ALLGEMEINE BEDINGUNGEN AUFTRAGSVERARBEITUNG

PRÄAMBEL

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist. Die vorliegende Bedingung konkretisiert als Vereinbarungsbestandteil die zwischen dem Auftragnehmer und Auftraggeber getroffene Vereinbarung.

§ 1 BEGRIFFSBESTIMMUNGEN

1.
Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die alleine oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

2.
Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

3.
Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

4.
Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DS-GVO, biometrischen Daten gem. Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

5.
Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

6.
Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

§ 2 ANGABE DER ZUSTÄNDIGEN DATENSCHUTZ-AUFSICHTSBEHÖRDE

Die zuständige Aufsichtsbehörde für den Auftragnehmer ist die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Kavalleriestr. 2-4, 40213 Düsseldorf. Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 VERTRAGSGEGENSTAND

1.
Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Rahmen des Webseiten-System („Hauptvertrag“). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und der dazugehörigen Leistungsbeschreibung sowie den Anlagen des Hauptvertrages). Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

2.
Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

3.
Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

4.
Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 4 WEISUNGSRECHT

1.
Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

2.
Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus der

Vereinbarung zur Auftragsverarbeitung. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

3.
Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

4.
Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 ART DER VERARBEITETEN DATEN, KREIS DER BETROFFENEN

1.
Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf folgende personenbezogenen Daten: Anschrift, Vorname, Nachname, Telefon, E-Mailadresse.

2.
Der Kreis der von der Datenverarbeitung Betroffenen sind Kunden und Interessenten des Auftraggebers.

§ 6 SCHUTZMASSNAHMEN DES AUFTRAGNEHMERS

1.
Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

2.
Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens folgende Maßnahmen der

a) Zutrittskontrolle
b) Zugangskontrolle
c) Zugriffskontrolle
d) Weitergabekontrolle
e) Eingabekontrolle
f) Auftragskontrolle
g) Verfügbarkeitskontrolle
h) Trennungskontrolle

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3.
Beim Auftragnehmer ist als Datenschutzbeauftragter bestellt:
Dipl. Inform. Olaf Tenti,
GDI Gesellschaft für Datenschutz und Informationssicherheit mbH, datenschutz@gdi-mbh.eu.
Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

4.
Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 INFORMATIONSPFLICHTEN DES AUFTRAGNEHMERS

1.
Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren.
Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

2.
Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

3.
Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

4.
Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO liegen.

5.

Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

6.
Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

7.
Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

8.
An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 KONTROLLRECHTE DES AUFTRAGGEBERS

1.
Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig in angemessenen Abständen von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

2.
Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

3.
Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

4.
Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

5.
Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

§ 9 EINSATZ VON SUBUNTERNEHMERN

1.
Die vertraglich vereinbarten Leistungen werden unter Einschaltung von Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung neuer und/ oder anderen Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

2.
Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 10 ANFRAGEN UND RECHTE BETROFFENER

1.
Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.

2.
Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 11 HAFTUNG

1.
Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

2.
Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

§ 12 BEENDIGUNG DES HAUPTVERTRAGS

1.

Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger des Auftraggebers zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen sind mit einem Aktenvernichter nach DIN 32757-1 zu vernichten. Zu entsorgende Datenträger sind nach DIN 66399 zu vernichten.

2.
Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

3.
Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 13 SCHLUSSBESTIMMUNGEN

1.
Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB und/ oder Vermieterpfandrecht hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

2.
Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

3.
Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

4.
Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist der Sitz des Auftragnehmers.

ANLAGE 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der **Vertraulichkeit, Integrität, Belastbarkeit und Verfügbarkeit** der im Auftrag verarbeiteten Informationen.

Die verarbeiteten personenbezogenen Daten unterliegen bei der Verarbeitung folgender Schutzkategorie:

Normal X **hoch ☐** **sehr hoch ☐**

A. Vertraulichkeit

1. Zutrittskontrolle

(Kein unbefugter Zutritt zu Räumlichkeiten und Datenverarbeitungsanlagen)

1.1. Eingangstüren Gebäude und Büroräume:

Normales Datenschutzniveau:

- **Es existiert ein manuelles Schließsystem** ☒ *Ja* ☐ *Nein*
- Die Türen nach außen sind
  - nur mit starrem Türknauf anstelle einer Klinke ausgestattet ☒ *Ja* ☐ *Nein*
  - mit einem automatischen Zuzieher ausgestattet ☒ *Ja* ☐ *Nein*
  - stets geschlossen, außer zum Betreten und Verlassen ☒ *Ja* ☐ *Nein*
  - während der Geschäftszeiten, außer zum Betreten und Verlassen geschlossen ☒ *Ja* ☐ *Nein*
  - außerhalb der Geschäftszeiten fest abgesperrt ☒ *Ja* ☐ *Nein*

1.2. Fenster:

Normales Datenschutzniveau:

- Fenster sind in allen Lagen außerhalb der Geschäftszeiten geschlossen ☒ *Ja* ☐ *Nein*

1.3. Serverräume:

Normales Datenschutzniveau:

- Es existiert ein manuelles Schließsystem
  ☒ *Ja*
  ☐ *Nein*
  - Die Türen sind nach außen nur mit starrem Türknauf anstelle einer Klinke ausgestattet
    ☒ *Ja*
    ☐ *Nein*
  - mit einem automatischen Zuzieher gesichert
    ☐ *Ja*
    ☒ *Nein*
- Die Reinigung der Serverräume erfolgt innerhalb der Arbeitszeit durch externes Reinigungspersonal
  ☒ *Ja*
  ☐ *Nein*

1.4. Gebäudesicherung außerhalb der Geschäftszeiten:

Normales Datenschutzniveau:

- Es besteht eine Zugangsbeschränkung für Büro- und Geschäftsräume
  ☒ *Ja*
  ☐ *Nein*
- Die Gebäudesicherung außerhalb der Geschäftszeiten erfolgt
  - durch Videoüberwachung
    ☐ *Ja*
    ☒ *Nein*
  - durch Geländeüberwachung
    ☐ *Ja*
    ☒ *Nein*

1.5. Zutrittsregelung für betriebsfremde Personen:

Normales Datenschutzniveau:

- Ein zentraler Empfangsbereich (z. B. Pförtner, Sekretariat) ist vorhanden
  ☒ *Ja*
  ☐ *Nein*
- Zu- und Abgänge von betriebsfremden Personen werden festgestellt
  - durch Besucherlisten
    ☐ *Ja*
    ☒ *Nein*
  - oder persönliche Begleitung durch Mitarbeiter
    ☒ *Ja*
    ☐ *Nein*
  - und protokolliert
    ☐ *Ja*
    ☒ *Nein*
- **Hilfspersonen** (z.B. Reinigungsunternehmen) werden sorgfältig ausgewählt
  ☒ *Ja*
  ☐ *Nein*

1.6. Zutrittsregelung für Mitarbeiter:

Normales Datenschutzniveau:

○ Zutrittsmittel werden ausschließlich an Berechtigte ausgegeben	☒ *Ja* ☐ *Nein*
○ Zutrittsmittel werden sofort eingezogen, wenn die Berechtigung erlischt	☒ *Ja* ☐ *Nein*

2. Zugangskontrolle

(Verhinderung der unbefugten Benutzung der Datenverarbeitungssysteme)

2.1 Sicherstellung des berechtigten Zugangs:

Normales Datenschutzniveau:

○ Ein *Passwortsystem* für den Zugriff auf die Datenverarbeitungssysteme ist eingerichtet	☒ *Ja* ☐ *Nein*
○ Jeder Berechtigte erhält eine individuelle Benutzerkennung und ein persönliches, geheim zu haltendes Passwort, das nicht an Dritte weitergegeben werden darf	☒ *Ja* ☐ *Nein*
○ Es existiert organisatorisch eine Richtlinie zur Passwortsicherheit	☒ *Ja* ☐ *Nein*
○ Zur Anmeldung muss ein Passwort eingegeben werden	☒*Ja* ☐ *Nein*
○ Das Passwort besteht aus wenigstens 8 Zeichen (zufällig ausgewählten Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen)	☒ *Ja* ☐ *Nein*
○ Generische Begriffe oder Eigennamen dürfen verwendet werden	☐ *Ja* ☒ *Nein*
○ Eine Authentifizierung erfolgt über Benutzername *und* Passwort	☒ *Ja* ☐ *Nein*
○ Es besteht eine Regelung für den Fall der Abwesenheit (Urlaub, Krankheit etc.)	☐ *Ja* ☒ *Nein*
○ Berechtigungen werden regelmäßig kontrolliert	☐ *Ja* ☒ *Nein*
○ Das Passwort wird sofort gesperrt, falls die Berechtigung erlischt	☒ *Ja* ☐ *Nein*

2.2 Schutz vor unberechtigtem Zugang von außen:

Normales Datenschutzniveau:

- Interne Netze werden nach dem Stand der Technik gegen Zugriffe von außen durch Firewalls abgeschottet — ☒ *Ja* ☐ *Nein*
- Private Speichermedien sind vertraglich oder durch Organisationsanweisung verboten — ☒ *Ja* ☐ *Nein*
- Es besteht eine Organisationsanweisung zum Download von Apps auf dienstliche Endgeräte — ☒ *Ja* ☐ *Nein*

Hohes Datenschutzniveau:

- Interne Netze werden nach dem Stand der Technik gegen Zugriffe von außen durch Verschlüsselung abgeschottet — ☐ *Ja* ☐ *Nein*
- Bestimmungsgemäße Zugriffe von außen werden durch Virtual Private Network (VPN) abgesichert — ☐ *Ja* ☐ *Nein*
- Interne Schnittstellen (USB-Port, Disketten-/ CD-Laufwerke etc.) werden gesperrt — ☐ *Ja* ☐ *Nein*
- Daten / Festplatten von mobilen Endgeräten (Blackberry, Notebook, USB-Stick etc.) werden verschlüsselt — ☐ *Ja* ☐ *Nein*
- Schutzprogramme und Administrationsprogramme auf Smartphones und Tablet-PCs sind im Einsatz — ☐ *Ja* ☐ *Nein*
- Der Download von Apps auf dienstliche Endgeräte erfolgt nur durch die IT — ☐ *Ja* ☐ *Nein*

3. Zugriffskontrolle

(Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen innerhalb des Datenverarbeitungssystems)

3.1 Berechtigungskonzept

Normales Datenschutzniveau:

- Der Zugriff auf Computersysteme und Netzlaufwerke ist auf berechtigte Benutzer beschränkt — ☒ *Ja* ☐ *Nein*
- Der Zugriff auf Backup-Datenträger ist auf Systemadministratoren beschränkt — ☒ *Ja* ☐ *Nein*

○ Es existiert ein Berechtigungskonzept	☒ *Ja* ☐ *Nein*
○ Das Berechtigungskonzept umfasst die Verwaltung der Zugriffsrechte durch Systemadministratoren	☒ *Ja* ☐ *Nein*
○ Es werden Benutzerprofile erstellt und den Datenverarbeitungssystemen zugeordnet	☒ *Ja* ☐ *Nein*
○ Die Beantragung, Genehmigung, Vergabe und Rückgabe von Zugriffsberechtigungen ist in einer Organisationsanweisung geregelt	☐ *Ja* ☒ *Nein*
○ Die mit der Verarbeitung von Daten befassten Mitarbeiter verfügen auch über Administratorenrechte für die zu diesen Zwecken eingesetzten Systeme	☐ *Ja* ☒ *Nein*
○ Nicht benötigte Ports (USB) und Wechselmedien (CD/DVD-Geräte) werden deaktiviert und gesichert	☐ *Ja* ☒ *Nein*
○ Datenträger werden vor einer Wiederverwendung mit geeigneter Software überschrieben	☐ *Ja* ☒ *Nein*
○ Die Internet- und E-Mail-Nutzung erfolgt kontrolliert und organisiert	☒ *Ja* ☐ *Nein*
○ Erfolgte / versuchte Sicherheitsverletzungen werden gemeldet und ausgewertet	☐ *Ja* ☒ *Nein*

3.3 Trennungskontrolle und Pseudonymisierung

(Art. 32 Abs. 1 a DSGVO)

Normales Datenschutzniveau:

○ Büroräume, Archive und Server werden von Fremdfirmen mitbenutzt	☐ *Ja* ☒ *Nein*
○ Daten werden physisch getrennt auf gesonderten Systemen, Laufwerken und Datenträgern gespeichert	☒ *Ja* ☐ *Nein*
○ Daten für mehr als einen Verantwortlichen werden in einer mandantenfähigen Datenbank verarbeitet	☒ *Ja* ☐ *Nein*

3.4 Zugriff auf Datenträger und Datenträgervernichtung:

Normales Datenschutzniveau:

○ Nicht mehr benötigte Datenträger und Fehldrucke werden datenschutzgerecht entsorgt	☒ *Ja* ☐ *Nein*
○ Datenträger werden ordnungsgemäß vernichtet, durch physische Zerstörung	☒ *Ja* ☐ *Nein*
○ Papier wird vernichtet durch Reißwolf, Schredder	☒ *Ja* ☐ *Nein*
○ Bei Lagerung von nicht mehr benötigten Datenträgern und Fehldrucken sind geeignete Datenschutzbehälter zur Verhinderung unbefugter Entnahmen im Einsatz	☐ *Ja* ☒ *Nein*

B. Integrität, Weitergabekontrolle, Auftragskontrolle und Fernwartung (Art. 32 Abs. 1 b DSGVO)

1. Weitergabekontrolle

(Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport)

Normales Datenschutzniveau:

○ Bei den zur Verarbeitung von Daten eingesetzten Systemen sind Bildschirme oder andere Ausgabegeräte so angeordnet, dass unbefugte Dritte keinen Einblick in Daten nehmen können	☒ *Ja* ☐ *Nein*
○ Als Sicherheitsmaßnahmen werden Firewalls eingesetzt	☒ *Ja* ☐ *Nein*
○ Auch bei der Weitergabe von Daten werden Passwörter mit Vorgaben für die Passwortsicherheit eingesetzt	☐ *Ja* ☒ *Nein*

2. Eingabekontrolle und Protokollierung:

(Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungs-systemen eingegeben, verändert oder entfernt worden sind)

Normales Datenschutzniveau:

○ Unbefugte Eingaben, Veränderungen und Löschungen werden durch ein Passwortsystem (s. 2. Zugangskontrolle) verhindert	☒ *Ja* ☐ *Nein*
○ Die Eingabeberechtigungen werden schriftlich erteilt	☐ *Ja* ☒ *Nein*
○ Zugriffe sind anhand der *Benutzergruppen* nachvollziehbar	☒ *Ja* ☐ *Nein*

3. Fernwartung

- Eine Fernwartung von Datenverarbeitungsanlagen und/oder Software findet statt ☒ *Ja* ☐ *Nein*
- Es besteht eine gesicherte Verbindung bei Fernwartung ☒ *Ja* ☐ *Nein*
- Es wurde ein Wartungsvertrag abgeschlossen ☒ *Ja* ☐ *Nein*

Folgende Maßnahmen werden zur Sicherung der Fernwartung angewendet

- Ereignisauslösung vom Auftraggeber ☒ *Ja* ☐ *Nein*
- Rückrufautomatik ☐ *Ja* ☒ *Nein*
- Einmal-Passwort ☐ *Ja* ☒ *Nein*
- Virtual Private Network (VPN) ☒ *Ja* ☐ *Nein*
- Protokollierung der Datenübermittlung und der Empfänger ☐ *Ja* ☒ *Nein*
- Auswertungsmöglichkeiten der Übermittlungsprotokolle ☐ *Ja* ☒ *Nein*
- Sonstige: ..... ☐ *Ja* ☒ *Nein*

C. Wiederherstellbarkeit der Daten und des Datenzugangs nach physischem oder technischem Zwischenfall und Kontrollverfahren

1. Datensicherung (Art. 32 Abs. 1 c DSGVO)

Normales Datenschutzniveau:

- Sicherungskopien werden nach dem Generationenprinzip in geeigneten zeitlichen Abständen erstellt ☒ *Ja* ☐ *Nein*

Der Datenbestand wird wenigstens

- einmal täglich inkrementell ☒ *Ja* ☐ *Nein*

- einmal wöchentlich vollständig auf externen Speichermedien

☒ *Ja*
☐ *Nein*

gesichert

- Die jeweils letzte vollständige Sicherungskopie wird unmittelbar nach ihrer Erstellung an einem sicheren Ort in der gleichen Immobilie untergebracht (anderer Brandschutzbereich)

☒ *Ja*
☐ *Nein*

2. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 d DSGVO)

- Die vorhandenen Dokumentationen der Datensicherheit werden regelmäßig auf Aktualität geprüft

☐ *Ja*
☒ *Nein*

- Es erfolgt mindestens jährlich ein technischer Check der Datenverarbeitungssysteme

☒ *Ja*
☐ *Nein*

- Protokolle über alle Aktivitäten auf dem Datenverarbeitungssystem werden auf etwaige Unregelmäßigkeiten in regelmäßigen zeitlichen Abständen ausgewertet

☐ *Ja*
☒ *Nein*

☐ *Ja* ☐ *Nein*

- Sicherheitsvorfälle werden dokumentiert und ausgewertet

☐ *Ja*
☒ *Nein*

- Es besteht ein für Sicherheitsvorfälle geschultes Krisenteam

☐ *Ja*
☒ *Nein*

- Es werden Tests zur Simulation von Sicherheitsvorfällen durchgeführt und die Ergebnisse dokumentiert

☐ *Ja*
☒ *Nein*

- Es erfolgen interne Audits durch den betrieblichen Datenschutzbeauftragten oder die IT

☐ *Ja*
☒ *Nein*

- Es erfolgen externe Audits durch zertifizierte Prüfer

☒ *Ja*
☐ *Nein*

- Das Unternehmen wurde nach festgelegten Sicherheitskriterien zertifiziert

☐ *Ja*
☒ *Nein*

Art der Zertifizierung:

.....

Anmerkungen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

.....
.....
.....

3. Organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs-1 d DSGVO)

3.1. Datenschutzbeauftragter:

○ Ein betrieblicher Datenschutzbeauftragter ist erforderlich	☒ *Ja* ☐ *Nein*
○ Ein betrieblicher Datenschutzbeauftragter wurde bestellt	☒ *Ja* ☐ *Nein*
○ Stellung des betrieblichen Datenschutzbeauftragten:	
○ hauptamtlich	☐ *Ja* ☒ *Nein*
○ nebenamtlich	☐ *Ja* ☒ *Nein*
○ extern	☒ *Ja* ☐ *Nein*
○ Der Datenschutzbeauftragte oder von ihm oder der Geschäftsleitung beauftragte Mitarbeiter führen regelmäßig interne Kontrollen der Einhaltung der technischen und organisatorischen Maßnahmen der Datensicherheit durch	☒ *Ja* ☐ *Nein*

3.2. Vertraulichkeit der Mitarbeiter

○ Alle Mitarbeiter, die personenbezogene Daten verarbeiten, sind auf Vertraulichkeit (das Datengeheimnis) verpflichtet	☒ *Ja* ☐ *Nein*
○ Fremdpersonal ist ebenfalls auf Vertraulichkeit verpflichtet	☒ *Ja* ☐ *Nein*
○ Datenschutzschulungen für die Mitarbeiter werden regelmäßig durchgeführt	☒*Ja* ☐ *Nein*
○ Ist die private Nutzung betrieblicher Kommunikationstechnik geregelt?	☒ *Ja* ☐ *Nein*

- Ist die private Nutzung betrieblicher Kommunikationstechnik verboten? ☐ *Ja* ☒ *Nein*
- Wird Adressmarketing betrieben? ☒ *Ja* ☐ *Nein*
- Falls ja: Werden Direkt-/Adressmarketing nach datenschutzrechtlichen Vorgaben betrieben? ☒ *Ja* ☐ *Nein*
- Wird Cloud-Computing eingesetzt? ☒ *Ja* ☐ *Nein*
- Falls ja: Wird Cloud-Computing nach datenschutzrechtlichen Vorgaben eingesetzt? ☒ *Ja* ☐ *Nein*
- Existiert ein dokumentiertes Datenschutzkonzept? ☒ *Ja* ☐ *Nein*

Anmerkungen zum den organisatorischen Maßnahmen

.....
.....
.....

E. Internetauftritt

- Existiert eine Datenschutzerklärung/Datenschutzhinweise? ☒ *Ja* ☐ *Nein*
- Existiert eine Anbieterkennzeichnung? ☒ *Ja* ☐ *Nein*
- Sind kommerzielle Kommunikation / Inhalte gekennzeichnet? ☒ *Ja* ☐ *Nein*
- Wird Tracking-Software eingesetzt? ☒ *Ja* ☐ *Nein*
  - Falls ja: Wird Tracking-Software gemäß datenschutzrechtlicher Vorgaben eingesetzt? ☒ *Ja* ☐ *Nein*
- Besteht die Möglichkeit, Tracking zu widersprechen? ☒ *Ja* ☐ *Nein*
- Wird Google Analytics eingesetzt? ☒ *Ja* ☐ *Nein*
  - Falls ja: Erfolgt der Einsatz von Google Analytics unter folgenden Voraussetzungen:

- Schriftlicher Vertrag zur Auftragsdatenverarbeitung ☒ *Ja* ☐ *Nein*
- Hinweis in Datenschutzerklärungen ☒ *Ja* ☐ *Nein*
- Widerspruchsmöglichkeit ☒ *Ja* ☐ *Nein*
- Einbindung der Anonymisierungsfunktion in Quellcode ☒ *Ja* ☐ *Nein*

- Werden Social Media eingesetzt? ☒ *Ja* ☐ *Nein*
  - Falls ja: Existieren Social Media Guidelines für den Umgang mit Facebook, Google+, Twitter etc.? ☒ *Ja* ☐ *Nein*

Anmerkungen zum Internetauftritt:

.....
.....
.....