Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

1. Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags
Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

Bereitstellung von IT-Dienstleistungen einschließlich die Wartung und der Support per Fernzugriff und auch vor Ort.

Dauer des Auftrags
Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 14 Tagen gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts:

Art und Zweck der vorgesehenen Verarbeitung von Daten
Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

Personenbezogene Daten werden lediglich vom Auftraggeber als Anwendungsdaten erzeugt. Der Auftragnehmer erhebt, verarbeitet oder nutzt diese Daten nicht. Allerdings ist es anlässlich der Arbeiten zu unter 1. genannten Gegenstand nicht ausgeschlossen, dass der Dienstleister rein zufällig Kenntnis von solchen personenbezogenen Daten erhält.

Eigens vom Auftragnehmer aus dem Auftragsverhältnis erhobene, verarbeitete, gespeicherte und genutzte Daten beziehen sich auf Daten, die für die Erfüllung von Aufgaben notwendig sind. Jene betreffen die Kontaktdaten von Ansprechpartnern, Angaben zu in Projekten oder Supportfällen relevante Personen (bspw. Auftraggeber, Melder/Verursacher/Betroffener einer Störung) oder Angaben zu Anwendern, für die ein Benutzerkonto eingerichtet wird.

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 der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)
Die durch den Auftraggeber erzeugten Anwendungsdaten können „einfache“ personenbezogene Daten darstellen als auch besondere personenbezogene Daten sein; die Verarbeitung zu systemadministrativen Zwecken erstreckt sich potentiell auf alle Daten.

Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
☒ Kunden
☒ Interessenten
☒ Abonnenten
☒ Beschäftigte i. S. d. § 3 Abs. 11 BDSG
☒ Lieferanten
☒ Handelsvertreter
☒ Ansprechpartner

3. Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen 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

siehe Anlage 1

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen
unverzüglich an den Auftraggeber weiterleiten.

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung,

Daten Portabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten siehe Anhang].

- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen

- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt

- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard-und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

7. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch

Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge
- unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen,
die die Umstände und Zwecke der
Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch
Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm
in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf kein

Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

Kopien oder Duplikate der Daten 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.

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der
Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse
sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung 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.

ANLAGE 1: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

1. Verantwortliche Stelle

Firma: Systemhaus Erdmann GmbH & Co.KG
Straße: Heiligenstock 34c
PLZ/Ort: 42697 Solingen
Telefon: 0212 65985-0
Fax: 0212 65985-20
E-Mail: info@systemhaus-erdmann.de
Internet Adresse (URL): www.systemhaus-erdmann.de
Fachverantwortlicher für dieses Verfahren: Tobias Erdmann
Organisationseinheit: Geschäftsführer

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

Zutrittskontrolle:
Abgeschlossene Serverräume
Alarmanlage
Besucherbuch/Besucherliste
Schlüsselregelung/Schlüsselbuch
Sicherheitsschlösser
Regelungen für Zutritt zu Serverräumen externer Personen
Regelmäßige Überprüfung der Schutzmaßnahmen für Serverräume.
Personenkontrolle beim Empfang
Chipkarten-/Transponder-Schließsystem

Zugangskontrolle:
Authentifikation mit Benutzer und Passwort
Einsatz von Anti-Viren-Software
Einsatz von Firewalls
Einsatz von VPN-Technologie
Erstellen von Benutzerprofilen
Passwortvergabe/Passwortregeln
Personenkontrolle beim Empfang
Regelung für den Umgang mit Passwörtern
Schlüsselregelung/Schlüsselbuch
Protokollierung der Besucher/Besucherbuch
Sorgfältige Auswahl von Reinigungspersonal
Verschlüsselung von Datenträgern
W-LAN ist gesichert
Verschlüsselung von Smartphones

Zugriffskontrolle:

Anzahl der Administratoren auf das Mindeste begrenzt
Clean Desk
Einsatz von Aktenvernichtern
Passwortrichtlinie inkl. Länge und Wechsel
Sichere Aufbewahrung von Datenträgern

Verschlüsselung von Datenträgern
Verschlüsselung von Smartphones
Verwaltung der Benutzerrechte durch Systemadministratoren
Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

Trennungskontrolle:

Erstellen eines Berechtigungskonzepts.
Logische Mandantentrennung (softwareseitig).
Physikalisch getrennte Speicherung auf gesonderten Systemen und Datenträgern.
Trennung von Produktiv- und Testsystem

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO):
Eine Pseudonymisierung findet nicht statt.

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

Weitergabekontrolle:

E-Mail-Verschlüsselung
Einrichtung von VPN-Tunneln
Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
Prüfung der Rechtmäßigkeit der Weitergabe von Daten
Mitarbeiterunterweisung
Regelungen bei Ausscheiden von Mitarbeitern
Verpflichtung der Mitarbeiter auf das Datengeheimnis
Sichere Transportbehälter/-verpackungen
Sorgfältige Auswahl von Transportpersonal und Transportfahrzeugen

Eingabekontrolle:

Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitung übernommen worden sind
Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
Plausibilitätskontrollen
Protokollierung der Eingabe, Änderung und Löschung von Daten
Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

Verfügbarkeitskontrolle:

Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
Erstellen eines Backup & RecoverykonzeptsBackup-Strategie (offline, online z.B. Cloud)
Erstellen eines Notfallplans
Feste Prozesse zur Datensicherung
Feuer- und Rauchmeldeanlagen
Feuerlöschgeräte in Serverräumen
Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
Serverräume nicht unter sanitären Anlagen
Testen von Datenwiederherstellung
Unterbrechungsfreie Stromversorgung (USV)
Schutzsteckdosenleisten in Serverräumen

Widerherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO):

Backup Konzept (Offline/Online in der Cloud).
Notfallmanagement inkl. Notfallpläne.
Testen der Wiederherstellungssysteme.

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

Datenschutz Maßnahmen:

Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
Interner / externer Datenschutzbeauftragter
Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
Software-Lösungen für Datenschutz-Management im Einsatz
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ?)

Incident-Response-Management:

Einbindung von DSB und/oder ISB in Sicherheitsvorfälle und Datenpannen
Einsatz von Firewall und regelmäßige Aktualisierung
Einsatz von Virenscanner und regelmäßige Aktualisierung
Einsatz von Spamfilter und regelmäßige Aktualisierung
Regelmäßige Datenschutzschulungen
Datenschutz-Management
Dokumentation von Sicherheitsvorfällen und Datenpannen

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

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

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

Auftragskontrolle:

Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
Auszusondernde Hardware wird sicher zerstört
Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
Prozesse für Betroffenenrechte
Schriftliche Weisungen an den Auftragnehmer (z. B. durch Auftragsverarbeitungsvertrag) i.S.d. Art. 28 DS-GVO
Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
Unterauftragnehmer haben die gleichen Anforderungen wie Auftraggeber zu erfüllen
Verpflichtung der Mitarbeiter des Auftragnehmers auf die Vertraulichkeit
Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbaren