ff. DS-GVO zukommenden Rechte geltend macht, hat der Auftragnehmer den Auftraggeber bei der Erfüllung dieser Ansprüche in angemessenem und für den Auftraggeber erforderlichen Umfang zu unterstützen, sofern der Auftraggeber die Ansprüche nicht ohne Mitwirkung des Auftragnehmers erfüllen kann.

4) Der Auftragnehmer wird es dem Auftraggeber ermöglichen, „Auftraggeber-Daten“ zu berichtigen oder zu löschen oder die Verarbeitung einzuschränken oder die personenbezogenen Daten an die betroffene Person oder einen von dieser benannten Dritten herauszugeben oder auf Verlangen des Auftraggebers die Berichtigung, Löschung, Einschränkung der Verarbeitung oder Datenübertragung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist. Gesetzliche Pflichten, Datensätze nachträglich bis zum Ende gesetzlicher Aufbewahrungspflichten unveränderbar zu halten (z.B. elektronische Fahrtenbücher), bleiben unberührt.

§11

Rückgabe und Löschung überlassener Daten und Datenträger

1) Der Auftragnehmer hat sämtliche „Auftraggeber-Daten“ nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des „Vertrags“) zu löschen und von dem Auftraggeber erhaltene Datenträger, die zu diesem Zeitpunkt noch „Auftraggeber-Daten“ enthalten, an den Auftraggeber zurückzugeben.

2) Über eine Löschung bzw. Vernichtung von „Auftraggeber-Daten“ hat der Auftragnehmer ein Protokoll zu erstellen, das dem Auftraggeber auf Anforderung vorzulegen ist.

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

§12
Verhältnis zum „Vertrag“

Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des „Vertrags“. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem „Vertrag“, gehen die Regelungen aus diesem Vertrag vor.

Ort, Datum	Ort, Datum
Unterschrift, Auftragnehmer	Unterschrift / Firmenstempel, Auftraggeber

Anlagen:

Anlage 1: Zweck, Art und Umfang der Auftragsverarbeitung, Art der Daten und Kategorien betroffener Personen

Anlage 2: Technische und organisatorische Maßnahmen der Bornemann AG

Anlage 3: Genehmigte Unterauftragnehmer

Anlage 4: Übersicht weisungsberechtigter Personen

Anlage 1

Zweck, Art und Umfang der Auftragsverarbeitung; Art der Daten und Kategorien betroffener Personen **[Rot umrandete Felder sind vom Auftraggeber auszufüllen]**

1. **Der Auftraggeber hat den Auftragnehmer mit der Erbringung von Leistungen beauftragt. Diese bestehen im Einzelnen aus den nachfolgenden Leistungen:**

   - Erhebung und Verarbeitung von GPS-Ortungsdaten
   - Supportleistungen für GPS-Ortungsgeräte
   - Hosting von Daten des Auftraggebers im Rechenzentrum
   - ☐ Track & Tracing
   - ☐ Fuhrparkmanagement
   - ☐ _____
   - ☐ _____

   und sind in den Verträgen

   ☐ alle Nutzungsverträge zu Kundennummer _____
   ☐ Nutzungsvertrag vom _____
   ☐ Nutzungsvertrag vom _____
   ☐ Nutzungsvertrag vom _____

   im Einzelnen spezifiziert.

2. **Im Rahmen der Leistungserbringung nach den vorgenannten Verträgen hat der Auftragnehmer zum Zwecke der Vertragserfüllung Einblick in und Zugriff auf folgende "Auftraggeber-Daten:**

   - Ortungsdaten
   - Personenstammdaten (z.B. Name, Anschrift, Geburtsdatum etc.)
   - Kommunikationsdaten (wie z. B. Telefon, E-Mail)
   - Vertragsstammdaten (Vertragsverhältnis, Produktinteresse oder Vertragsinteresse)
   - Kundenhistorie
   - Vertragliche Abrechnungs- und Zahlungsdaten
   - Planungs- und Steuerungsdaten
   - Auskunftsangaben (von „Dritten“, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

   Der Umfang der Datenverarbeitung erstreckt sich dabei allein und ausschließlich auf das zur Erfüllung der Vertragspflichten Erforderliche, also regelmäßig lediglich die Kenntnisnahme von Daten im Rahmen von Wartungs- und Supportarbeiten. Insbesondere ist jede Datenverarbeitung für eigene Zwecke des Auftragnehmers ausgeschlossen.

3. **Folgende Kategorien betroffener Personen sind von der Auftragsverarbeitung umfasst:**
   [Sofern neben den Beschäftigten weitere Personen von der Auftragsverarbeitung betroffen sind, müssen diese durch ankreuzen der Checkboxen markiert werden.]

- ☐ Kunden
- ☐ Versicherte
- ☐ Patienten
- ☐ Interessenten
- ☐ Abonnenten
- ☒ Beschäftigte i.S.d. § 26 Abs. 8 BDSG
- ☐ Lieferanten
- ☐ Handelsvertreter

[Zutreffendes **bitte ankreuzen**; z.B. wären anzukreuzen für den Fall eines Handwerksbetriebs, der Ortungsgeräte des Auftragnehmers beschafft hat, diese im Rechenzentrum des Auftragnehmers verarbeiten lässt und Supportleistungen des Auftragnehmers in Anspruch nimmt: Kunden und Interessenten (jeweils über angefahrene Anschriften feststellbar), Beschäftigte (jedenfalls im Rahmen der Vertrags-/Rechnungsabwicklung oder über Supportanfragen mitgeteilt) , u.U. auch Lieferanten und Handelsvertreter (wenn z.B. ebenfalls über Anschriften feststellbar) ; anders z.B. für den Fall eines mobilen Pflegedienstes, der Ortungsgeräte des Auftragnehmers beschafft hat, diese im Rechenzentrum des Auftragnehmers verarbeiten lässt und Supportleistungen des Auftragnehmers in Anspruch nimmt: hier wären anstelle von Kunden Patienten auszuwählen.]

Ort, Datum	
Unterschrift / Firmenstempel Auftraggeber	

Anlage 2

Technische und organisatorische Maßnahmen Bornemann AG

Technische und organisatorische Maßnahmen

der Bornemann AG

20.11.2023

V 0.5

Technische und organisatorische Maßnahmen

Änderungshistorie

Versionsnummer	Vorgenommene Änderung	Änderungsdatum	Kürzel des Mitarbeiters
V 0.1	Erstellung der technischen und organisatorischen Maßnahmen	14.03.2016	NIE
V 0.2	Überarbeitung der kompletten technischen und organisatorischen Maßnahmen	28.07.2020	WDU
V 0.3	Aktualisierung der technischen und organisatorischen Maßnahmen	04.01.2021	ULZ
V 0.4	Überprüfung der technischen und organisatorischen Maßnahmen	14.12.2022	ULZ YHO (Externer DSB)
V 0.5	Aktualisierung der technischen und organisatorischen Maßnahmen	20.11.2023	ULZ YHO (Externer DSB)

Technische und organisatorische Maßnahmen

Definitionen

Auftraggeber

Bei dem Auftraggeber im Sinne des Vertrages über die Verarbeitung personenbezogener Daten gemäß Art. 28 DS-GVO handelt es sich um den Kunden.

Auftragnehmer

Bei dem Auftragnehmer im Sinne des Vertrages über die Verarbeitung personenbezogener Daten gemäß Art. 28 DS-GVO handelt es sich um die Bornemann AG.

Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

01. Zutrittskontrolle

In den Niederlassungen der Bornemann AG sind die Türen und Tore der Gebäude mit Sicherheitsschlössern versehen. Türen und Fenster sind außerhalb der Betriebszeiten fest verschlossen.

Außerhalb der Betriebszeiten erfolgt eine Überwachung der Liegenschaften und der darauf befindlichen Gebäude mittels Videokameras, die außerhalb und innerhalb der Gebäude installiert sind. Die Videokameras verfügen über eine Motion-Detection-Funktion, mittels derer bei definierten Anlassarten (z.B. Perimeterschutz, Linienüberquerung, Einbruchserkennung usw.) eine Alarmmeldung an einen hierfür autorisierten Personenkreis versendet wird. Dieser Personenkreis kann per Fernzugriff auf die Livebilddateien der Videokameras zugreifen, die aktuelle Situation prüfen und ggf. Sicherheitskräfte informieren.

Zudem werden die Liegenschaften und Gebäude der Bornemann AG außerhalb der Betriebszeiten mehrfach in unregelmäßigen Abständen durch einen privaten Sicherheitsdienst bestreift und kontrolliert.

Es existieren folgende Maßnahmen zur Zutrittskontrolle:

a. Festlegung befugter Personen
b. Vorhandensein von Regelungen für Firmenfremde
c. Durchführung von Anwesenheitsaufzeichnungen
d. Sicherung der Liegenschaften und Gebäude außerhalb der Betriebszeiten durch den Einsatz von Videotechnik
e. Mehrfache unregelmäßige Bestreifung und Kontrolle der Liegenschaften und Gebäude außerhalb der Betriebszeiten durch einen privaten Sicherheitsdienst
f. Einteilung der Unternehmensgebäude in unterschiedliche Sicherheitsbereiche (z.B. Verwaltung, Entwicklung usw.)
g. Ausstattung der Maßnahmen zur Objektsicherung (Einsatz eines privaten Sicherheitsdienstes, Einsatz von Videotechnik, Stahltüren, Umzäunung des Geländes, elektr. Rolltor)

02. Zugangskontrolle

Die Schlüssel zu den Räumlichkeiten, in denen die Auftragsdaten verarbeitet bzw. vernichtet werden, befinden sich in der ausschließlichen Obhut der Geschäftsleitung des Auftragnehmers sowie der zuständigen Mitarbeiter. Dritte haben zu den Räumlichkeiten keinen Zutritt. Die Vergabe von Schlüsseln ist schriftlich geregelt. Firmenfremde werden zentral in Empfang genommen und im Gebäude begleitet.

Eine Übersicht der Maßnahmen zur Zugangskontrolle:

a. Festlegung befugter Personen
b. Vorhandensein von Regelungen für Firmenfremde
c. Durchführung von Anwesenheitsaufzeichnungen
d. Vorhandensein von Passwörtern (bei PC-Arbeitsplätzen)
e. Anforderung der regelmäßigen Passwortänderung (bei PC-Arbeitsplätzen)

03. Zugriffskontrolle

Der Zugriff auf Systeme ist mit Benutzerkennungen und regelmäßig zu ändernden Passwörtern geschützt. Zugriffe von außen erfolgen durch ausgewählte Mitarbeiter mit Identifizierung gegenüber dem Datenverarbeitungssystem durch Identifikation und Authentifizierung. Aktuelle Virenscanner sind installiert. Es wird gewährleistet, dass zur Verarbeitung bestimmte Daten während ihres Transports gegen unberechtigte Einsichtnahme und Verlust geschützt sind (SSL, Verschlüsselung bei Datenfernübertragung):

a. Umsetzung von Teilzugriffsmöglichkeit auf Datenbestände und Funktionen
b. Durchführung einer Identifizierung gegenüber dem Datenverarbeitungssystem durch Identifikation und Authentifizierung
c. Überprüfung der Berechtigung, maschinell
d. Umsetzung von Regelungen zur Zugriffs- und Benutzerberechtigung
e. Durchführung der Auswertung von Protokollen

04. Trennungsgebot

Die Trennung der Datensätze erfolgt durch die physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern.

Es existieren folgende Maßnahmen zum Trennungsgebot:

a. Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
b. Logische Mandantentrennung (softwareseitig)

• Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) …

… ist die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen. Unter Berücksichtigung und Wahrung der durch die jeweiligen Auftraggeber benannten Zwecke der Datenverarbeitung, findet eine Pseudonymisierung der personenbezogenen Daten, die im Zuge der sich aus dem Hauptvertrag zu erbringenden Leistungen ergeben, nicht statt. Bei Verarbeitungen der personenbezogenen Daten, die über den durch den Kunden im Voraus definierten Zweck hinausgehen, nämlich konkret der Verarbeitung der Daten zu statistischen Zwecken, findet zuvor eine Anonymisierung statt. Hierbei werden nicht personenbezogenen Extrakte einzelner Datensätze aus den Datenbanken entnommen und miteinander vermischt, so dass ein späterer Personenbezug nicht mehr ableitbar ist.

II. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

01. Weitergabekontrolle

Für die datenschutzgerechte Vernichtung von Fehldrucken und sonstigem Datenabfall stehen für kleine Mengen elektrische Einzelschredder sowie für größere Mengen ein Papiervernichtungscontainer eines gewerblichen Vernichters zur Verfügung.

Es existieren folgende Maßnahmen zur Weitergabekontrolle:

a. Vorhandensein von Dokumentationen der Abruf- und Übermittlungsprogramme
b. Vorhandensein von Dokumentationen zu den Stellen, an die eine Übermittlung vorgesehen ist sowie deren Übermittlungswege
c. Durchführung einer Verschlüsselung (SSL, SFTP, SSH)
d. Feststellung zur Übermittlung befugter Personen
e. Lagerung von Datenträgern in Sicherheitsbereichen (Vorhandensein von Dateiarchiven bzw. Tresoren)
f. Durchführung regelmäßiger Bestandskontrollen (Tages-, Wochen-, Monatscheck)
g. Kontrollierte Vernichtung von Datenträgern (Papier und elektronische Datenträger) nach DIN 66399
h. Zertifiziertes Dokumentenvernichtungssystem

02. Eingabekontrolle

Um Eingaben, Änderungen und Löschungen nachvollziehen zu können, wird eine Historie der Änderungen erstellt, die die Änderung sowie den Benutzer enthält, der die Änderung vorgenommen hat. Die Rechte der Benutzer sind an die jeweiligen Arbeitsabläufe und Abteilungen angepasst.

Es existieren folgende Maßnahmen zur Eingabekontrolle:

a. Protokollierung der Eingabe, Änderung und Löschung von Daten
b. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
c. Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

01. Verfügbarkeitskontrolle

Um die Verfügbarkeit der Daten zu gewährleisten, werden regelmäßige Backups im Rechenzentrum erstellt (siehe TOM Rechenzentrum).

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

a. Vorhandensein und Umsetzung eines Konzeptes zur Durchführung von regelmäßigen Datensicherungen (Datensicherheitskonzept gem. IT-Grundschutz)
b. Überwachung der Betriebsparameter von Rechenzentren (SNMP, Nagios).

02. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Sollte das Problem einer korrupten Datenbank hervortreten, so sind geeignete Maßnahmen einer raschen Wiederherstellbarkeit getroffen worden, indem die korrupte Datenbank mithilfe eines RAID-10-Systems wiederhergestellt werden kann. Soweit auch dieser automatische Prozess erfolglos bleiben sollte, ist eine manuelle Erstellung von Backups innerhalb einer Stunde möglich.

Der Serverstandort beherbergt weiterhin geeignete Maßnahmen im Falle eines entzündenden Feuers, indem Feuerabsenkungsanlagen installiert worden sind.

Der Serverstandort ist außerdem so ausgestattet, dass er sich für einen Zeitraum von vier Tagen mit einem eigenem Notstromsystem versorgen kann, um so die Funktionalität der Server zu gewährleisten.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

01. Datenschutz-Management

- Bestellung eines Datenschutzbeauftragten (DSB)
- Erstellung der nach der DSGVO und dem BDSG notwendigen Dokumentation
- Regelmäßige Überprüfung des Datenschutzmanagementsystems durch den DSB
- Regelmäßige Datenschutz-Schulungen der Mitarbeiter
- Etablierung eines Betroffenenrechte-Prozesses
- Durchführung von Datenschutz-Folgenabschätzungen, sofern notwendig

02. Incident-Response-Management

- Identifizierung zur Zugangsfreischaltung durch die Zusammenführung eines nach SHA1-Standard gehashten Passwortes mit einem Salt-Hash generierten Passwortes
- Sperreinrichtung des Zuganges bei mehrmaligen Fehleingaben
- IP-Sperren bei Botangriffen
- IP-Blacklist (Drittländer, in die keine Kundenbeziehungen unterhalten werden, werden ausgeschlossen)
- Passwortaufforderung nach 30 Tagen (Passwort muss nach 30 Tagen geändert werden und bereits in der Vergangenheit generierte Passwörter können nicht mehr genutzt werden)
- Nutzername darf sich nicht in dem Passwort wiederfinden
- Vorgabe von Sonderzeichen, Groß- und Kleinschreibung innerhalb der Erstellung von Passwörtern
- Erstmalige von dem Auftragnehmer an den Auftraggeber gegebene Passwörter müssen unmittelbar mit der ersten Nutzung des Zuganges geändert werden
- Neu erstellte Passworte werden an die im Portal hinterleget E-Mail-Adresse gesendet
- Supportanfragen, die ggf. eine Auskunft von personenbezogenen Daten mit sich ziehen, werden nur nach Nennung eines im Voraus vergebenen PINS beantwortet
- Installierte physische und softwaretechnischen Firewalls

03. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

- Privatschalter (Sofern gebucht, werden bei Betätigung des Privatschalters die GPS-Ortungsdaten nicht mehr aufgezeichnet.)
- Privattaste Smartphone (Start- und Endpunkt der zurückgelegten Strecke bei dem Produkt Logbook, können im Nachhinein mithilfe der Privattaste der Smartphone-App als Privatfahrt deklariert werden. Hierbei werden die aufgezeichneten Punkte unmittelbar unwiderruflich gelöscht)
- Optionale Möglichkeit der Nutzung von Zeitfiltern, um das Life-Tracking von Personen verhindern zu können
- Portfreigabe-, Portgruppenmanagement

04. Auftragskontrolle

Alle Mitarbeiter des Auftragnehmers sind vertraglich zur Vertraulichkeit verpflichtet worden und werden fortlaufend auf den Bereich Datenschutz sensibilisiert.

Anlage 3

Genehmigte Unterauftragnehmer

Der Auftraggeber stimmt der Beauftragung folgender Sub-Dienstleister zu, die der Auftragnehmer entsprechend den Anforderungen von Art. 28 Abs. 4 DS-GVO unter besonderer Berücksichtigung der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen ausgewählt hat. Der Auftragnehmer bestätigt, dass er sich von der Angemessenheit der technischen und organisatorischen Maßnahmen vorab überzeugt hat.

Lfd. Nummer	Name, Anschrift	Tätigkeitsbeschreibung
01	Wirleless Logic mdex GmbH Bäckerbarg 6 22889 Tangstedt	Externes Rechenzentrum
02	TACHOfresh GmbH Freiheitstraße 120 / Aufgang C 15745 Wildau	Telematikanwendungen (webbasierend)
03	freenet.de GmbH Deelbögenkamp 4 22297 Hamburg	cloudbasierten Software-as-a-Service (SaaS)-Plattform für Fuhrparkmanagement

Anlage 4

Weisungsberechtigte Personen

(Änderungen bei den nachfolgend aufgeführten berechtigten Personen sind der anderen Vertragspartei umgehend schriftlich mitzuteilen.)

Folgende Personen sind zur **Erteilung von Weisungen** befugt:

Zumindest eines der rot umrandeten Felder ist vom Auftraggeber auszufüllen.

Lfd. Nummer	Auftraggeber (Name + E-Mail-Adresse)	Auftragnehmer (Name + E-Mail-Adresse)
01		Volker Gau vga@bornemann.net
02		Tim Blumenberg tbl@bornemann.net

Folgende Personen sind zur **Entgegennahme von Weisungen** befugt:

Zumindest eines der rot umrandeten Felder ist vom Auftraggeber auszufüllen.

Lfd. Nummer	Auftraggeber (Name + E-Mail-Adresse)	Auftragnehmer (Name + E-Mail-Adresse)
01		Volker Gau vga@bornemann.net
02		Tim Blumenberg tbl@bornemann.net