

# Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO

zwischen

und

---

---

---

B+D Datentechnik GmbH

Lübbecker Straße 211

32584 Löhne

- Auftraggeber (Verantwortlicher) -

- Auftragnehmer (Auftragsverarbeiter) -

## 1 Einführung

- 1.1 Die Rechtslage ändert sich mit Anwendbarkeit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (EU - Datenschutzgrundverordnung – (kurz: DS-GVO) ab 25.05.2018. Auch das Bundesdatenschutzgesetz ist mit dem Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 30.06.2017 (Datenschutz-Anpassungs - und- Umsetzungsgesetz EU – DSAnpUG –EU) neu gefasst.

## 2 Gegenstand und Dauer der Vereinbarung

- 2.1 Der Gegenstand des Auftrages ergibt sich aus **Anlage 1**.
- 2.2 Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO nur auf der Grundlage dieses Vertrages.
- 2.3 Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
- 2.4 Diese Vereinbarung wird zum 25.5.2018 wirksam und ersetzt bisherige zur Auftragsverarbeitung getroffenen Vereinbarungen zum Datenschutz und zur Datensicherheit.

## 3 Dauer des Auftrags

- 3.1 Die Dauer des Auftrages ergibt sich aus der **Anlage 1**.
- 3.2 Der Auftraggeber kann den Vertrag ohne Einhaltung einer Frist ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO grob fahrlässig oder vorsätzlich verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen, mithin weder vorsätzlichen noch grob fahrlässigen Verstößen setzt der Auftraggeber eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

## 4 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

- 4.1 Die Art, der Zweck, die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen ergibt sich aus **Anlage 1** bzw. aus der Leistungsbeschreibung des Hauptvertrages.

## 5 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

- 5.1 Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche

Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

- 5.2 Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
- 5.3 Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
- 5.4 Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
- 5.5 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- 5.6 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.
- 5.7 Die Weisungsberechtigten des Auftraggebers sowie die Weisungsempfänger des Auftragnehmers ergeben sich aus der **Anlage 1**.
- 5.8 Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.
- 5.9 Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

## **6 Pflichten des Auftragnehmers**

- 6.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).
- 6.2 Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.
- 6.3 Der Auftragnehmer verpflichtet sich, im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung gemäß der vereinbarten Maßnahmen vorzunehmen.
- 6.4 Er gewährleistet, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert. Das Ergebnis der Kontrollen ist zu dokumentieren.
- 6.5 Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang gegen Vergütung mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an die weisungsberechtigte Person des Auftraggebers weiterzuleiten.
- 6.6 Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

- 6.7 Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechnete Interessen des Auftragnehmers dem nicht entgegenstehen.
- 6.8 Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung zu üblichen Bürozeiten und mit angemessener Vorlaufzeit - berechnete ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO). Der Auftragnehmer hat das Recht seinen Datenschutzbeauftragten hinzuziehen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrolle, sofern davon die Betriebsabläufe des Auftragnehmers gestört werden, nur im erforderlichen Umfang durchgeführt wird.
- 6.9 Der Auftragnehmer ist verpflichtet, soweit erforderlich, bei diesen Kontrollen gegen Vergütung unterstützend mitwirkt.
- 6.10 Für die Verarbeitung von Daten in Privatwohnungen oder mobil hat der Auftragnehmer mit seinen Mitarbeitern eine Regelung getroffen, die den datenschutzrechtlichen Anforderungen entspricht. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall getroffen.
- 6.11 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich auch gemäß **Anlage 1** für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen.
- 6.12 Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.
- 6.13 Der Auftragnehmer verpflichtet sich, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO).
- 6.14 Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb. Die/Der Beauftragte(r) für den Datenschutz Herr/Frau des Auftragnehmers ergibt sich aus **Anlage 1**. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
- 6.15 Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von etwaig genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer erhaltenen, für den Auftraggeber relevanten Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.
- 6.16 Für Verpflichtungen aus diesem Vertrag gilt: Kosten für etwaige Unterstützungsleistung en benennt der Auftragnehmer vorab und sind vom Auftraggeber zu zahlen.
- 7 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten**
- 7.1 Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO.
- 7.2 Der Auftragnehmer verpflichtet sich, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.
- 8 Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)**
- 8.1 Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO.

- 8.2 Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt.
- 8.3 Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.
- 8.4 Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
- 8.5 Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten.
- 8.6 In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern.
- 8.7 Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.
- 8.8 Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).
- 8.9 Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.
- 8.10 Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.
- 8.11 Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.
- 8.12 Zurzeit sind für den Auftragnehmer die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.
- 8.13 Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO). Die Bestellung des Unterauftragnehmers, gegen den Einspruch erhoben wurde, nicht möglich.
- 9 **Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)**
  - 9.1 Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet.
  - 9.2 Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.
  - 9.3 Für die auftragsgemäße Verarbeitung personenbezogener Daten wird eine Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt.
  - 9.4 Das in **Anlage 2** beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.
  - 9.5 Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen

zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber auf Anfrage mitzuteilen.

- 9.6 Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.
- 9.7 Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.
- 9.8 Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

**10 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO**

- 10.1 Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen.

**11 Haftung**

- 11.1 Auf Art. 82 DS-GVO wird verwiesen. Der Auftragnehmer haftet nur dann im Innenverhältnis, wenn der Auftraggeber nachweist, dass der Auftragnehmer für den erlittenen Schaden verantwortlich ist.
- 11.2 Im Übrigen richtet sich die Haftung nach den getroffenen Vereinbarungen aus dem Hauptvertrag.

**12 Sonstiges**

- 12.1 Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
- 12.2 Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.
- 12.3 Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
- 12.4 Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- 12.5 Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

\_\_\_\_\_,den

\_\_\_\_\_,den

\_\_\_\_\_  
Auftraggeber (Verantwortlicher)

\_\_\_\_\_  
Auftragnehmer (Auftragsverarbeiter)

**Gegenstand des Auftrags, Laufzeit, konkrete Beschreibung der Dienstleistungen**

**1 Der Auftrag umfasst Folgendes:**

**IT-Support, Cloudservices, Hotline mittels Software-Tools zur Übertragung von Bildschirmhalten, Consulting, Administration von IT-Systemen, Projektumsetzung, Einführung von Software, Einzelheiten bestimmen sich nach dem Hauptleistungsvertrag**

**1.1 Der Vertrag beginnt mit Unterzeichnung. Gleichzeitig endet der Vertrag mit Beendigung des Hauptleistungsvertrages.**

**1.2 Art und Zweck der vorgesehenen Verarbeitung von Daten**

- Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der jeweiligen Leistungsvereinbarung**

**Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf einer Mitteilung an den Auftraggeber und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.**

**1.3 Art der Daten**

- Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)**

- Personenstammdaten**
- Kommunikationsdaten (z.B. Telefon, E-Mail)**
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)**
- Kundenhistorie**
- Vertragsabrechnungs- und Zahlungsdaten**
- Planungs- und Steuerungsdaten**
- Sonstige? Bitte angeben. \_\_\_\_\_**

**1.4 Kategorien betroffener Personen**

- Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:**
- Kunden**
  - Interessenten**

- Beschäftigte
- Lieferanten
- Ansprechpartner
- Sonstige Dritte
- Sonstige? Bitte angeben. \_\_\_\_\_

**1.5 Weisungsberechtigte Personen des Auftraggebers sind:**

\_\_\_\_\_

**1.6 Weisungsempfänger beim Auftragnehmer sind:**

Thomas Dammeier, Kirsten Grotegut

**1.7 Für Weisung zu nutzende Kommunikationskanäle:**

Alle Weisungen haben mindestens in Textform zu erfolgen.

1.8 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch gemäß Anlage 1 für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

(z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB etc.)

**1.9 Beim Auftragnehmer ist als Beauftragte für den Datenschutz**

Frau Rechtsanwältin Carola Sieling  
 Klingenderstraße 5  
 33100 Paderborn  
 05251-1428742  
[carola.sieling@kanzlei-sieling.de](mailto:carola.sieling@kanzlei-sieling.de)

**1.10 Mit dem Einsatz folgender Subunternehmern ist der Auftraggeber einverstanden:**

	Subunternehmer (Firma und Anschrift)	Teilleistung
	Wortmann AG, Bredenhop 20 in 32609 Hüllhorst	Backup
		Hosting

### Technische und organisatorische Maßnahmen nach der DSGVO des Auftragnehmers

#### 1. Vertraulichkeit (Artikel 32 Abs. 1 lit. b) DSGVO)

##### a) Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen

- Gebäudesicherung
  - Pforte
  - Überwachung des Eingangs per Kamera
  - Bewegungsmelder für Beleuchtung
- Sicherung der Räume
  - Türen
  - Sicherheitsschlösser an Gebäudeeingangstüren
  - Alarmanlage
  - Schlüssel für jeden Mitarbeiter einzeln vorhanden / Schlüsselregelung
  - Rollos an sämtlichen Fenstern, werden außerhalb der Geschäftszeiten heruntergelassen
  - Rollo am Eingang, wird außerhalb der Geschäftszeiten heruntergelassen, nur per Fernbedienung zu öffnen
  - Kein unbegleiteter Publikumsverkehr
  - Zeiterfassungssystem

##### b) Zugangskontrolle: Keine unbefugte Systembenutzung

- Zugang zu Rechnern/Systemen (Authentifizierung)
  - Benutzerkennung mit Passwort
  - Passwortverfahren in Richtlinie geregelt (Mindestlänge, Zeichenzusammensetzung, regelmäßiger Wechsel)
  - Bildschirmsperre bei Pausen mit Passwortaktivierung
  - Zugangssperre bei mehr als 3 Anmeldeversuchen
  - Protokollierung des Zugangs
  - Verschlüsselung mobiler Datenträger, wenn Kundendaten oder personenbezogene Daten betroffen sind
  - Firewall (Securepoint)
  - Virenschanner (Avira)
  - zertifikatsbasierte Zugangsberechtigung (VPN)

##### c) Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

- Berechtigungskonzept
- Benutzerkennung mit Passwort
- Differenzierte Berechtigungen für Kenntnisnahme, Veränderung, Löschung
- Inventarliste
- zertifikatsbasierte Zugriffsberechtigung (VPN)
- Einsatz von Aktenvernichtern
- Richtlinie zur Entsorgung/Vernichtung von Fehldrucken und unbrauchbaren bzw. nicht mehr brauchbaren Datenträgern
- Datenschutzgerechte Löschung verwendeter Datenträger vor neuer Verwendung bzw. Weitergabe durch externen Dienstleister



d) **Trennungskontrolle:** Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

- Physische Trennung von Produktiv- und Testsystemen
- getrennte Ordnerstrukturen (Auftragsdatenverarbeitung)
- getrennte Datenbanken
- separate Tables innerhalb von Datenbanken

e) **Pseudonymisierung** (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO):

Die Verarbeitung von personenbezogener Daten erfolgt, wo geboten und erforderlich 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;

## 2. Integrität, Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

a) **Weitergabekontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

- **Sicherung bei der elektronischen Übertragung**
  - Verschlüsselung der Datenübertragung
  - VPN mit IPSec/ Securepoint SSLVPN
  - Firewall
  - Fax-Protokoll
  - Passwordeingabe bei Fernwartung
- **Sicherung beim Transport**
  - Verschlüsselung
- **Sicherung bei der Übermittlung**
  - Verfahrensverzeichnis
  - Protokollierungsmaßnahmen
- **Löschung gemäß Standard VSITR (*Richtlinien zum Geheimschutz von Verschlusssachen beim Einsatz von Informationstechnik*)**

b) **Eingabekontrolle:** Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

- Protokollierung Teamviewer
- Benutzeridentifikation
- Softwarebezogene Protokollierung

c) **Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit** (Artikel 32 Abs. 1 lit. c) DSGVO): Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust und Vorkehrungen, um möglichst schnell die Daten wieder herzustellen

- **Brandschutzmaßnahmen**
  - Feuerlöscher
  - Rauchmelder
- **Überspannungsschutz**
- **Unterbrechungsfreie Stromversorgung (USV)**
- **Klimaanlage**
- **RAID (Festplattenspiegelung)/ Sicherungskopien**

- Backupkonzept
- Virenschutzkonzept
- Datenlöschkonzept
- Schutz vor Diebstahl

**3. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Artikel 32 Abs. 1 lit. d) DSGVO; Artikel 25 Abs. 1 DSGVO)**

- Bestellung eines Datenschutzbeauftragten
- Datenschutzkonzept
- Regelmäßige interne Überprüfung / Aktualisierung der getroffenen Maßnahmen gemäß dem Stand der Technik (durch DSB, IT-Revision etc.)

**4. Datenschutzfreundliche Voreinstellungen und Datenschutz durch Technikgestaltung (Art. 25 Abs. 2 DSGVO)**

- Minimierung von Pflichtfeldern
- Verwendung von Opt-In-Lösungen
- Richtlinien zur Datenminimierung, Datensparsamkeit und Erforderlichkeit

**5. Auftragskontrolle: Auftragsverarbeitung im Sinne von Art. 28 DSGVO**

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Regelmäßige Überprüfung des Auftragnehmers hinsichtlich Datenschutz/Datensicherheit
- Abschluss von Verträgen zur Auftragsverarbeitung unter Berücksichtigung aller gesetzlichen Anforderungen gemäß Art. 28 DSGVO
- Stichprobenprüfung
- Weisungsbefugnisse festgelegt

Zusätzlich gelten die technischen und organisatorischen Maßnahmen des Subunternehmers als vereinbart, die auf Anfrage gern zur Verfügung gestellt werden.

**AUFTRAGSSPEZIFISCHE MASSNAHMEN ZUR TECHNISCHEN UND ORGANISATORISCHEN DATENSICHERUNG**

Gemäß Vereinbarung mit dem Auftraggeber.