# Vertrag über die Auftragsverarbeitung bei Cloud Services

zwischen

_____

_____

(nachfolgend „**Kunde**“)

und

**Infotech Gesellschaft für Informations- und Datentechnik mbH**
Holthoffstraße 122a
45669 Recklinghausen
Deutschland

(nachfolgend „**Infotech**“)

## § 1 Auftrag und Festlegungen zur Verarbeitung

1.1. Dieser Vertrag über die Auftragsverarbeitung (nachfolgend „**AVV**“) konkretisiert für alle Verarbeitungen die datenschutzrechtlichen Rechte und Pflichten der Parteien, welche sich aus dem Vertrag der Parteien über die Nutzung von Cloud Services im Service Rechenzentrum Emscher-Lippe-Cloud (nachfolgend „**Hauptvertrag**“) ergeben, unter denen es zu einer Verarbeitung personenbezogener Daten durch Infotech für den Kunden kommt.

1.2. Dieser AVV kommt mit all seinen Bestandteilen zur Anwendung, wenn der Kunde die Infotech zur Verarbeitung personenbezogener Daten (nachfolgend „**Daten**“) im Auftrag gemäß Art. 28 DSGVO verpflichtet hat. Dabei bildet dieser AVV den Rahmen für eine Vielzahl unterschiedlicher Vorgänge der Auftragsverarbeitung.

1.3. Bei etwaigen Widersprüchen gehen die Regelungen dieses AVV mit all seinen Bestandteilen den Regelungen des zugehörigen Hauptvertrages vor.

1.4. Die für die einzelnen Verarbeitungen geltenden spezifischen datenschutzrechtlichen Festlegungen (nachfolgend „**Festlegungen**“) werden vor Beginn der Verarbeitung in Anlagen zum AVV (nachfolgend „**Anlagen**“) geregelt. Dies sind insbesondere Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, die Kategorien von Daten und die Kategorien betroffener Personen sowie die technischen und organisatorischen Maßnahmen (nachfolgend „**TOM**“).

1.5. Die Anlagen sind Teil des AVV. Bei etwaigen Widersprüchen gehen die Anlagen der allgemeineren Regelung im AVV vor. Wird im Folgenden oder in den Anlagen auf den AVV Bezug genommen, so ist der AVV mit all seinen Bestandteilen gemeint.

## § 2 Verantwortlichkeit und Verarbeitung auf Weisung

2.1. Der Kunde ist im Rahmen dieses AVV für die Einhaltung der anwendbaren gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Offenlegung gegenüber Infotech sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich („Verantwortlicher“ gemäß Art. 4 Nr. 7 DSGVO).

2.2. Infotech handelt wegen der Verarbeitung der Daten ausschließlich weisungsgebunden, es sei denn es liegt ein Ausnahmefall gemäß Art. 28 Abs. 3 lit. a) DSGVO vor (anderweitige gesetzliche Verarbeitungspflicht). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Wird der Kunde als Auftragnehmerin einer Auftragsverarbeitung für einen Dritten tätig, gelten die Verpflichtungen des Kunden aus dieser Auftragsverarbeitung für den Dritten unmittelbar als Weisungen des Kunden im Verhältnis zur Infotech, sofern diese Verpflichtungen strenger sein sollten als diejenigen aus diesem AVV. Der Kunde wird Infotech über solche Anforderungen Dritter an die Auftragsverarbeitung schriftlich in Kenntnis setzen.

2.3. Infotech berichtigt oder löscht die vertragsgegenständlichen Daten oder schränkt deren Verarbeitung ein (nachfolgend „Sperrung“), wenn der Kunde dies anweist und dies sonst vom Weisungsrahmen umfasst ist.

2.4. Infotech informiert den Kunden unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen anwendbare Vorschriften über den Datenschutz oder diese AVV verstößt. Infotech darf die Umsetzung der Weisung solange aussetzen, bis diese vom Kunden in Textform bestätigt oder abgeändert wurde. Die Ausführung offensichtlich datenschutzrechtswidriger Weisungen darf Infotech ablehnen.

2.5. Die Parteien benennen gegenseitig in Textform einen oder mehrere Ansprechpartner in datenschutzrechtlichen Angelegenheiten, einschließlich der benannten Datenschutzbeauftragten. Ergeben sich bei den Ansprechpartnern Änderungen, haben sich die Parteien hierüber in Textform zu informieren.

2.6. Infotech gewährleistet, dass die zur Verarbeitung der Daten befugten Personen (a) die

Weisungen des Kunden kennen und diese beachten, sowie (b) sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht auch nach Beendigung der Verarbeitung fort.

2.7. Wird der Kunde als Auftragnehmer einer Auftragsverarbeitung für einen Dritten tätig, gelten die Verpflichtungen von Infotech aus diesem AVV auch unmittelbar im Verhältnis zwischen dem Dritten und Infotech. Dies gilt für alle Leistungen von Infotech, welche diese im Auftrag des Kunden gegenüber dem Dritten erbringt. Insbesondere stehen dem Dritten die Kontroll- und Informationsrechte aus § 8 unmittelbar gegenüber Infotech zu.

## § 3 Sicherheit der Verarbeitung

3.1. Die Parteien vereinbaren TOM gemäß Art. 32 DSGVO zum angemessenen Schutz der Daten (nachfolgend „**Anlage-TOM**“).

3.2. Änderung der Anlage-TOM bleiben Infotech vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau insgesamt nicht unterschritten wird. Wesentliche Änderungen sind dem Kunden auf dessen Verlangen in Textform mitzuteilen.

## § 4 Unterrichtung bei Datenschutzverletzungen und Fehlern der Verarbeitung

4.1. Infotech unterrichtet den Kunden unverzüglich, wenn ihr Verletzungen des Schutzes der ihr von dem Kunden anvertrauten Daten im Sinne des Art. 4 Nr. 12 DSGVO in ihrem Organisationsbereich bekannt werden oder ein konkreter Verdacht einer solchen Datenschutzverletzung bei Infotech besteht.

4.2. Stellt der Kunde Fehler bei der Verarbeitung fest, hat er Infotech unverzüglich hierüber zu unterrichten.

4.3. Infotech trifft unverzüglich die erforderlichen Maßnahmen zur Behebung der Datenschutzverletzung gemäß § 4.1 oder der Fehler gemäß § 4.2 sowie zur Minderung möglicher nachteiliger Folgen, insbesondere für die betroffenen Personen. Hierüber stimmt sie sich mit dem Kunden ab. Mündliche Unterrichtungen § 4.1 oder § 4.2 sind unverzüglich in Textform nachzureichen.

## § 5 Übermittlung von Daten an einen Empfänger in einem Drittland oder in einer internationalen Organisation

Die Übermittlung von Daten an einen Empfänger in einem Drittland außerhalb von EU und EWR ist unter Einhaltung der in Art. 44 ff. DSGVO festgelegten Bedingungen zulässig. Einzelheiten werden bei Bedarf in einer oder mehreren Anlagen geregelt.

## § 6 Unterbeauftragung weiterer Auftragsverarbeiter

6.1. Infotech darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (nachfolgend „**Unterauftragnehmer**“) erbringen lassen.

6.2. Infotech informiert den Kunden in Textform rechtzeitig vorab über die Beauftragung von Unterauftragnehmern oder Änderungen in der Unterbeauftragung. Der Kunde kann bei Vorliegen eines wichtigen Grundes der Unterbeauftragung innerhalb von vier Wochen nach Kenntnisnahme in Textform widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln besteht, dass der Unterauftragnehmer die vereinbarte Leistung entsprechend den anwendbaren gesetzlichen Bestimmungen zum Datenschutz oder gemäß dieser AVV erbringt. Im Fall eines begründeten Widerspruchs des Kunden räumt dieser Infotech eine angemessene Frist ein, um den vom Widerspruch betroffenen Unterauftragnehmer durch einen anderen Unterauftragnehmer zu ersetzen. Ist Infotech dies nicht möglich oder dem Kunden nicht zumutbar, ist die jeweilige Partei zur außerordentlichen Kündigung des Hauptvertrags aus wichtigem Grund berechtigt.

6.3. Infotech wird mit dem Unterauftragnehmer die in diesem AVV getroffenen Regelungen inhaltsgleich vereinbaren. Insbesondere müssen die mit dem Unterauftragnehmer zu vereinbarenden TOM ein gleichwertiges Schutzniveau aufweisen.

6.4. Keine Unterbeauftragungen im Sinne dieser Regelung sind Leistungen, die Infotech als reine Nebenleistung zur Unterstützung ihrer geschäftlichen Tätigkeit außerhalb der Auftragsverarbeitung in Anspruch nimmt. Infotech ist jedoch verpflichtet, zur Gewährleistung des Schutzes der Daten auch für solche Nebenleistungen angemessene Vorkehrungen zu ergreifen.

## § 7 Rechte betroffener Personen und Unterstützung des Kunden

Macht eine betroffene Personen Ansprüche gemäß Kapitel III der DSGVO bei einer der Parteien geltend, so informiert sie die jeweils andere Partei darüber unverzüglich. Infotech unterstützt den Kunden im Rahmen ihrer Möglichkeiten bei der Bearbeitung solcher Anträge sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

## § 8 Kontroll- und Informationsrechte des Kunden

8.1. Infotech weist den Kunden die Einhaltung ihrer Pflichten mit geeigneten Mitteln nach. Der Kunde überprüft die Geeignetheit.

8.2. Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit kann Infotech auf angemessene Zertifizierungen oder andere geeignete Prüfungsnachweise verweisen. Angemessen sind insbesondere Zertifizierungen nach Art. 42 DSGVO oder Nachweise nach Art. 40 DSGVO. Daneben kommen unter anderem in Betracht: eine Zertifizierung nach ISO 27001 oder ISO 27017, eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz, eine Zertifizierung nach anerkannten und geeigneten Branchenstandards oder ein Prüfungsnachweis gemäß SOC / PS 951. Die Zertifizierungs- und Prüfungsverfahren sind von einem anerkannten unabhängigen Dritten durchzuführen. Infotech hat etwaige Zertifikate oder Prüfungsnachweise zur Verfügung zu stellen. Weitere geeignete Mittel (z.B. Tätigkeitsberichte des Datenschutzbeauftragten oder Auszüge aus Berichten der Wirtschaftsprüfer) können zum Nachweis der Einhaltung der vereinbarten Schutzmaßnahmen dem Kunden zur Verfügung gestellt werden. Das Inspektionsrecht des Kunden aus § 8.3 bleibt hiervon unberührt.

8.3. Der Kunde ist berechtigt, zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, regelmäßig nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit, Inspektionen bei Infotech zur Prüfung der Einhaltung der datenschutzrechtlichen Bestimmungen durchzuführen. Infotech darf die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der von ihr getroffenen TOM abhängig machen. Infotech ist verpflichtet, Überprüfungen und Inspektionen des Kunden zu ermöglichen und dazu beizutragen.

8.4. Zur Behebung der bei einer Inspektion getroffenen Feststellungen stimmen die Parteien die umzusetzenden Maßnahmen ab.

8.5. Macht eine Aufsichtsbehörde von Befugnissen nach Art. 58 DSGVO Gebrauch, so informieren sich die Parteien hierüber unverzüglich. Sie unterstützen sich in ihrem jeweiligen Verantwortungsbereich bei Erfüllung der gegenüber der jeweiligen Aufsichtsbehörde bestehenden Verpflichtungen.

## § 9 Haftung und Schadenersatz

9.1. Macht eine betroffene Person gegenüber einer Partei Schadenersatzansprüche wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen geltend, so hat die beanspruchte Partei die andere Partei hierüber unverzüglich zu informieren.

9.2. Der Kunde und Infotech haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

9.3. Die Parteien unterstützen sich wechselseitig bei der Abwehr von Schadenersatzansprüchen betroffener Personen, es sei denn, dies würde die Rechtsposition der einen Partei im Verhältnis zur anderen Partei, zur Aufsichtsbehörde oder gegenüber Dritten gefährden.

## § 10 Kosten

Die durch Maßnahmen des Kunden bei Infotech anfallenden Kosten sind vom Kunden zu tragen, soweit diese nicht mit der Vergütung nach dem Hauptvertrag abgegolten sind. Dies gilt insbesondere für durch Kontrollen und Inspektionen des Kunden nach § 8 der Infotech anfallende Kosten.

## § 11 Laufzeit

11.1. Der AVV wird auf unbestimmte Zeit geschlossen. Die Laufzeit einer Anlage wird in der jeweiligen Anlage geregelt; ohne eine solche Regelung läuft die Anlage auf unbestimmte Zeit.

11.2. Der AVV kann mit einer Frist von drei Monaten zum Quartalsende gekündigt werden, wenn gleichzeitig oder zuvor alle Anlagen beendet wurden.

11.3. Eine Anlage endet mit Beendigung des zugehörigen Hauptvertrags, ohne dass es einer gesonderten Kündigung dieser Anlage bedarf. Infotech hat in diesem Fall nach Wahl des Kunden unverzüglich die nach der Anlage verarbeiteten Daten herauszugeben oder datenschutzkonform zu löschen und dies dem Kunden in Textform zu bestätigen. Sofern Infotech eine eigene gesetzliche Pflicht zur Speicherung dieser Daten hat, hat sie dies dem Kunden in Textform anzuzeigen.

## § 12 Fortgeltung und Überleitung von Altverträgen

Der AVV ersetzt mit Wirkung ab seiner Unterzeichnung die bestehenden Verträge nach § 11 BDSG. Haben die Parteien vor Abschluss dieses AVV Festlegungen nach § 1 vereinbart, so gelten diese sinngemäß unter dem AVV fort, es sei denn sie werden durch Anlagen ersetzt, denen derselbe Verarbeitungsgegenstand zu Grunde liegt.

### § 13 Schlussbestimmungen

13.1. Sollten die Daten des Kunden bei Infotech durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat Infotech den Kunden unverzüglich darüber in Textform zu informieren. Infotech wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Verantwortung für die Daten ausschließlich beim Kunden liegt.

13.2. Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen des AVV bedürfen zu ihrer Wirksamkeit der Textform und der ausdrücklichen Bezugnahme auf die AVV. Abweichende mündliche Abreden der Parteien sind unwirksam. Dies gilt auch für Änderungen dieser Klausel.

13.3. Sollte nur eine Bestimmung dieses AVV ganz oder teilweise rechtsunwirksam oder nichtig sein oder werden, bleibt dieser AVV im Übrigen unberührt. An Stelle der rechtsunwirksamen oder nichtigen Bestimmung gilt das Gesetz, sofern die hierdurch entstandene Lücke nicht durch ergänzende Vertragsauslegung gemäß §§ 133, 157 BGB geschlossen werden kann. Beide Parteien sind jedoch verpflichtet, unverzüglich Verhandlungen aufzunehmen mit dem Ziel einer Vereinbarung an Stelle der rechtsunwirksamen oder nichtigen Bestimmung, die deren Sinn und Zweck in rechtlicher und wirtschaftlicher Hinsicht am Nächsten kommt, insbesondere dem Charakter der Vereinbarung als Dauerschuldverhältnis zur Regelung datenschutzrechtlicher Belange gerecht wird.

13.4. Es gilt deutsches Recht unter Ausschluss des Kollisionsrechts; Art. 3 Abs. 3, Abs. 4 ROM-I-VO bleiben unberührt.

| | |
|---|---|
| _____ | _____ |
| Ort, Datum | Ort, Datum |
| _____ | _____ |
| Unterschrift Infotech | Unterschrift Kunde |
| _____ | _____ |
| Name, Funktion Unterzeichner (in Druckbuchstaben) | Name, Funktion Unterzeichner (in Druckbuchstaben) |

# Anlage 1: Festlegungen zur Auftragsverarbeitung

Die Parteien treffen zum Vertrag über die Auftragsverarbeitung ergänzend folgende Festlegungen:

### § 1 Gegenstand und Dauer der Verarbeitung

Gegenstand der Verarbeitung ist die Bereitstellung der im Vertrag der Parteien über die Nutzung von Cloud Services im Service Rechenzentrum Emscher-Lippe-Cloud (nachfolgend „**Hauptvertrag**“) bezeichneten Cloud Services einschließlich der zugehörigen Wartungs-, Pflege- und Supportleistungen durch Infotech für den Kunden. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags.

### § 2 Zweck der Verarbeitung

Die Verarbeitung erfolgt fortlaufend über die Laufzeit des Hauptvertrags.

Ausschließlich zur Erfüllung der Pflichten von Infotech aus dem Hauptvertrag im Zusammenhang mit der Bereitstellung der Cloud Services werden personenbezogene Daten aus dem Herrschaftsbereich des Kunden durch Infotech vollumfänglich i.S.d. Art. 4 Nr. 2 DSGVO verarbeitet, insbesondere erhoben, gespeichert, verändert, ausgelesen, abgefragt, verwendet, offengelegt, abgeglichen, verknüpft und gelöscht.

### § 3 Kategorien personenbezogener Daten

Die von der Verarbeitung betroffenen Kategorien von Daten hängen von der Nutzung der Cloud Services durch den Auftraggeber ab. Als Gegenstand der Verarbeitung in Betracht kommende Kategorien von Daten sind: Bestandsdaten (z.B. Anschriften, Benutzerkennungen), Inhaltsdaten (z.B. aus Dokumenten) und Nutzungsdaten (bei der Auswertung von Zugriffen und der Erstellung von Reports), einschließlich ggf. besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO und anderer Daten mit einem hohen oder sehr hohen Schutzbedarf.

### § 4 Kategorien betroffener Personen

Die von der Verarbeitung betroffenen Kategorien betroffener Personen hängen von der Nutzung der Cloud Services durch den Kunden ab. In Betracht kommen Beschäftigte, Kunden, Interessenten, Lieferanten und andere Vertragspartner, unbeteiligte Dritte und Gesellschafter sowie Organe des Kunden.

**§ 5 Offenlegung von Daten an Empfänger in Drittländern oder internationalen Organisationen**

Eine Offenlegung von Daten an Empfänger in Drittländern oder an internationale Organisationen erfolgt nicht.

# Anlage 2: Technische und organisatorische Maßnahmen zur Sicherheit der Verarbeitung

### 1) Zutrittskontrolle

Die Verarbeitung findet an folgenden Standorten statt:

a) Rechenzentren in Recklinghausen
b) Backup Rechenzentrum in Recklinghausen
c) Verwaltungsgebäude in Recklinghausen.

Die Zutrittskontrolle ist wie folgt geregelt:

Zu a): Zwei-Faktor-Authentisierung (Smart-Key, PIN), Vereinzelung, Videoüberwachung, Einbruchmeldeanlage.

Zu b): Zwei-Faktor-Authentisierung (Smart-Key, PIN), Videoüberwachung, Einbruchmeldeanlage.

Zu c): Empfang am Gebäudeeingang. Bewegung im Hause nur in Begleitung eines Mitarbeiters. Videoüberwachung, Einbruchmeldeanlage.

### 2) Zugangskontrolle

- Passwortschutz der Rechner (Client-Betriebssystem, Server-Betriebssystem, Datenbank, Anwendung): Mindestlänge 8 Zeichen, Zeichenmix, Wechselforcierung)
- Bildschirmsperre bei Pausen mit Passwortaktivierung
- Zugriffssperren durch zentrale Firewalls
- Einsatz von VPNs bei Remote-Zugriffen
- Einsatz von Anti-Viren-Software.

### 3) Zugriffskontrolle

Für die Aufgabenwahrnehmung bestehen folgende Zugriffsberechtigungen:

a) Kundenbetreuung
Die Mitarbeiter haben schreibenden und lesenden Zugriff auf die Verwaltungsdaten und somit ggf. Zugriff auf personalisierte Mailaccounts, wenn der Kunde solche benutzt. Der Zugriff erfolgt ausschließlich über eine Anwendung (Lavreso) mit einem persönlichen Account. Datenänderungen werden feldbezogen mit altem Wert/neuem Wert und Account protokolliert.

b) Entwicklung
Die Mitarbeiter erhalten im Einzelfall zum Zwecke des Supports (i.d.R. Fehleranalyse) Zugriff auf alle Daten. Der Zugriff erfolgt auf Datenbankebene. Die Zugriffe werden nicht protokolliert.

Die Zugriffe werden im Einzelfall durch den Leiter des Supports überwacht.

c) Business Service
Die Mitarbeiter fahren die produktiven Maschinen. Sie haben normalerweise keinen Zugriff auf personenbezogene Daten. Sie können im Einzelfall Zugriff auf die IT-Verwaltungsdaten erhalten, wenn Wartungsarbeiten dies erfordern. Der Zugriff wird in diesen Fällen vom Abteilungsleiter überwacht. Einzelne Zugriffe werden nicht protokolliert.

### 4) Weitergabekontrolle

Zur Datenübermittlung zwischen Kunde und Cloud werden VPNs eingesetzt.

Eine sonstige Übermittlung personenbezogener Daten ist nicht vorgesehen.

### 5) Eingabekontrolle

Hinsichtlich der Verwaltungsdaten werden Eingaben und Änderungen benutzerbezogen protokolliert.

### 6) Auftragskontrolle

Infotech stellt sicher, dass Weisungen des Kunden unverzüglich umgesetzt und etwaige Unterauftragnehmer ausschließlich unter Beachtung der Vorgaben aus der Vereinbarung zur Auftragsdatenverarbeitung tätig werden.

### 7) Trennungsgebot

Infotech stellt technisch sicher, dass die Daten des Kunden von den Daten anderer Kunden mindestens logisch getrennt sind.

**Textende**
**Stand: 22. Mai 2018**