

# Vertrag zur Auftragsverarbeitung

Version 12.00 / Stand: 11.12.2025

CWA GmbH, 28865 Lilienthal

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Dieser Vertrag zur Auftragsverarbeitung gem. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien. Dieser Vertrag ist eine Ergänzung zu den Allgemeinen Geschäftsbedingungen vom Auftragnehmer, und wird vom Auftraggeber gemeinsam mit den Allgemeinen Geschäftsbedingungen bei der Annahme eines Angebots bzw. bei einer Bestellung für die Wartung von Software und für den Betrieb einer SaaS-Anwendung (Cloud-Version) anerkannt.

## 1. Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Wartung der Software CWA SmartProcess und bei einer SaaS-Lösung Betrieb für die Software CWA SmartProcess.

(2) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der beauftragten Wartung und des beauftragten SaaS-Betriebes für die Software CWA SmartProcess.

## 2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten:

- Bei einer Cloud-Version (SaaS) wird die Software CWA SmartProcess für den Auftraggeber gehostet.
- Fernwartung und Pflege der Software CWA SmartProcess
- Helpdesk und Support – Auf Anfrage Zugriff auf die Software CWA SmartProcess per Remote Software

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich für Auftraggeber aus Europa 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.

(2) Art der Daten

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

- Benutzerdaten für das System wie Benutzername, Anrede, Titel, Vorname, Nachname, Position, Firma, Abteilung, Rolle, Telefon, Mobil-Nr, E-Mail, Firmenadresse, Kostenstelle
- Vorgänge mit benutzerdefinierten Feldern und Daten, die vom Kunden selbst definiert werden.
- Unternehmensdokumente und Unternehmensinformationen, die vom Kunden individuell eingestellt bzw. gespeichert werden.

### (3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Beschäftigte
- Lieferanten

## 3. Technisch-organisatorische Maßnahmen

(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 auf Anfrage zur Prüfung zu übergeben.

(2) 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.

(3) Die technischen und organisatorischen Maßnahmen in der Anlage sind Grundlage des Auftrages.

(4) Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen Weiterentwicklung angepasst werden. Dabei müssen die angepassten Maßnahmen mindestens dem Sicherheitsniveau der in der Anlage vereinbarten Maßnahmen entsprechen. Wesentliche Änderungen sind zu dokumentieren.

## 4. Berichtigung, Einschränkung und Löschung von Daten

(1) 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.

## 5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

- a) Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten. Dessen Kontaktdaten werden dem Auftraggeber auf Anforderung mitgeteilt.
- b) Die Wahrung der Vertraulichkeit gemäß Artt. 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 dokumentierten Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO.
- d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- e) 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.
- f) 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.
- g) 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.

- h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.
- i) Der Auftragnehmer verpflichtet sich, angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Personen nachzukommen."

## 6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. 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.

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

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift	Leistung
Amazon Web Services (AWS)	Server-Standort AWS: Frankfurt am Main  Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxembourg  Amazon Web Services EMEA SARL Niederlassung Deutschland Marcel-Breuer-Str. 12 80807 München	Hosting der Anwendung CWA SmartProcess  Bei einer Cloud-Version (SaaS) wird die Software bei AWS in Frankfurt für Auftraggeber aus Europa gehostet.
Microsoft Ireland Operations Ltd	South County Business Park Leopardstown Dublin 18, D18 P521, Irland	Bereitstellung von KI-Diensten für das KI-Zusatzmodul. Die Daten vom Auftraggeber werden nicht für das Training öffentlicher KI-Modelle genutzt.  Server-Standort für die KI-Dienste: Deutschland

Der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird. Der Auftraggeber wird bei einem Wechsel eines Unterauftragnehmers informiert.

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

(5) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

## **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. Der Auftragnehmer wird die Kontrollen ermöglichen und zu ihnen beitragen. 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 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.

## **8. Mitteilung bei Verstößen des Auftragnehmers**

(1) 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-Folgeabschätzung

- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

## **9. Weisungsbefugnis des Auftraggebers**

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

## **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. Eventuell erstellte Kopien sind zu löschen. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- (3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Hiervon sind Daten mit Personenbezug ausgenommen. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

## **11. Haftung und Recht auf Schadenersatz**

Die Haftung richtet sich nach den Bestimmungen des Art. 82 DS-GVO.

# Anlage zum Vertrag zur Auftragsverarbeitung

## Technische und Organisatorische Maßnahmen (TOMs)

### 1. Zutrittskontrolle

Ziel: Verhindern, dass unbefugte Personen einen Zugang zu Gebäuden und Räumen bekommen.

#### CWA-Maßnahmen:

- Der physische Zugang zu Betriebsräumen ist auch während der Betriebszeiten durch Zutrittskontrollmaßnahmen eingeschränkt. Nur autorisierte Personen erhalten Zugang.
- Alle Besucher werden mit Datum und Uhrzeit ihres Betretens und Verlassens erfasst und durch autorisiertes Personal begleitet.
- Das Gebäude ist mit einer VDS-Alarmanlage und einem Schlüsselsystem gesichert.
- Die Ausgabe und Rücknahme der Zugriffsmittel wird dokumentiert. Die Vollständigkeit und Zuordnung der Zugriffsmittel wird regelmäßig geprüft.

#### AWS-Maßnahmen (Hosting der SaaS-Anwendung SmartProcess):

Die Kundensysteme werden bei AWS mit strengen Zutrittskontrollen und nicht bei CWA gehostet.

- Zugriff nur für autorisiertes Personal
- Mehrstufige Authentifizierung
- Hochsicherheitszäune
- Rund-um-die-Uhr Videoüberwachung und Monitoring-Überwachung
- Einbruchserkennungssysteme
- ISO 27001 zertifiziert und regelmäßige Audits
- Vorbereitete Notfallmaßnahmen

### 2. Zugangskontrolle

Ziel: Verhindern des unbefugten Zugangs zu IT-Systemen und Daten.

- Einsatz von Firewalls zum Schutz vor externen Angriffen.
- Zwei-Faktor-Authentifizierung (2FA) für den Zugang zu kritischen Systemen.
- Verschlüsselte VPN-Verbindungen für externen Zugriff auf das Unternehmensnetzwerk.
- Zugriffsberechtigungen basierend auf dem „Need-to-know“-Prinzip. Bedarfsorientiertes Berechtigungskonzept und der Zugriffsrechte.

- Jeder Zugang wird ausschließlich auf eine individuelle Person bezogen vergeben.
- Regelmäßige Überprüfung und Aktualisierung von Benutzerrechten.
- Die IT-Systeme und Programme sind über Passwörter und verschlüsselten Zugang gesichert.
- Es sind Maßnahmen zum Schutz der Passwort-Authentifizierung implementiert.
- Es werden strenge Passwörter mit ausreichender Komplexität und Länge verwendet. Der Aufbau und die Handhabung der Passwörter sind in der IT-Sicherheitsrichtlinie definiert.
- Mitarbeiterschulungen zur sicheren Nutzung von Passwörtern und Zugangssystemen.

### **3. Zugriffskontrolle**

Ziel: Verhindern des unbefugten Zugriffs auf Daten.

- Die Zugriffskontrolle erfolgt durch ein Berechtigungssystem, das sowohl für Services, Server-Anwendungen als auch für Netzwerklaufwerke implementiert ist.
- Rollenbasierte Zugriffskontrolle (RBAC) für sensible und personenbezogener Daten.
- Protokollierung und Überwachung aller Zugriffe auf sensible und personenbezogene Daten.
- Verschlüsselung gespeicherter sensibler und personenbezogener Daten und Daten bei der Übertragung.
- Die Freigabe von Berechtigungen wird durch den jeweiligen Vorgesetzten genehmigt und vom IT-Support administriert.
- Vergebene Zugriffsrechte werden regelmäßig überprüft.
- Sofortige Entziehung von Zugriffsrechten bei Verlassen des Unternehmens oder Rollenwechsel.
- Mitarbeiterschulungen zum Schutz personenbezogener und sensibler Daten.

### **4. Übertragungskontrolle**

Ziel: Sicherstellen, dass Daten bei der Übertragung nicht abgefangen oder manipuliert werden können.

- Nutzung von verschlüsselten Verbindungen (z. B. HTTPS, SFTP) für den Datentransfer.
- Verschlüsselung vertraulicher E-Mails und Datentransfers.
- Verwendung von Virtual Private Networks (VPN) für alle externen Zugriffe.
- Schulung der Mitarbeiter zur sicheren Übertragung von Informationen.

### **5. Weitergabekontrolle**

Ziel: Sicherstellung der Datenintegrität, dass die Daten während der Übermittlung nicht verändert oder manipuliert werden.

- Die Weitergabe von Daten erfolgt über verschlüsselte Verbindungen. Die Übertragung ist über https.

## 6. Eingabekontrolle

Ziel: Sicherstellen, dass jede Datenveränderung oder -eingabe eindeutig einer Person oder einem System zugeordnet werden kann.

- Protokollierung von Änderungen in zentralen Systemen.
- In SmartProcess werden Änderungen in der Datenbank protokolliert.
- Versionskontrolle für Softwareentwicklungsprojekte.
- Regelmäßige Überprüfung von Protokollen.
- Dokumentation und Kontrolle von Änderungen an sensiblen Daten.

## 7. Verfügbarkeitskontrolle

Ziel: Sicherstellen, dass Daten und Systeme jederzeit verfügbar sind.

- Monitoring der Verfügbarkeit von IT-Systemen.
- Regelmäßige Backups aller kritischen Systeme.
- Regelmäßige Tests der Backup-Systeme.
- Bei einer Cloud-Lösung hat der Provider Amazon Web Services (AWS) eigene Maßnahmen, die eine unterbrechungsfreie Stromversorgung (USV), Brandschutz etc. gewährleisten.
- Bei einer Cloud-Lösung wird die Datensicherung automatisch von den AWS-Services verwaltet. Es gibt ein Backup/Snapshot pro Tag. Die Daten werden mehrfach innerhalb der 3 Availability Zones der AWS-Region Frankfurt repliziert. Für Kunden aus USA werden die Daten in Ohio gespeichert.
- Bei einer Inhouse-Lösung ist der Auftraggeber für das Backup zuständig.
- Erstellter Notfall- und Wiederanlaufplan (Disaster Recovery).

## 8. Trennungskontrolle

Ziel: Sicherstellen, dass Daten zu unterschiedlichen Zwecken getrennt verarbeitet werden.

- Logische Trennung von Daten in verschiedenen Umgebungen (Entwicklung, Test, Produktion).
- Virtuelle Trennung von Kundendaten bei einer Cloud-Lösung.
- Überwachung der Trennung von Daten in verschiedenen Systemen.
- Die Weitergabe von Daten erfolgt über verschlüsselte Verbindungen. Die Übertragung ist über https.

## 9. Verschlüsselung und Pseudonymisierung

Ziel: Erhöhung des Schutzes personenbezogener Daten.

- Verschlüsselung aller gespeicherten personenbezogener Daten.
- Nutzung von Transportverschlüsselung (TLS) bei Datenübertragungen.
- Pseudonymisierung von personenbezogenen Daten in Entwicklungs- und Testumgebungen.

## 10. Datenträgerkontrolle

Ziel: Schutz von Datenträgern vor unbefugtem Zugriff oder Missbrauch.

- Verschlüsselung von mobilen Datenträgern
- Sicherstellung der sicheren Lagerung von sensiblen Datenträgern.
- Sichere Löschung und Entsorgung von Datenträgern.
- Schulung der Mitarbeiter im sicheren Umgang mit mobilen Datenträgern.

## 11. Notfall- und Wiederanlaufmanagement

Ziel: Sicherstellung des Betriebs im Falle eines Ausfalls.

- Regelmäßige Datensicherung aller kritischen Daten.
- Implementiertes Backup-System mit regelmäßigen Tests der Funktionsfähigkeit.
- Erstellter Notfallwiederherstellungsplans (Disaster Recovery Plan).
- Regelmäßige Tests und Übungen zur Überprüfung der Wiederherstellungsprozesse.

## 12. Allgemeine Maßnahmen zur Informationssicherheit

Ziel: Sicherstellung der Informationssicherheit

- Es ist eine Leitlinie zur Informationssicherheit, ein IT-Sicherheitskonzept und eine IT-Sicherheitsrichtlinie im Unternehmen vorhanden und bekannt.
- Die Ausgabe von Hardware wie PCs und Notebooks an Mitarbeiter wird über den Prozess Asset Management gesteuert.
- Es werden Risiken innerhalb eines Risikomanagements identifiziert, bewertet und überprüft. Für die Behandlung von Risiken werden Maßnahmen definiert.
- Es ist ein Prozess für die Behandlung von Datenschutzverstößen und Sicherheitsvorfällen vorhanden.
- Ein Vertrag zur Auftragsdatenverarbeitung gemäß Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) wird als Ergänzung zu den Allgemeinen Geschäftsbedingungen vom Auftragnehmer und vom Auftraggeber bei der Annahme eines Angebots geschlossen.

- Auftragskontrolle: Personenbezogene Daten und sonstige Kundendaten werden nur nach Einzelauftrag bzw. separater schriftlicher Weisung vom Auftraggeber vom Auftragnehmer verarbeitet.
- Die genannten Maßnahmen in diesem Dokument werden mindestens einmal pro Jahr von der Geschäftsführung und vom Informationssicherheitsbeauftragten überprüft.
- Sollten sich bei dieser Überprüfung Änderungen bei technologischen Standards oder organisatorischen Abläufen ergeben, die eine Anpassung der aufgeführten Maßnahmen erfordern, werden die Maßnahmen angepasst.