

Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen

im Folgenden Auftraggeber genannt

und

active logistics AG, Gahlenfeldstraße 53, 58313 Herdecke

und den Tochterunternehmen

active logistics Herdecke GmbH, Gahlenfeldstr. 53, 58313 Herdecke

active logistics Koblenz GmbH, Bahnhofplatz 9, 56068 Koblenz

active logistics Nürnberg AG, Lina-Ammon-Straße 22, 90471 Nürnberg

im Folgenden Auftragsverarbeiter genannt

nachfolgend gemeinsam die "Vertragsparteien" und einzeln jeweils die "Vertragspartei".

Inhaltsverzeichnis

| | | |
|------|--|----|
| 0 | Präambel | 3 |
| 1 | Definitionen | 3 |
| 2 | Gegenstand und Dauer des Auftrags | 4 |
| 3 | Konkretisierung des Auftragsinhalts | 4 |
| 4 | Technische und organisatorische Maßnahmen | 5 |
| 5 | Berichtigung, Einschränkung und Löschung von Daten | 5 |
| 6 | Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters | 5 |
| 7 | Unterauftragsverhältnisse | 7 |
| 8 | Kontrollrechte und sonstige Pflichten des Auftraggebers | 7 |
| 9 | Mitteilung bei Verstößen des Auftragsverarbeiters | 8 |
| 10 | Weisungsbefugnis des Auftraggebers | 9 |
| 11 | Geheimhaltungspflichten | 9 |
| 12 | Löschung und Rückgabe von personenbezogenen Daten | 9 |
| 13 | Schlussbestimmungen | 10 |
| I. | Beschreibung der betroffenen Daten und Personen | 11 |
| II. | Verzeichnis der Unterauftragnehmer | 12 |
| III. | Verzeichnis der zuständigen Personenkreise | 13 |
| IV. | Kontaktdaten Datenschutzbeauftragte(r) beim Auftraggeber | 15 |
| V. | Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO des Auftragsverarbeiters | 16 |

0 Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Hauptvertrag in ihren Einzelheiten beschriebenen Auftrags(daten)verarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragsverarbeiters oder durch den Auftragsverarbeiter beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrags.

Diese Vereinbarung berücksichtigt die mit Inkrafttreten der EU-Datenschutzgrundverordnung (EU-DSGVO) sowie das Bundesdatenschutzgesetz in der vom Deutschen Bundestag am 27. April 2017 und dem Deutschen Bundesrat am 12. Mai 2017 beschlossenen Fassung („BDSG-neu“) geltende Rechtslage

1 Definitionen

Gemäß Datenschutzgrundverordnung (DSGVO)

- (1) Personenbezogene Daten (siehe Art 4 lit. 1 DSGVO „Begriffsbestimmungen“)

„Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen;

- (2) Auftragsverarbeiter (siehe Art. 28 DSGVO „Auftragsverarbeiter“)

„Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet)

- (3) Weisung (siehe Art. 28 lit 3 a DSGVO „Auftragsverarbeiter“)

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation.

2 Gegenstand und Dauer des Auftrags

2.1 Gegenstand des Auftrags

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Auftraggebers gemäß gesonderter Vereinbarung.

2.2 Dauer des Auftrags

Die Dauer des Auftrags (Laufzeit) ergibt sich aus der gesonderten Vereinbarung.

3 Konkretisierung des Auftragsinhalts

3.1 Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten

- (1) Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung.

- (2) 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 §§ 4b, 4c BDSG bzw. Art. 44 ff. DSGVO erfüllt sind.

3.2 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind in **[Anlage 1]** „1. Art der Daten“ beschrieben.

3.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen sind in **[Anlage 1]** „2. Kategorien betroffener Personen“ beschrieben.

4 Technische und organisatorische Maßnahmen

- (1) Der Auftragsverarbeiter stellt die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung und dem Auftraggeber zur Prüfung dar. 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. Etwaige Kosten trägt der Auftraggeber.
- (2) Der Auftragsverarbeiter wird die Sicherheitsvorgaben gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere i.V.m. Art. 5 Abs. 1, Abs. 2 DSGVO berücksichtigen. 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 **[Einzelheiten in Anlage 5]**.
- (3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht über Gebühr unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragsverarbeiter informiert den Auftraggeber über gravierende Änderungen.

5 Berichtigung, Einschränkung und Löschung von Daten

- (1) Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder sperren bzw. oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen an den Auftraggeber weiterleiten.
- (2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers durch den Auftragsverarbeiter sicherzustellen.

6 Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzlich Pflichten gem. Art. 28 bis 33 DSGVO; insofern sorgt er insbesondere für die Einhaltung folgender Vorgaben:

- Schriftliche Bestellung, sofern gesetzlich vorgeschrieben, eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO i.V.m. § 38 BDSG (neu) ausüben kann. Die Kontaktdaten des Datenschutzbeauftragten des Auftragsverarbeiters sind:

Stefan Kleiner mann +49 (0) 2401 60 540 info@das-datenschutz-team.de

Für das Rechenzentrum Niederaula:

DPP Data Protection GmbH +49 (0) 69175366960 rf@dataprotectionpartner.de

- Die Kontaktdaten der/des Datenschutzbeauftragte(n) ist beim Auftraggeber ist in **[Anlage 4]** „Kontaktdaten Datenschutzbeauftragte(r) beim Auftraggeber“ beschrieben.

Ein Wechsel des Datenschutzbeauftragten ist der jeweils anderen Partei unverzüglich mitzuteilen.

- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragsverarbeiter 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 Auftragsverarbeiter und jede dem Auftragsverarbeiter 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 in Anlage 5]**.
- Der Auftraggeber und der Auftragsverarbeiter 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 Auftragsverarbeiter 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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.
- Der Auftragsverarbeiter kontrolliert 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 9 dieses Vertrages.

7 Unterauftragsverhältnisse

(1) 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 Auftragsverarbeiter 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 Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu ergreifen.

(2) Der Auftragsverarbeiter darf Unterauftragnehmer (weitere Auftragsverarbeiter) jederzeit beauftragen, soweit

- der Auftragsverarbeiter eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.
- Die vom Auftragsverarbeiter beauftragten Unterauftragnehmer sind in **[Anlage 2]** „Verzeichnis der Unterauftragnehmer“ beschrieben.

8 Kontrollrechte und sonstige Pflichten des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen während der üblichen Betriebszeiten durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch

Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu den jeweils üblichen Geschäftszeiten zu überzeugen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragsverarbeiters durch die Kontrollen nicht unverhältnismäßig zu stören.

- (2) Der Auftragsverarbeiter stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
- (3) Den Nachweis solcher Maßnahmen, die den konkreten Auftrag betreffen, kann der Auftragsverarbeiter erbringen 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);
 - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).
- (4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragsverarbeiter einen Vergütungsanspruch geltend machen.

9 Mitteilung bei Verstößen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Einhaltung der in den Art. 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 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 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

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

10 Weisungsbefugnis des Auftraggebers

- (1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
- (2) Der Auftragsverarbeiter hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.
- (3) Beide Parteien definieren bei Beginn der Auftragsdatenverarbeitung schriftlich die weisungsberechtigten Personen des Auftraggebers und die Weisungsempfänger beim Auftragsverarbeiter **[Anlage 3]** „Verzeichnis der zuständigen Personenkreise“. Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner schriftlich ein Nachfolger bzw. eine Vertretung mitzuteilen.

11 Geheimhaltungspflichten

- (1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.
- (2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

12 Löschung und Rückgabe von personenbezogenen Daten

- (1) Kopien oder Duplikate der Daten außerhalb der Beauftragung werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien und Backups, 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 Auftragsverarbeiter 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.
- (3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

13 Schlussbestimmungen

- (1) Sollte das Eigentum des Auftraggebers beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber zu informieren. Der Auftragsverarbeiter wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, informieren.
- (2) Für Nebenabreden ist die Schriftform erforderlich.
- (3) Es gilt deutsches Recht.
- (4) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

ORT, den

Herdecke, den

.....

Auftraggeber

.....

Auftragsverarbeiter

Anlage 1

I. Beschreibung der betroffenen Daten und Personen

1. Art der Daten

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

| |
|--|
| Kundenstammdaten <i>(z.B. Vor- und Nachname, Adresse, Geschäftspartnernummer, Vertragskontonummer, Kundenhistorie)</i> |
| Lieferantenstammdaten <i>(z.B. Vor- und Nachname, Adresse, Funktion der Ansprechpartner)</i> |
| Geschäfts-/Ansprechpartnerdaten <i>(z.B. Vor- und Nachname, Adresse, Funktion der Ansprechpartner)</i> |
| Kommunikationsdaten <i>(z.B. E-Mail, Telefon- und Faxnummer)</i> |
| Kundenabrechnungs- und -zahlungsdaten <i>(z.B. Verbrauchsdaten, Bankverbindungsdaten, Zahlungsverhalten/Mahnhistorie, Bonitätsauskünfte)</i> |
| Lieferantenabrechnungs- und -zahlungsdaten <i>(z.B. Bankverbindungsdaten, Zahlungsverhalten/Mahnhistorie, Bonitätsauskünfte)</i> |
| Protokollierungsdaten <i>(z.B. Benutzer-ID, ggfs. IP-Adresse, Anmelde- und Änderungshistorie und Protokollierungsdaten)</i> |

2. Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

| |
|---|
| Beschäftigte |
| Interessenten |
| Kunden |
| Lieferanten |
| Beschäftigte von Kunden oder Lieferanten (Ansprechpartner) |
| Geschäftspartner |

Anlage 2

II. Verzeichnis der Unterauftragnehmer

| Unterauftragnehmer | Geschäftssitz | Erbrachte Dienstleistung |
|---|---|---------------------------------|
| Vision-Flow Software GmbH | Riedgasse 11, A – 6850 Dornbirn | Programmierung |
| IMC Zlin a.s. | Kvitkovà 119, CZ 76001 Zlin | Programmierung |
| Prologia Unternehmensberatung GmbH | Dietigheimer Str. 18, 61350 Bad Homburg | Programmierung |
| Ondot Software Solution | Brown-Boveri-Straße 8/1, AT- 2351 Wiener Neudorf | |
| Sapper Institut für interaktive Lernsysteme GmbH & Co.KG | Möhlenring 48, 47906 Kempen | Compliance |
| Diamant Software GmbH & Co.KG | Stadtring 2, 33647 Bielefeld | Software |
| PTV | Stumpfstr. 1, 76131 Karlsruhe | |
| Oxseed logistics GmbH | Gahlenfeldstr. 53, 58313 Herdecke | Archiv |
| Halstenbach GmbH | Breidenbrucher Str. 2, 51674 Wiehl-Bomig | |
| Rüdiger Kerkeloh | Gartenstr. 44, 59387 Ascheberg | |
| BAB DATA-Systeme Vertriebs GmbH | Berghauser Str. 104, 42349 Wuppertal | Software |
| Easy Software AG | Am Hauptbahnhof 4, 45468 Mülheim | Software |
| TIS Technische Informationssysteme GmbH | Müller-Armack-Str. 8, 46397 Bocholt | |
| Four J's Development Tools Software Vertriebs GmbH | Laufzorner Weg 4, 82064 Strasslach | |
| Richard Müller GmbH | Westfalendamm 263, 44141 Dortmund | |
| T & A Systeme GmbH | Am Walzwerk 1, 45527 Hattingen | |

Anlage 3

III. Verzeichnis der zuständigen Personenkreise

Als **weisungsbefugte** Stellen gegenüber dem Auftragsverarbeiter benennt der Auftraggeber insbesondere folgende Ansprechpartner:

Herr/Frau:
Tel.:
Mobil:
E-Mail:

sowie

Herr/Frau:
Tel.:
Mobil:
E-Mail:

Als **weisungsempfangende** Stellen benennt der Auftragsverarbeiter gegenüber dem Auftraggeber insbesondere folgende Ansprechpartner:

Für den Standort Koblenz:

Herr/Frau: Herr Peter Fuchs
Tel.: 0261-8099420
E-Mail: peter.fuchs@active-logistics.com

sowie

Herr/Frau: Frau Kathleen Franke
Tel.: 0261-8099137
E-Mail: kathleen.franke@active-logistics.com

Für den Standort Herdecke:

Herr/Frau: Herr Tim Steiner
Tel.: 02330-9191111
E-Mail: tim.steiner@active-logistics.com

sowie

Herr/Frau: Herr Michael Lorei
Tel.: 02330-9191179
E-Mail: michael.lorei@active-logistics.com

Für den Standort Niederaula:

Herr/Frau: Herr Bernd Leibold
Tel.: 06625-105373
E-Mail: bernd.leibold@active-logistics.com

sowie

Herr/Frau: Frau Nicole Schütze
Tel.: 06625-105327
E-Mail: nicole.schuetze@active-logistics.com

Für den Standort Nürnberg:

Herr/Frau:
Tel.:
Mobil:
E-Mail:

sowie

Herr/Frau:
Tel.:
Mobil:
E-Mail:

Anlage 4

IV. Kontaktdaten Datenschutzbeauftragte(r) beim Auftraggeber

Als Datenschutzbeauftragte(r) ist beim Auftraggeber bestellt ist

Herr/Frau:

Tel.:

Mobil:

E-Mail:

Anlage 5

V. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO des Auftragsverarbeiters

1. Vertraulichkeit (Art. 32 Absatz 1, b. DS-GVO)

| | |
|--|--|
| Zutrittskontrolle <i>(Kein unbefugter Zutritt zu Datenverarbeitungsanlagen und Informationsablageorten (z.B. Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen, Büros))</i> | Zutrittskontrollsystem, Ausweisleser, Chipkarte |
| | Dokumentierte Schlüsselvergabe |
| | Türsicherung (elektrische Tür) |
| | Empfang / Pforte |
| | Überwachungseinrichtung, z.B. Alarmanlage, Video-/Fernsehmonitor |
| | Schließanlage |
| Zugangskontrolle <i>(Keine unbefugte Systembenutzung, z.B. (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern)</i> | Kennwortverfahren (u.a. Sonderzeichen, 8 Zeichen Mindestlänge, regelmäßiger Wechsel) |
| | Automatische Sperrung von Endgeräten bei Inaktivität / Bildschirmsperre |
| | Einrichtung <u>eines</u> Benutzerstammsatzes pro User |
| | Verschlüsselung von mobilen Datenträgern |
| | Domänenlogin |
| Zugriffskontrolle <i>(Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen)</i> | Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte) |
| | Regelmäßige Auswertung und Kontrolle bestehender Berechtigungen |
| | Zeitnahe Aktualisierung bzw. Löschung der Berechtigungen |
| | Verschlüsselung von besonders schutzbedürftigen Daten |
| | Zugriff auf Kundensysteme via VPN oder ISDN-Einwahl über RDP, SSH, TeamViewer, PCVisit oder Telnet |
| | Router-Authentifizierung mittels verschlüsselter Kennung und Passwort |

| | |
|--|---|
| | Kontrolle der Fernwartung |
| Trennungskontrolle <i>(Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken. Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing)</i> | Interne Mandantenfähigkeit / Zweckbindung |
| | Funktionstrennung (Produktion / Test / Entwicklung), soweit möglich |
| | Pseudonymisierung (Art. 32 Absatz 1, a. DS-GVO, Art. 25 Absatz 1 DS-GVO) in Test- und/oder Entwicklungssystemen |

2. Integrität (Art. 32 Absatz 1, b DS-GVO)

| | |
|---|--|
| Weitergabekontrolle <i>(Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur)</i> | Verschlüsselung/Tunnelverbindung (VPN) oder ISDN-Direkteinwahl |
| | Elektronische Signatur |
| | Protokollierung |
| | Transportsicherung |
| Eingabekontrolle <i>(Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement)</i> | Protokollierungs- und Protokollauswertungssysteme |
| | Datenbank-Zugriffsprotokollierung durch aH.4 |

3. Verfügbarkeit und Belastbarkeit (Art. 32 Absatz 1, b DS-GVO)

| | |
|--|---|
| Verfügbarkeitskontrolle <i>(Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne)</i> | Backup-Verfahren (Verantwortung des Auftraggebers) |
| | Spiegeln von Festplatten, z.B. RAID-Verfahren |
| | Unterbrechungsfreie Stromversorgung (USV) |
| | Getrennte Aufbewahrung von Backupmedien |
| | Virenschutz/Firewall |
| | Notfallplan |
| | Rasche Wiederherstellbarkeit (Art. 32 Absatz 1, c DS-GVO) |

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Absatz 1 d DG-GVO, Art. 25 Absatz 1 DS-GVO)

| | |
|--|---|
| Datenschutzmanagement | Datenschutz durch Technikgestaltung (privacy by design, Art. 25 Absatz 1 DS-GVO) |
| | Datenschutzfreundliche Voreinstellungen (privacy by default, Art. 25 Absatz 2 DS-GVO) |
| Incident-Management | Incident-Management (1st level, 2nd level) |
| Auftragskontrolle <i>(Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B. eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen)</i> | Nur weisungsberechtigte Personen des Auftraggebers können Weisungen erteilen. |
| | Ausschließlich schriftlich erteilte Weisungen |
| | Formalisierte Auftragserteilung (Auftragsformular) |
| | Eindeutige Vertragsgestaltung |
| | Kriterien zur Auswahl des Auftragnehmers, sofern Unterauftragnehmer im Einsatz |
| | Kontrolle der Vertragsausführung, sofern Unterauftragnehmer im Einsatz |