AUFTRAGSVERARBEITUNGSVERTRAG

GEMÄß ART. 28 UND 29 DSGVO

VEREINBARUNG

zwischen dem / der

- nachstehend Auftraggeber genannt –

und der

Hees GmbH
Leimbachstr. 266
57074 Siegen

- nachstehend Auftragnehmer genannt –

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand des Auftrags

Definition der Aufgaben:

1.2 Dauer des Auftrags

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von zum gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Auftragsinhalt

Der Auftragnehmer ist verpflichtet, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden.

Dem Auftragnehmer ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Duplikatsdateien zur leistungsgemäßen Verarbeitung oder Nutzung der personenbezogenen Daten zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt.

Dem Auftragnehmer ist nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen.

Daten aus Adressbüchern und Verzeichnissen dürfen nur zur Kommunikation im Rahmen der Auftragserfüllung mit dem Auftraggeber verwendet werden. Eine anderweitige Nutzung und Übermittlung für eigene oder fremde Zwecke, einschl. Marketingzwecke, ist nicht gestattet.

Weitere Einzelheiten zu Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder –nutzung sind unter Buchstabe A. der Anlage 1 zu dieser Vereinbarung aufgeführt.

Die Art der personenbezogenen Daten sind unter Buchstabe B. der Anlage 1 aufgeführt.

Der Kreis der Personen ist unter Buchstabe C. der Anlage 1 aufgeführt

3. Technisch-organisatorische Maßnahmen

Der Auftragnehmer trifft alle erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, soweit ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Die insoweit konkret getroffenen Maßnahmen ergeben sich aus **Anlage 2** zu dieser Vereinbarung.

Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieses Auftrags sind die technischen und organisatorischen Maßnahmen durch den Auftragnehmer fortlaufend an die Anforderungen dieses Auftrags anzupassen und dem technischen Fortschritt

entsprechend weiterzuentwickeln. Das Sicherheitsniveau der hier und in der **Anlage 2** festgelegten technischen und organisatorischen Maßnahmen darf nicht unterschritten werden.

Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber, auf Anfrage, die für die Führung der internen Verarbeitungsübersicht nach DSGVO erforderlichen Angaben zur Verfügung zu stellen.

4. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Erfüllung seiner Pflichten im Zusammenhang mit den Rechten betroffener Personen gemäß Art. 15 bis 22 DSGVO.

Hierzu gehört insbesondere die Mitwirkung bei der Bearbeitung von Anträgen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit sowie Widerspruch. Der Auftragsverarbeiter stellt dem Verantwortlichen die hierfür erforderlichen Informationen zur Verfügung und setzt auf Weisung des Verantwortlichen geeignete technische und organisatorische Maßnahmen um, soweit dies zur Erfüllung der Betroffenenrechte erforderlich ist.

5. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach Art. 28, 29 u. EG81ff folgende Pflichten:

- Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 37 Abs. 1 DSGVO ausüben kann. Die Kontaktdaten des Datenschutzbeauftragten entnehmen Sie bitte der Anlage 3.
- Die Wahrung des Datengeheimnisses entsprechend Art. 29 DSGVO. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.
- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Art. 24, 25, 32, 35, 36 u. EG 78, 98ff DSGVO und Anlage.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde. Dies gilt auch, soweit eine zuständige Behörde nach Art. 34 DSGVO beim Auftragnehmer ermittelt.
- Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren,

Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001 oder VdS 3473) vorlegen. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten gemäß Art. 32 bis 36 DSGVO.

Insbesondere wirkt der Auftragnehmer im erforderlichen Umfang bei der Umsetzung und Bewertung geeigneter technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO mit, unterstützt den Auftraggeber bei der Erkennung, Untersuchung und Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 und 34 DSGVO und stellt die hierfür notwendigen Informationen zur Verfügung.

Ferner unterstützt der Auftragnehmer den Auftraggeber bei der Durchführung von Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO sowie bei gegebenenfalls erforderlichen Konsultationen der zuständigen Aufsichtsbehörde gemäß Art. 36 DSGVO, soweit die jeweilige Verarbeitung in seinem Verantwortungs- und Einflussbereich liegt.

6. Unterauftragsverhältnisse

Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

- Die Einschaltung von Unterauftragnehmern ist grundsätzlich nur mit schriftlicher Zustimmung des Auftraggebers gestattet.
- Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem / den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.
- Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

7. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu Art. 5, 25, 32, 35, 36 DSGVO vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die mit einer Frist von 14 Tagen anzukündigen sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

Im Falle eines Sicherheitsvorfalls kann der Auftragnehmer die Ausübung von Kontrollrechten des Auftraggebers vorübergehend einschränken, soweit und solange dies erforderlich ist, um:

- die Behebung des Vorfalls nicht zu gefährden,
- die IT-Sicherheit aufrechtzuerhalten,
- behördliche Ermittlungen nicht zu beeinträchtigen.

Der Auftragnehmer informiert den Auftraggeber unverzüglich über die Gründe und Dauer der Einschränkung und stellt nach Wegfall der Gründe die Kontrollrechte wieder vollständig her

Im Hinblick auf mögliche Kontrollverpflichtungen des Auftraggebers vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß **Art. 32 DSGVO**, und der Anlage 2 nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheitsoder Datenschutzaudit (z.B. ISO 27001 oder VdS 3473) erbracht werden.

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

Es ist bekannt, dass nach Art. 34 DSGVO Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung spätestens innerhalb von 24 Stunden nach Bekanntwerden dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach Art. 34 DSGVO treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

9. Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, sofern er nicht durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zu einer hiervon abweichenden Verarbeitung verpflichtet ist.

(2) Ist der Auftragsverarbeiter aufgrund einer solchen rechtlichen Verpflichtung gehalten, von den Weisungen des Verantwortlichen abzuweichen, informiert er den Verantwortlichen unverzüglich über die betreffende rechtliche Anforderung und die daraus resultierende Abweichung von der Weisung, bevor er die Verarbeitung durchführt, sofern das einschlägige Recht eine solche Information nicht aus wichtigen Gründen des öffentlichen Interesses untersagt.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers auszuhändigen oder datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

11. Drittlandübermittlung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich innerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR). Eine Übermittlung personenbezogener Daten im Sinne der Art. 44 ff. DSGVO in Staaten außerhalb der EU bzw. des EWR (Drittländer) findet nicht statt.

Ort, Datum	Ort, Datum
Auftraggeber	Auftragnehmer

Liste der Unterauftragnehmer:

Anlage 1: A. Ergänzungen zu § 2 Umfang, Art und Zweck der Datenverarbeitung
B.Aufführung der Art der Daten gemäß § 2
C.Kreis der Personen gemäß § 2

Anlage 2: Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Anlage 3: Datenschutzbeauftragte gemäß Art. 37 Abs. 1 DSGVO

ANLAGE 1

A. Zu § 2 Ergänzungen zu Umfang, Art und Zweck der Datenverarbeitung

B. Zu § 2 Art der personenbezogenen Daten

(maßgebliche Datenarten sind angekreuzt)

- ☐ Adressdaten
- ☐ Kontaktdaten
- ☐ Vertragsdaten
- ☐ Bankverbindungsdaten
- ☐ Kontodaten
- ☐ Abrechnungsdaten inkl. Bonuszahlungen
- ☐ Leistungsdaten
- ☐ Finanzdaten
- ☐ Angebotsdaten
- ☐ Mitarbeiter-/Personaldaten
- ☐ Pensionsdaten
- ☐ Bewerberdaten
- ☐ Qualifikationsdaten
- ☐ Videoaufzeichnungen
- ☐ Gesundheitsdaten
- ☐ Angaben zur Konfessionszugehörigkeit
- ☐ Angaben zu Schwerbehinderungen
- ☐ Krankheitsdaten
- ☐ Zeitdaten,
- ☐ Informationen zu Abfindungszahlungen
- ☐ Reisebuchungs- und kostendaten,
- ☐ Kreditkartenabrechnungen

Andere Kategorien personenbezogener Daten:

C.Zu § 2 Kreis der Personen

- ☐ Mitarbeiter
- ☐ Kunden
- ☐ Praktikanten
- ☐ Bewerber
- ☐ Lieferanten/Dienstleister
- ☐ Sonstige:

ANLAGE 2

Bei der Hees Gruppe werden insbesondere folgende technische und organisatorische Maßnahmen im Detail getroffen, um den Schutz von Daten zu gewährleisten, dies schließt personenbezogene Daten jeder Kategorie ein.

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

1.1. Zutrittskontrolle

Folgende Maßnahmen verhindern, dass unbefugte Personen Zutritt zu Datenverarbeitungsanlagen haben:

- ☒ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)
- ☒ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)
- ☒ Sicherheitstüren / -fenster
- ☐ Gitter vor Fenstern/Türen
- ☒ Zaunanlagen
- ☒ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- ☒ Werkschutz, Pförtner
- ☒ Alarmanlage
- ☐ Videoüberwachung
- ☒ Spezielle Schutzvorkehrungen des Serverraums
- ☒ Spezielle Schutzvorkehrungen für die Aufbewahrung von Backups und anderen Datenträgern
- ☒ Nicht-reversible Vernichtung von Datenträgern
- ☒ Mitarbeiter- und Berechtigungsausweise
- ☒ Sperrbereiche
- ☒ Besucherregelung (z.B. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)
- ☐ Andere Maßnahmen: _____

Anlage 2 zu Auftragsverarbeitungsvereinbarung: Technische und organisatorische Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus gemäß Art. 32 DSGVO

1.2. Zugangskontrolle

Folgende Maßnahmen verhindern, dass unbefugte Dritte Zugang zu Datenverarbeitungsanlagen haben:

☒ Persönlicher und individueller Login bei Anmeldung am System/Netzwerk
☒ Autorisierungsprozess für Zugangsberechtigungen
☒ Begrenzung der befugten Benutzer
☒ Single Sign-On
☒ BIOS-Passwörter
☒ Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
8 Zeichen, Groß -und Kleinschreibung, Zahl und Sonderzeichen, 90 Tage Gültigkeit
☒ Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
☒ Personalisierte Chipkarten, Token, PIN-/TAN, etc.
☒ Protokollierung des Zugangs
☒ Zusätzlicher Login für bestimmte Anwendungen
☒ Automatische Sperrung der Clients nach Zeitablauf ohne Useraktivität
☒ Firewall
☐ Andere Maßnahmen: _____

1.3. Zugriffskontrolle

Folgende Maßnahmen stellen sicher, dass unbefugte Dritte keinen Zugriff auf Daten haben:

☒ Verwaltung und Dokumentation von differenzierten Berechtigungen
☒ Abschluss von Verträgen zur Auftragsverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von Daten Gegenstand der Leistung des Auftragnehmers ist.
☒ Auswertungen/Protokollierungen von Datenverarbeitungen
☒ Autorisierungsprozess für Berechtigungen
☐ Genehmigungsroutinen
☒ Profile/Rollen
☒ Verschlüsselung von Datenträgern
☒ Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf mobile Datenträger (z.B. Kopierschutz, Sperrung von USB-Ports, Data Loss Prevention System/DLP)
☒ Mobile Device Management (MDM)
☒ Vier-Augen-Prinzip
☒ Funktionstrennung (Segregation of Duties)
☒ Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399
☒ Nicht-reversible Löschung von Datenträgern
☒ Sichtschutzfolien für mobile Datenverarbeitungsanlagen
☐ Andere Maßnahmen: _____

1.4. Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

☐ Speicherung der Datensätze in physikalisch getrennten Datenbanken
☒ Verarbeitung auf mindestens logisch getrennten Systemen
☒ Zugriffsberechtigungen nach funktioneller Zuständigkeit
☒ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
☒ Mandantenfähigkeit von IT-Systemen
☒ Verwendung von Testdaten
☒ Trennung von Entwicklungs- und Produktionsumgebung
☐ Andere Maßnahmen: _____

Anlage 2 zu Auftragsverarbeitungsvereinbarung: Technische und organisatorische Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus gemäß Art. 32 DSGVO

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

Die Verarbeitung von Daten erfolgt so, 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 (Art. 32 Abs. 1 lit. b DS-GVO)

2.1.Weitergabekontrolle

Es ist sichergestellt, dass Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert, entfernt oder sonst verarbeitet werden können und überprüft werden kann, welche Personen oder Stellen Zugriff auf Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

☒ Verschlüsselung von E-Mail oder E-Mail-Anhängen
☒ Verschlüsselung von Datenträgern
☒ Gesicherter File Transfer oder sonstiger
☐ Physikalische Transportsicherung
☒ Verpackungs- und Versandvorschriften
☐ Qualifizierte elektronische Signatur
☒ Verschlüsseltes WLAN
☒ Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort)
☒ Mobile Device Management (MDM)
☒ Data Loss Prevention System (DLP)
☒ Regelung zum Umgang mit mobilen Datenträgern (z.B. Laptop, USB-Stick, Mobiltelefon)
☒ Protokollierung von Datenübertragung oder Datentransport
☒ Protokollierung von lesenden Zugriffen
☐ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten
☐ Andere Maßnahmen: _____

2.2. Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- ☒ Zugriffsrechte
- ☒ Systemseitige Protokollierungen
- ☒ Dokumenten Management System (DMS)
- ☒ Sicherheits-/Protokollierungssoftware
- ☒ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- ☐ Vieraugenprinzip
- ☒ Data Loss Prevention System (DLP)
- ☐ Andere Maßnahmen: _____

§3 VERFÜGBARKEIT UND BELASTBARKEIT (ART. 32 ABS. 1 LIT. B DS-GVO)

Durch folgende Maßnahmen ist sichergestellt, dass Daten gegen zufällige Zerstörung oder Verlustgeschützt und für den Auftraggeber stets verfügbar sind:

- ☒ Sicherheitskonzept für Software- und IT-Anwendungen
- ☒ Backup Verfahren
- ☒ Aufbewahrungsprozess für Backups (z.B. brandgeschützter Safe, getrennter Brandabschnitt)
- ☒ Gewährleistung der Datenspeicherung im gesicherten Netzwerk
- ☒ Bedarfsgerechtes Einspielen von Sicherheits-Updates
- ☒ Spiegeln von Festplatten
- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☒ Geeignete Archivierungsräumlichkeiten für Papierdokumente
- ☒ Brand- und/oder Löschwasserschutz des Serverraums
- ☒ Brand- und/oder Löschwasserschutz der Archivierungsräumlichkeiten
- ☒ Klimatisierter Serverraum
- ☒ Virenschutz
- ☒ Firewall
- ☒ Notfallplan
- ☒ Erfolgreiche Notfallübungen
- ☒ Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)
- ☐ Andere Maßnahmen: _____

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

4.1. Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- ☒ Datenschutzleitbild des Anbieters
- ☒ Datenschutz-Richtlinie des Anbieters
- ☒ Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit
- ☒ Benennung eines Datenschutzbeauftragten
- ☒ Verpflichtung der Mitarbeiter auf die Vertraulichkeit
- ☒ Hinreichende Schulungen der Mitarbeiter im Datenschutz
- ☒ Führen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO)
- ☒ Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)
- ☒ Externe Prüfung oder Auditierung
- ☐ Andere Maßnahmen: _____

4.2. Management bei Datenschutzverletzungen

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- ☒ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- ☒ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüberbetroffenen Personen (Art. 34 DSGVO)
- ☐ Andere Maßnahmen:

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

Datenschutzfreundliche Voreinstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Verarbeitungen zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben oder Eingabemöglichkeiten festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden.

Anlage 2 zu Auftragsverarbeitungsvereinbarung: Technische und organisatorische Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus gemäß Art. 32 DSGVO
Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden) oder die Verfügbarkeit bestimmter Verarbeitungen, Funktionen oder Protokollierungen.

4.4. Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass Daten nur nach Weisungen des Auftraggebers verarbeitet werden:

- ☒ Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten der Parteien
- ☒ Prozess zur Erteilung und/oder Befolgung von Weisungen
- ☐ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- ☐ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- ☒ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Anbieter
- ☐ Unabhängige Auditierung der Weisungsgebundenheit
- ☒ Verpflichtung der Beschäftigten auf die Vertraulichkeit
- ☐ Vereinbarung von Vertragsstrafen für Verstöße gegen Weisungen
- ☐ formalisiertes Auftragsmanagement
- ☐ dokumentiertes Verfahren zur Auswahl von Unterauftragnehmern
- ☐ standardisiertes Vertragsmanagement zur Kontrolle von Unterauftragnehmern
- ☐ Andere Maßnahmen: _____

Sollten darüber hinaus Details zu den aufgeführten Maßnahmen gewünscht sein, so kann der Informationssicherheitsbeauftragte der HEES Gruppe Auskunft geben:

FELIX KREUZ
Tel: 0271.4881-387
Mail: felix.kreuz@hees.de

ANLAGE 3

Zur Datenschutzbeauftragte für die Unternehmen der HEES Gruppe wurde bestellt:

Hees GmbH
Leimbachstraße 266
57074 Siegen
Webseite: www.hees.de

LENA FERAJ
Datenschutzbeauftragte
E-Mail: datenschutz@hees.de