Auftrag gemäß Art. 28 DSGVO zur Auftragsverarbeitung

Vereinbarung

zwischen

– nachfolgend „Auftraggeber“ genannt –

und

BAUER GROUP IT GmbH
Janahof 30
93413 Cham
Deutschland
vertreten durch den Geschäftsführer Herrn Karl Bauer

– nachfolgend Auftragnehmer genannt –

zur Auftragsverarbeitung gemäß Art. 28 DSGVO.

§ 1 Gegenstand und Dauer des Auftrags

Gegenstand und Dauer des Auftrags bestimmen sich vollumfänglich nach den im jeweiligen Vertragsverhältnis gemachten Angaben.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Auftrags.

§ 2 Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von Daten

Der Umfang, die Art und der Zweck einer etwaigen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, die Art der Daten und der Kreis der Betroffenen werden dem Auftragnehmer durch den Auftraggeber gemäß der vom Auftraggeber ausgefüllten Anlage 1 beschrieben, soweit sich das nicht aus dem Vertragsinhalt der in § 1 beschriebenen Vertragsverhältnisse ergibt.

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. DSGVO erfüllt sind.

§ 3 Technisch-organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

(1) 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 (siehe Anlage 2). Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 Satz 2 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen.

(3) 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, Sperrung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig 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.

(2) 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 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Als verantwortliche Person ist beim Auftragnehmer Herr Karl Bauer, +49 9971 20098-100, karl.bauer@bauer-group.com bestellt. Ein Wechsel der verantwortlichen Person ist dem Auftraggeber unverzüglich mitzuteilen. Dessen jeweils aktuelle Kontaktdaten sind unter der Adresse https://go.bauer-group.com/privacypolicy des Auftragnehmers leicht zugänglich hinterlegt.

(2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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 notwendigen technischen und organisatorischen Maßnahmen entsprechen Art. 28 Abs. 3 Satz 2 lit. c, 32 DSGVO und Anlage 2.

(3) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(4) 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.

(5) 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.

(6) 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.

(7) Dokumentation der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber, die gemäß § 3 unter https://go.bauer-group.com/av-tom abrufbar sind.

§ 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 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.

Wenn der Kunde ein Produkt mit einem Standort außerhalb der europäischen Union wählt, erklärt er sich mit Subunternehmern an diesem Standort einverstanden. Eine Liste der eingesetzten Subunternehmer mit Standortangaben ist unter https://go.bauer-group.com/av-subunternehmen abrufbar.

§ 7 Kontrollrechte des Auftraggebers

(1) 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.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO 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.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann wahlweise erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) und/oder eine

geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

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

§ 8 Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO 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;

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

§ 9 Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform oder Schriftform.

(2) 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.

(3) Weisungsberechtigte Personen des Auftraggebers sind berechtigt, weitere weisungsberechtigte Personen zur Ausführung/Organisation/Kontrolle des gemeinsam vereinbarten Leistungsumfanges zu bevollmächtigen.

(4) Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

(5) Die Weisungsberechtigte Personen des Auftraggebers und der Weisungsempfänger des Auftragnehmers, sind in der Anlage 3 zu diesem Auftrag festgelegt.

§ 10 Löschung und Rückgabe von personenbezogenen Daten

(1) 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.

(2) 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. Der Auftragnehmer gibt dem Auftraggeber auf Anfrage hin Auskunft zur Natur und dem Zeitpunkt der Löschung.

(3) 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 Vergütung

(1) Eine gesonderte Vergütung für diesen Auftrag wird nicht gefordert. Die Vergütung richtet sich nach dem diesem Auftrag zu Grunde liegenden Vertragsverhältnis.

(2) Soweit der Auftraggeber Unterstützung nach § 4 für die Beantwortung von Anfragen Betroffener benötigt, hat er die hierdurch entstehenden Kosten zu erstatten.

(3) Soweit der Auftraggeber nach § 7 Kontrollrechte ausüben wird, orientiert sich die vorab zu vereinbarende Höhe des Entgelts an einem festzulegenden Stundensatz des für die Betreuung vom Auftragnehmer abgestellten Mitarbeiters.

(4) Erteilt der Auftraggeber dem Auftragnehmer Weisungen nach § 9, so hat er durch diese Weisung entstehende Kosten zu erstatten.

§ 12 Vertragsdauer

(1) Diese Vereinbarung ist abhängig vom Bestand eines zu Grunde liegenden Hauptvertragsverhältnisses gemäß § 1.

(2) Die Kündigung oder anderweitige Beendigung des Hauptvertragsverhältnisses gemäß § 1 beendet gleichzeitig diese Vereinbarung.

(3) Das Recht zur isolierten, außerordentlichen Kündigung dieser Vereinbarung sowie die Ausübung gesetzlicher Rücktrittsrechte, konkret für die Vereinbarung bleiben hierdurch unberührt.

§ 13 Schlussbestimmungen

(1) Es gilt das Recht der Bundesrepublik Deutschland.

(2) Die Parteien vereinbaren als Gerichtsstand den Sitz des für den Auftragnehmer zuständigen Gerichts.

(3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Cham, 04.03.2020	Cham, 04.03.2020
.....	.....
- Unterschrift Auftraggeber -	- Unterschrift Auftragnehmer -

Anlage 1 zum Auftrag gemäß Art. 28 DSGVO:

Auflistung der personenbezogenen Daten und Zweck ihrer Verarbeitung

Art der Daten:

Gegenstand der Zusatzvereinbarung sind folgende Datenarten und -Kategorien:

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z. B. Telefon, E-Mail)
- ☒ Vertragsstammdaten (z. B. Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☒ Planungs- und Steuerungsdaten
- ☒ Kundenhistorie
- ☒ Korrespondenz
- ☒ Auskunftsangaben (z.B. aus öffentlichen Verzeichnissen)
- ☒ Protokolldaten

Kreis der Betroffenen:

Der Kreis der durch diese Zusatzvereinbarung Betroffenen umfasst:

- ☒ Interessenten
- ☒ Kunden
- ☒ Lieferanten
- ☒ Abonnenten
- ☒ Beschäftigte
- ☒ Ansprechpartner
- ☒ Handelsvertreter
- ☒ Behörden

Anlage 2 zum Auftrag gemäß Art. 28 DSGVO:

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

- Ein abgestuftes Zutrittskontrollsystem (Schlüssel mit individuellen Zutrittsrechten) schützt vor unberechtigtem Zutritt.
- Zutrittsberechtigungen werden zentral erteilt.
- Die Beantragung der Zutrittsrechte ist nur über den entsprechenden Verantwortlichen möglich.
- Zutritt zu Serverräumen ist nur dem notwendigen Personal gestattet und eingerichtet.
- Es ist eine Gästeregelung implementiert. Dies bedeutet das nichtöffentliche Bereiche nur in Begleitung von Mitarbeitern betreten werden können.

Zugangskontrolle

- Der Schutz der IT-Systeme ist durch Authentifikations- und Autorisierungssysteme (Benutzerkennung und Passwort) gewährleistet.
- Zugangsberechtigungen erfolgen nach dem Minimalprinzip (nur die notwendigen Rechte zur Aufgaben- und Leistungserfüllung).
- Die Vergabe und der Entzug (Deaktivierung) von Benutzerkonten durch die IT erfolgt nur nach schriftlicher Beauftragung der Personalabteilung.
- Bei mehrmaliger Fehleingabe der Zugangsdaten wird das Benutzerkonto gesperrt.
- Die Entsperrung erfordert eine persönliche Authentifizierung des Users und ist nur vom IT Support umsetzbar.
- Der Umgang mit Zugängen und Passwörtern ist verbindlich in Richtlinien geregelt und wird in regelmäßigen Mitarbeiter-Schulungen kommuniziert.
- Die Netzwerksegmentierung trennt Netzwerke verschiedener Sicherheitsstufen mittels Firewalls.
- Es werden Firewall-Systeme genutzt, die fortlaufend auf dem aktuellen technischen Stand gehalten werden.
- Es werden speicherresidente Virenscanner, mit mehrmals täglichem Updates, auf allen Client-Systemen verwendet.
- Die Administration und Überwachung der Virenscanner wird zentral gesteuert.

- Alle Freigaben (z.B. Datei- und Druckerfreigaben), Anwendungseinstellungen und weitere sicherheitsrelevante Einstellungen sind über zentral gesteuerte Richtliniensätze für den Benutzer unveränderlich vorgegeben.
- Der Schutz vor unberechtigtem Einsehen der Büro-Arbeitsplätze ist durch die automatisch startende Sperre (Energiesparmodus) mit Passwortschutz gewährleistet.
- Eine regelmäßige Belehrung der Mitarbeiter zur Notwendigkeit des manuellen Sperrens bei Verlassen des Arbeitsplatzes sorgt für die notwendige Sensibilisierung.
- Software-Installationen werden zentral über den IT Support durchgeführt.
- Anwendungen, die Arbeitsplatzfreigaben ermöglichen, sind nur für vertraglich vereinbarte Wartung durch IT-Dienstleister zugelassen und dürfen nur mit Genehmigung oder im Beisein eines IT-Administrators benutzt werden.

Zugriffskontrolle

- Zugriffsberechtigungen werden nach dem Minimalprinzip erteilt. In den IT-Systemen existiert ein granulares Rechtesystem (d.h. Sicherstellung, dass Daten je nach Recht komplett verborgen, nur angezeigt, veränderbar oder löschbar werden).
- Die Steuerung der Neuanlage von Daten erfolgt über separate Rechte.
- Die Erteilung und Änderung von Zugriffsrechten für die Mitarbeiter ist nur über den entsprechenden Verantwortlichen möglich.
- Die Umsetzung von Löschanforderungen ist in den jeweiligen Prozessabläufen sowie den dazu bestehenden Arbeitsanweisungen und Richtlinien geregelt.
- Funknetzen (WLAN) sind sicher nach dem Stand der Technik verschlüsselt.

Datenträgerkontrolle

- Festplatten werden nach Ausmusterung mit einem definierten Verfahren mehrfach überschrieben (gelöscht).
- Defekte Festplatten, die nicht sicher gelöscht werden können, werden sicher zerstört (geschreddert).

Trennungskontrolle

- Durch die konsequente Rechtevergabe in den verarbeitenden Systemen ist sichergestellt, dass die Mitarbeiter ausschließlich nur auf Daten zugreifen können, die sie für Ihre Arbeitsaufgaben benötigen. Damit ist eine Trennung der Kunden- und

Partner-Daten von Daten anderer Auftraggeber oder Eigendaten gewährleistet (Mandantentrennung).

- Die Test- und Entwicklungsumgebungen sind von den Produktivumgebungen getrennt.

Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO, Art. 25 Abs. 1 DSGVO)

- Für die Pseudonymisierung ist der Auftraggeber verantwortlich.
- Im Supportfall ist es dem Verantwortlichen möglich eine Datensicherung verschlüsselt auf einen Server des Auftragnehmers zu übertragen. Die Daten sind grundsätzlich nur für den Bearbeiter beim Auftragnehmer einsehbar, der die Datensicherung verarbeitet.

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

- Standardmäßig werden gesicherte Übertragungswege bzw. eine verschlüsselte Kommunikation bei Datenaustausch (insbesondere bei automatisierten Schnittstellen) verwendet.
- Der E-Mail-Verkehr ist nur für den dienstlichen Verkehr zugelassen (organisatorisch in der entsprechenden Richtlinie geregelt).
- Die Versendung von E-Mails mit vertraulichen Daten erfolgt standardmäßig verschlüsselt (diese Anforderung ist in einer Richtlinie geregelt, die Mitarbeiter werden diesbezüglich durch regelmäßige Schulungen sensibilisiert).
- Die Internetnutzung ist durch geeignete Kontroll- und Filtermaßnahmen geregelt.
- Die Verwendung mobiler Datenträger ist durch die entsprechende Richtlinie organisatorisch geregelt.
- Insbesondere werden zur Weitergabe von Daten nur registrierte und verschlüsselte Speichermedien verwendet.
- In Bereichen wo prozessual bedingt externe mobile Datenträger verwendet werden, ist die Einhaltung des Datenschutzes sowie der Datensicherheit durch entsprechende Arbeitsanweisungen gesondert geregelt.

Eingabekontrolle

- Die Verarbeitung personenbezogener Daten im Sinne des Datenschutzes ist durch die konsequente Rechtevergabe in den verarbeitenden Systemen und durch spezielle Arbeitsanweisungen sichergestellt.
- Es erfolgt ein Logging (Anlagedatum, letztes Änderungsdatum, Bearbeiter) in den verarbeitenden Systemen zur Nachvollziehbarkeit von Änderungen.
- Die Auswertungen der Logging-Daten werden nach Datenschutz- und Kundenrichtlinien zentral erstellt.
- Eine Beantragung der Auswertungen ist nur durch den entsprechenden Verantwortlichen möglich.

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

- Es existiert ein ständig optimiertes IT-Sicherheitskonzept.
- Die redundante Anbindung sichert die erforderliche Verfügbarkeit der Internetverbindung durch Redundanz.
- Es stehen eigens eingerichtete und abgesicherte Netzwerkbereiche (DMZ's) für Partner mit direkter Anbindung über VPN-Verbindung zur Verfügung.
- Die DMZ's schützen von außen zugängliche IT-Systeme.
- Die Administration und Wartung der IT-Systeme wird durch Verfahren und Prozesse sichergestellt.
- Die Ausfallsicherheit wird durch ein geeignetes Notfallkonzept und die Vorhaltung von Redundanzen gewährleistet.
- Kritische Systeme sind untereinander redundant ausgelegt.
- Eine USV-Anlage dient zum Schutz vor Stromausfällen der Server- und Netzwerkräume.
- Eingesetzte Anwendungssoftware und Betriebssysteme werden durch festgelegte Routinen aktuell gehalten (z.B. sicherheitsrelevante Updates und Fixes).
- Änderungen an Kernsystemen erfolgen erst nach erfolgreichen Prüfungen und Tests auf den Testumgebungen.
- Die datenschutzgerechte Entsorgung von elektronischen Datenträgern (insbesondere Festplatten, USB-Sticks, Speicherkarten, optische Datenträger, Bänder) sowie von Papierdokumenten wird durch ein zertifiziertes Unternehmen durchgeführt.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

- Ein abgestuftes Verfahren dient der Absicherung gegen Datenverlust und ist durch sekundäre Datenspeicher sowie Datenkopien auf Festplatte und weitere Medien realisiert.
- Die Backup Datenträger werden in einem gesicherten Bereich gelagert.

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

Auftragskontrolle

- Die Datenverarbeitung erfolgt durch eine eindeutige und schriftliche Vertragsgestaltung sowie einer regelmäßigen Kontrolle der Umsetzung.
- Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers.

Datenschutzmanagement

- Das Datenschutz-Management ist durch Datenschutz-Richtlinien, Arbeitsanweisungen und Prozessbeschreibungen sichergestellt. Diese Dokumente sind für alle Mitarbeiter im Intranet einsehbar.
- Die Verfahren, die der regelmäßigen Überprüfung, Bewertung und Evaluierung dienen, werden geprüft.

Incident-Response-Management

- Weiterführende Maßnahmen, Prozesse und Dokumente (z.B. Notfallpläne, Wiederanlaufpläne, Richtlinien) sind im Management System dokumentiert und unterliegen einer ständigen Qualitätskontrolle.

Datenschutzfreundliche Voreinstellungen

- Personenbezogene Datenverarbeitende Systeme und Anwendungen enthalten von den Benutzern nicht änderbare Privacy-by-Default- sowie Privacy-by-Design-Einstellungen

Hinweis:

Die getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber, sind auch unter https://go.bauer-group.com/av-tom abrufbar.

Anlage 3 zum Auftrag gemäß Art. 28 DSGVO:

Weisungsberechtigte Person(en) des Auftraggebers und Weisungsempfänger beim Auftragnehmer

Weisungsberechtigte Person(en) des Auftraggebers:

Name

Vorname

Dienststellung

Telefonnummer

Telefaxnummer

Mobiltelefonnummer

E-Mail-Adresse

Name

Vorname

Dienststellung

Telefonnummer

Telefaxnummer

Mobiltelefonnummer

E-Mail-Adresse

Weisungsempfänger beim Auftragnehmer:

Name	Bauer
Vorname	Karl
Dienststellung	Geschäftsführer
Telefonnummer	+49 9971 20098-100
Telefaxnummer	+49 9971 20098-4100
Mobiltelefonnummer	+49 178 1444855
E-Mail-Adresse	karl.bauer@bauer-group.com