Allgemeine Nutzungsbedingungen Datenschutz (AND) gemäß Art. 28 DSGVO

KDV Kanne Datenverarbeitung GmbH

Sylbeckestraße 20

32756 Detmold

(nachfolgend KDV genannt)

Kontakt
05231 3045-0
info@kdv-dt.de
www.kdv-dt.de

Anschrift
Sylbeckestr. 20
32756 Detmold

Geschäftsführer
Frank Greweling
Pierre Blidh

Steuer-Nr.
5313/5823/1169
Amtsgericht Lemgo
HRB 3405

Bankverbindung
Deutsche Bank
IBAN: DE 34 4767 0023 0418 0089 00
BIC: DEUTDE3B476

Inhalt

Kontakt
05231 3045-0
info@kdv-dt.de
www.kdv-dt.de

Anschrift
Sylbeckestr. 20
32756 Detmold

Geschäftsführer
Frank Greweling
Pierre Blidh

Steuer-Nr.
5313/5823/1169
Amtsgericht Lemgo
HRB 3405

Bankverbindung
Deutsche Bank
IBAN: DE 34 4767 0023 0418 0089 00
BIC: DEUTDE3B476

1 Gegenstand der AND

Gegenstand dieser AND ist die schriftliche Vereinbarung von Datenschutzangelegenheiten bei der KDV. Sie findet Anwendung auf alle Tätigkeiten, die mit dem individuellen Lizenz-/Dienstleistungsvertrag in Zusammenhang stehen und bei denen Beschäftigte der KDV oder durch die KDV Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

2 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1. Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung ergeben sich aus dem Lizenz-/Dienstleistungsvertrag. Die Laufzeit dieser AND richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser AND nicht darüberhinausgehende Verpflichtungen ergeben.
2. Welcher Kreis von Personen durch die Verarbeitung ihrer personenbezogenen Daten betroffen ist, ergibt sich aus dem Lizenz-/Dienstleistungsvertrag bzw. aus der Vorgabe des Auftraggebers (i. d. R. Mitarbeiterdaten des Auftraggebers).
3. Im Rahmen der Datenverarbeitung können Entgeltdaten und / oder Zeitdaten verarbeitet werden, damit inbegriffen besondere Arten personenbezogener Daten, wie Staatsangehörigkeit, Religion, Gewerkschaftsmitgliedschaft, etc.
4. Art und Zweck der Datenverarbeitung ist die Erstellung von Entgeltabrechnungen und / oder die Verarbeitung von Zeitdaten, Reisekostenabrechnungen sowie Auswertungen.
5. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich im Gebiet der Bundesrepublik Deutschland oder in einem Mitgliedsstaat der Europäischen Union statt. Jegliche Verlagerung in ein Drittland bedarf der Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

3 Anwendungsbereich und Verantwortlichkeit

Die KDV verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Lizenz-/Dienstleistungsvertrag konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an die KDV sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

4 Verpflichtung auf die Vertraulichkeit

1. Die KDV bestätigt, dass ihr die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Sie verpflichtet sich, sicherzustellen, dass bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Grundsätze der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben und der Transparenz eingehalten werden.
2. Die KDV sichert zu, dass sie bei der Verarbeitung die Vertraulichkeit streng wahren wird sowie die bei der auftragsgemäßen Datenverarbeitung beschäftigten Mitarbeiter schriftlich auf Vertraulichkeit verpflichtet und sie mit den für sie maßgeblichen datenschutzrechtlichen Vorschriften vertraut gemacht hat.
   Die KDV überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.
3. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Vertrages fort.

Kontakt
05231 3045-0
info@kdv-dt.de
www.kdv-dt.de

Anschrift
Sylbeckestr. 20
32756 Detmold

Geschäftsführer
Frank Greweling
Pierre Blidh

Steuer-Nr.
5313/5823/1169
Amtsgericht Lemgo
HRB 3405

Bankverbindung
Deutsche Bank
IBAN: DE 34 4767 0023 0418 0089 00
BIC: DEUTDE3B476

4. Die KDV verpflichtet sich und ihre Mitarbeiter, über nicht allgemein bekannte, geschäftlich relevante und bedeutsame Angelegenheiten des Auftraggebers (Geschäftsgeheimnisse) Verschwiegenheit zu wahren.
5. Der Auftraggeber verpflichtet sich, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datengeheimnissen der KDV vertraulich zu behandeln.

5 Pflichten des Auftraggebers

1. Der Auftraggeber hat die KDV unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
2. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der KDV vertraulich zu behandeln.
3. Der Auftraggeber nennt der KDV den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen sowie die weisungsberechtigten Personen zur Durchführung der Auftragsverarbeitung. Diese Ansprechpartner sind in der *„Anlage der AND Vereinbarung zu Datenschutz und Datensicherheit“* definiert.

6 Pflichten der KDV

1. Die KDV verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Die KDV informiert den Auftraggeber unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze im Bereich Datenschutz verstößt; dies schließt jedoch jegliche Rechts- oder Steuerberatung aus. Die KDV darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
2. Die Weisungsberechtigten werden anfänglich in der *„Anlage der AND Vereinbarung zu Datenschutz und Datensicherheit“* festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die von KDV bezeichnete Stelle (Anhang 3: Weisungsempfänger bei der KDV) durch einzelne Weisungsberechtigte geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen zu Leistungen, die im Lizenz-/Dienstleistungsvertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.
3. Die KDV wird in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.
    a. Die KDV hat technische und organisatorische Maßnahmen (TOMs) zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.
    b. Die KDV führt ein Verzeichnis zu allen Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO, die sie im Auftrag eines Verantwortlichen durchführt.
    c. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Eine Änderung, Weiterentwicklung oder Anpassung der getroffenen Sicherheitsmaßnahmen an den technischen Fortschritt bleibt der KDV vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert und die Dokumentation dem Auftraggeber unaufgefordert zur Verfügung gestellt.

Kontakt 05231 3045-0 info@kdv-dt.de www.kdv-dt.de
Anschrift Sylbeckestr. 20 32756 Detmold
Geschäftsführer Frank Greweling Pierre Blidh
Steuer-Nr. 5313/5823/1169 Amtsgericht Lemgo HRB 3405
Bankverbindung Deutsche Bank IBAN: DE 34 4767 0023 0418 0089 00 BIC: DEUTDE3B476

4. Sollten die bei KDV getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht mehr genügen, benachrichtigt der Auftraggeber die KDV unverzüglich. Entsprechendes gilt für Störungen, Verstöße der KDV oder der bei ihr beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Vertrag getroffenen Festlegungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.
5. Die KDV verwendet die vom Auftraggeber überlassenen Daten zu keinem anderen Zweck, als im Lizenz-/Dienstleistungsvertrag oder dieser AND festgelegt. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.
6. Die KDV unterstützt, soweit vereinbart, den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.
   Für Unterstützungsleistungen, die nicht im Lizenz-/Dienstleistungsvertrag enthalten oder nicht auf ein Fehlverhalten der KDV zurückzuführen sind, kann die KDV eine Vergütung verlangen.
7. Die KDV gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für die KDV tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten.
8. Die KDV unterrichtet den Auftraggeber unverzüglich, wenn ihr Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Die KDV trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

7 Datenschutzbeauftrage(r) der KDV

Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen ist

Herr Dipl. Inform. Olaf Tenti

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH
als externer Datenschutzbeauftragter
Fleyer Str. 61
58097 Hagen
Tel: +49 (0) 2331 / 35 68 32-0
Fax: +49 (0) 2331 / 35 68 32-1
E-Mail: datenschutz@gdi-mbh.eu
Internet: http://gdi-mbh.eu/

Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

8 Anfragen betroffener Personen

1. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an die KDV, wird die KDV die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Die KDV leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Die KDV unterstützt den Auftraggeber im Rahmen ihrer Möglichkeiten auf Weisung soweit vereinbart. Die KDV haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.
2. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich die KDV den

Kontakt 05231 3045-0 info@kdv-dt.de www.kdv-dt.de
Anschrift Sylbeckestr. 20 32756 Detmold
Geschäftsführer Frank Greweling Pierre Blidh
Steuer-Nr. 5313/5823/1169 Amtsgericht Lemgo HRB 3405
Bankverbindung Deutsche Bank IBAN: DE 34 4767 0023 0418 0089 00 BIC: DEUTDE3B476

Auftraggeber bei der Abwehr des Anspruches im Rahmen ihrer Möglichkeiten zu unterstützen. Für Unterstützungsleistungen, die nicht im Lizenz-/Dienstleistungsvertrag enthalten oder nicht auf ein Fehlverhalten der KDV zurückzuführen sind, kann die KDV eine Vergütung verlangen.

3. Im Falle einer Inanspruchnahme der KDV durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO gilt Nr. 2 entsprechend.

9 Nachweismöglichkeiten der Verpflichtungen

1. Die KDV weist dem Auftraggeber auf Verlangen, jedoch mindestens alle drei Jahre, die Einhaltung der in dieser AND niedergelegten Pflichten, insbesondere der technischen und organisatorischen Maßnahmen nach der Anlage dieses Vertrages, mit geeigneten Mitteln nach. Der Nachweis über die Umsetzung der technischen und organisatorischen Maßnahmen kann erfolgen durch:
    a) Zertifikat zum Datenschutz
    b) Eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz).
2. Die KDV erklärt sich damit einverstanden, dass der Auftraggeber oder ein von diesem beauftragter Prüfer jederzeit nach Absprache und mindestens 21-tägiger Voranmeldung berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme sowie Betreten und Besichtigung der Räumlichkeiten der KDV, welche die Leistungserbringung für den Auftraggeber betreffen. Die KDV verpflichtet sich insoweit, dem Auftraggeber oder einem von diesem beauftragten Dritten zu diesem Zwecke Zugang zu den Firmenräumen zu gewähren.
3. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu KDV stehen, hat die KDV gegen diesen ein Einspruchsrecht.
4. Für Unterstützungsleistungen bei der Durchführung einer Inspektion, die nicht im Lizenz-/Dienstleistungsvertrag enthalten sind, kann die KDV eine Vergütung verlangen.
5. Der Aufwand einer Inspektion ist für die KDV grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.
6. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Nr. 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

10 Subunternehmer (weitere Auftragsverarbeiter)

1. Mit Unterzeichnung des Vertrages stimmt der Auftraggeber zu, dass die KDV Subunternehmer hinzuzieht (allgemeine schriftliche Genehmigung gem. Art. 28 Abs. 2 DSGVO).
2. Die von der KDV hinzugezogenen Subunternehmer laut Anhang 2 zu dieser AND gelten mit Vertragsunterzeichnung des Lizenz-/Dienstleistungsvertrages als genehmigt.
3. Änderungen (Hinzuziehung oder Ersetzung) der Subunternehmer werden durch Veröffentlichung mitgeteilt. Der Auftraggeber kann innerhalb von 14 Tagen nach Veröffentlichung der Änderung aus wichtigem Grund widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben. Die Auftragserteilung an den Subunternehmer erfolgt erst nach Ablauf der Frist.

Kontakt 05231 3045-0 info@kdv-dt.de www.kdv-dt.de
Anschrift Sylbeckestr. 20 32756 Detmold
Geschäftsführer Frank Greweling Pierre Blidh
Steuer-Nr. 5313/5823/1169 Amtsgericht Lemgo HRB 3405
Bankverbindung Deutsche Bank IBAN: DE 34 4767 0023 0418 0089 00 BIC: DEUTDE3B476

4. Erteilt die KDV Aufträge an Subunternehmer, so obliegt es der KDV ihre datenschutzrechtlichen Pflichten aus dem Lizenz-/Dienstleistungsvertrag und dieser AND dem Subunternehmer zu übertragen.
   Die KDV überzeugt sich von der Einhaltung der vertraglich zugesicherten Sicherheitsmaßnahmen nachweislich und gewissenhaft.
5. Nicht als Untervertragsverhältnisse im Sinne dieser AND sind solche Dienstleistungen zu verstehen, die die KDV bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt (z. B. Telekommunikationsdienstleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern). Die KDV ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
6. Der Sitz der hinzugezogenen Subunternehmer befindet sich in einem oder mehreren Mitgliedsstaaten der EU.

11 Informationspflichten, Schriftformklausel, Zurückbehaltungsrecht, Rechtswahl

1. Sollten die Daten des Auftraggebers bei der KDV durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat die KDV den Auftraggeber unverzüglich darüber zu informieren. Die KDV wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.
2. Für Nebenabreden ist die Schriftform erforderlich.
3. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
4. Bei etwaigen Widersprüchen zum Thema Datenschutz gehen Regelungen der AND den Regelungen des Lizenz-/Dienstleistungsvertrages vor.
5. Sollten einzelne Teile dieser AND unwirksam sein, so berührt dies die Wirksamkeit der AND im Übrigen nicht.
6. Es gilt deutsches Recht.

12 Berichtigung, Löschung, Sperrung und Rückgabe der personenbezogenen Daten

1. Die KDV berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen gem. des Lizenz-/Dienstleistungsvertrages umfasst ist, und führt über die Löschung oder Berichtigung ein Protokoll.
2. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich,
   a. übernimmt die KDV die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder
   b. gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Lizenz-/Dienstleistungsvertrag bereits vereinbart.

Kontakt 05231 3045-0 info@kdv-dt.de www.kdv-dt.de
Anschrift Sylbeckestr. 20 32756 Detmold
Geschäftsführer Frank Greweling Pierre Blidh
Steuer-Nr. 5313/5823/1169 Amtsgericht Lemgo HRB 3405
Bankverbindung Deutsche Bank IBAN: DE 34 4767 0023 0418 0089 00 BIC: DEUTDE3B476

3. Sollten der KDV durch die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien Kosten entstehen, die die KDV nicht zu verantworten hat, kann die KDV eine Vergütung verlangen.
4. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Lizenz-/Dienstleistungsvertrag bereits vereinbart.
5. Nach Vertragsende sind auf Verlangen des Auftraggebers sämtliche aktiven Daten, Datenträger sowie sämtliche sonstige Materialien inklusive erstellter Verarbeitungs- und Nutzungsergebnisse entweder herauszugeben oder physisch zu löschen. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber. Die Löschung bzw. Vernichtung ist zu dokumentieren.
6. Die Daten des Auftraggebers werden 3 Monate nach Kündigung des Lizenz- / Dienstleistungsvertrages – also nach Kündigung der Auftragsdatenverarbeitung – aus dem aktiven Datenpool der KDV gelöscht.

13 Vergütung

Die Vergütung wird durch den individuellen Lizenz-/Dienstleistungsvertrag festgelegt.

14 Haftung und Schadensersatz

Eine zwischen den Parteien im Lizenz-/Dienstleistungsvertrag zur Leistungserbringung vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart.

15 Erläuterungen zu technischen und organisatorischen Maßnahmen (TOM)

Auch nach Einführung der DSGVO müssen personenbezogene Daten bei der Datenverarbeitung durch technische und organisatorische Maßnahmen geschützt werden. Die Datenschutzkontrollen des alten BDSG und die Gebote des Datenschutzes nach der Anlage zu § 9 BDSG-alt sind durch die DSGVO ersetzt worden.

Gemäß Art. 32 DSGVO haben der Verantwortliche (Auftraggeber) und der Auftragsverarbeiter (KDV) jedoch weiterhin „geeignete technische und organisatorische Maßnahmen“ zu treffen, „um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“.

Kontakt
05231 3045-0
info@kdv-dt.de
www.kdv-dt.de

Anschrift
Sylbeckestr. 20
32756 Detmold

Geschäftsführer
Frank Greweling
Pierre Blidh

Steuer-Nr.
5313/5823/1169
Amtsgericht Lemgo
HRB 3405

Bankverbindung
Deutsche Bank
IBAN: DE 34 4767 0023 0418 0089 00
BIC: DEUTDE3B476

Anhang 1: Beschreibung der technischen und organisatorischen Maßnahmen – Datensicherungsmaßnahmen

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

17 Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

Das Gebäude verfügt über einen Haupteingang und mehrere Fluchttüren mit separaten Schließkreisen. Lediglich der Haupteingang dient dem Zutritt in das Gebäude.

In dem Gebäude sind mehrere Unternehmen eingemietet. Der Schließkreis zum Zutritt in das Gebäude ist den Mietern gemeinsam. Die Zutritte in die Räumlichkeiten der einzelnen Unternehmen sind durch die Treppenhäuser und die damit verbundenen separaten Schließkreise voneinander differenziert.

Zusätzlich ist das gesamte Gebäude durch eine Brandmeldeanlage mit einer direkten Verbindung zur Feuerwehr gesichert.

Firmenfremde Personen werden im Unternehmen stets begleitet.
Besuchern ist es durch die verschlossenen Bereiche des Unternehmens und durch die verschlossenen Etagen nicht möglich, sich allein Zutritt in die Räume zu verschaffen. Durch schriftlich fixierte Anweisungen wird sichergestellt, dass Handwerker und kooperierende Dienstleistungsunternehmen in regelmäßigen Abständen kontrolliert werden.

Innerhalb des Gebäudes sind verschiedene Zutrittsbereiche definiert.
Für die Definition der Zutrittsbereiche sowie die Vergabe inklusive Dokumentation der Zutrittsberechtigungen ist die Geschäftsführung zuständig.
Die Vergabe der einzelnen Zutrittsberechtigungen orientiert sich an der Mitarbeiterfunktion. Es wird auf eine minimale Vergabe geachtet.

Bei Verlust eines Schüssels wird das entsprechende Schließsystem ausgetauscht. Bei Verlust eines Chips wird dieser in der Anlage gesperrt, so dass der verlorene Chip über keinerlei Zutrittsbefugnisse verfügt.

In dem Unternehmen gibt es mehrere räumlich getrennte Serverräume mit getrennten Strom- und Internetversorgungen. Die Serversysteme sind redundant ausgelegt.
Die Serverräume sind gesondert gegen unbefugten Zutritt gesichert.

18 Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

Die verschiedenen Bereiche des Unternehmens sind im Zugang beschränkt. Über verschiedene Schließsysteme werden verschiedene Berechtigungsgruppen realisiert. Die Bereiche und Räumlichkeiten sind stets verschlossen.

Kontakt 05231 3045-0 info@kdv-dt.de www.kdv-dt.de
Anschrift Sylbeckestr. 20 32756 Detmold
Geschäftsführer Frank Greweling Pierre Blidh
Steuer-Nr. 5313/5823/1169 Amtsgericht Lemgo HRB 3405
Bankverbindung Deutsche Bank IBAN: DE 34 4767 0023 0418 0089 00 BIC: DEUTDE3B476

Die Rechner des Unternehmens sind durch Benutzerprofile mit User-ID und Passwort vor unberechtigtem Zugriff geschützt. Durch das zentrale Active Directory werden starke Passwörter mit einer Mindestlänge sichergestellt. Durch das Active Directory wird ebenfalls kontrolliert, dass bereits verwendete Passwörter nicht erneut eingesetzt werden können. Alle Passwörter werden regelmäßig gewechselt. Alle Benutzerkonten des Unternehmens werden nach dreimaliger, falscher Eingabe der Benutzeridentifizierung automatisch gesperrt. Eine Entsperrung eines Benutzerkontos kann nur manuell von dem IT-Hauptadministrator vorgenommen werden.

19 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

Es liegt ein anwenderbezogenes Berechtigungskonzept vor, dass im Active Directory umgesetzt wird. Die realisierte Berechtigungsstruktur bezieht sich auf das gesamte System des Unternehmens und wird nach Verantwortungsbereichen oder Kundenkreisen eingeschränkt. Es wird sichergestellt, dass jeder Benutzer nur auf die Daten zugreifen kann, zu denen er zugriffsberechtigt ist.

Zum Schutz gegen unberechtigten Zugriff im Arbeitsalltag ist bei allen Benutzerkonten durch das Active Directory der Bildschirmschoner aktiviert. Jedes Konto wird nach sechs Minuten der Inaktivität durch eine erneut erforderliche Eingabe des Passwortes gesichert.

20 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Je Kunde wird grundsätzlich eine getrennte Datenbank vorgehalten. Weiter werden logische Trennungen in den Datenbanken realisiert.

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

Maßnahmen, die gewährleisten, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können. Die zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen entsprechenden technischen und organisatorischen Maßnahmen.

Eine Pseudonymisierung kann aufgrund des Auftragsinhaltes nicht vorgenommen werden.

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

22.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und

Kontakt 05231 3045-0 info@kdv-dt.de www.kdv-dt.de
Anschrift Sylbeckestr. 20 32756 Detmold
Geschäftsführer Frank Greweling Pierre Blidh
Steuer-Nr. 5313/5823/1169 Amtsgericht Lemgo HRB 3405
Bankverbindung Deutsche Bank IBAN: DE 34 4767 0023 0418 0089 00 BIC: DEUTDE3B476

festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

Personenbezogene Daten des Unternehmens werden zur Erfüllung der Dienstleistungen und zum Nachkommen der gesetzlichen Vorschriften an folgende externe Stellen übermittelt:

1. Im Falle der Entgeltabrechnung: Finanzamt, Sozialversicherung, sowie die jeweils betroffenen Kunden.
2. Im Falle der Zeitwirtschaft: Externe Entgeltabrechnungssysteme oder Anbieter des Kunden.

Zur Übertragung der Daten wird der Postweg, Fax, E-Mail oder die Softwareschnittstelle genutzt.

22.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind:

Zur Gewährleistung der Eingabekontrolle sind die vom Softwarehersteller mitgebrachten Log-Mechanismen und Transaktionsprotokolle zur Protokollierung aller Eingaben für alle Anwendungen aktiviert.

Veränderungen an den Kundendaten werden protokolliert.

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

Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

Für die Datenhaltung der Kundendaten bei der KDV gilt:
Die Daten auf dem Server werden zentral gesichert. Die Datensicherung ist konzeptionell durch die ISO 9001:2015 schriftlich definiert.
Auch das Testen einer Wiedereinspielung einer Datensicherung ist durch das Konzept gewährleistet und automatisiert sichergestellt. Die Backup-Datenträger sind zugriffsbeschränkt und gesondert gesichert.

Das Unternehmen setzt eine unterbrechungsfreie Stromversorgung (USV) für die Serverschränke ein, in der Blitz- und Überspannungseinrichtungen integriert sind. Die unterbrechungsfreie Stromversorgung wird automatisch einmal jährlich hinsichtlich ihrer Wirksamkeit getestet. Bei einem Stromausfall werden alle wichtigen Geräte (Server etc.) automatisch heruntergefahren.

Es wird ein regelmäßig automatisiert aktualisierter Virenscanner und eine regelmäßig kritisch überprüfte Firewall eingesetzt. Der Betrieb der Firewall wird ständig überwacht, so dass gewährleistet wird, dass die Firewall ständig zur Verfügung steht. Sicherheitsrelevante Ereignisse werden automatisch protokolliert.
Zur permanenten Sicherstellung der zur Verfügung stehenden EDV ist diese in allen Bereichen redundant ausgelegt.

Kontakt 05231 3045-0 info@kdv-dt.de www.kdv-dt.de
Anschrift Sylbeckestr. 20 32756 Detmold
Geschäftsführer Frank Greweling Pierre Blidh
Steuer-Nr. 5313/5823/1169 Amtsgericht Lemgo HRB 3405
Bankverbindung Deutsche Bank IBAN: DE 34 4767 0023 0418 0089 00 BIC: DEUTDE3B476

In den Serverräumen sind redundant geschaltete Klimaanlagen installiert. Für die Wartung und die Reinigung der Klimaanlagen ist eine spezialisierte Wartungsfirma über Wartungsverträge verantwortlich.

Die Sicherungsmaßnahmen zur Verfügbarkeit in allen anderen Fällen obliegen allein dem Kunden.

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

24.1 Datenschutz-Management

Die Datenschutz-Grundverordnung bringt für Unternehmen umfassende Nachweispflichten mit sich.

Sinn dieses Verfahrens ist es, einen kontinuierlichen Verbesserungsprozess zu etablieren. Im Rahmen dieses Verfahrens werden die technischen und organisatorischen Maßnahmen erst erdacht und geplant („plan“), im „Kleinen Kreis“ getestet („do“), die Wirksamkeit überprüft („check“), gegebenenfalls angepasst und dann im „Großen“ eingeführt („act“).

Dies schließt regelmäßige Schulungen der Mitarbeiter ein.

Der PDCA zum Datenschutz-Management wird durch die ISO 9001:2015 sowie die internen Wiki-Dokumente gewährleistet.

24.2 Incident-Response-Management

Es muss eine Ablaufstrategie vorliegen, was zu tun ist, wenn eine Sicherheitsverletzung entdeckt wird (Was ist passiert? Wie ist es passiert? Welchen Umfang hat die Verletzung? Welche Auswirkungen hat die Verletzung? Welche Schritte müssen unternommen werden?).

Datenschutzprozesse werden durch Arbeitsanweisungen und Prozessvorgaben definiert.

24.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Datenschutz durch datenschutzfreundliche Voreinstellungen ist der Grundsatz, wonach eine Organisation (der Verantwortliche) sicherstellt, dass durch Voreinstellung nur Daten, die für den jeweiligen bestimmten Verarbeitungszweck unbedingt erforderlich sind, verarbeitet werden (ohne Eingreifen des Nutzers).

Die Voreinstellungen unserer Software werden hinsichtlich datenschutzrelevanter Kriterien durch den eigenen Datenschutzbeauftragten überprüft.

24.4 Auftragskontrolle

Ohne entsprechende Weisung des Auftraggebers darf die KDV keine Auftragsdatenverarbeitung i. S. d. Art. 28 DSGVO vornehmen (Beispiele: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen).

Die Schutzmaßnahmen externer Dienstleister werden durch den Datenschutzbeauftragten regelmäßig überprüft.

Kontakt 05231 3045-0 info@kdv-dt.de www.kdv-dt.de
Anschrift Sylbeckestr. 20 32756 Detmold
Geschäftsführer Frank Greweling Pierre Blidh
Steuer-Nr. 5313/5823/1169 Amtsgericht Lemgo HRB 3405
Bankverbindung Deutsche Bank IBAN: DE 34 4767 0023 0418 0089 00 BIC: DEUTDE3B476

Anhang 2: Subunternehmer des Auftraggebers

Name/Firma	Adresse	Art der Verarbeitung	Kontaktdaten
Roman Kassebaum	Theodor-Heuss-Straße 8 32257 Bünde	Software-Entwicklung	05223 574304 roman@kassebaum.eu
Uwe Raabe	Kutscherweg 23 32312 Lübbecke	Software-Entwicklung	05741 310304 support@raabe-software.de
Nixdorf GmbH	Brakeler Straße 17 33014 Bad Driburg	ZDE Vertrieb und Support	05253 98850 info@nixdorf.de
Weder	Gildestraße 12 32760 Detmold	Gebäude-Reinigung	05231 308280 info@weder-gmbh.de
Thomas Reinhardt	Schützenstraße 13 32805 Horn-Bad Meinberg	Hausmeister	0171 8687707 Reinhardt-Heizung@t-online.de
Rhenus Data Office GmbH	Industriestraße 5 48301 Nottuln	Aktenvernichtung	02509 890 info.data-office@de.rhenus.com

Stand der Auflistung: 27.04.2018

Kontakt
05231 3045-0
info@kdv-dt.de
www.kdv-dt.de

Anschrift
Sylbeckestr. 20
32756 Detmold

Geschäftsführer
Frank Greweling
Pierre Blidh

Steuer-Nr.
5313/5823/1169
Amtsgericht Lemgo
HRB 3405

Bankverbindung
Deutsche Bank
IBAN: DE 34 4767 0023 0418 0089 00
BIC: DEUTDE3B476

Anhang 3: Weisungsempfänger bei der KDV

Name	Kontaktdaten	Position	Weisungsbereich
Dirk Sauerland	05231 3045-100	Projektleitung	Lohn, ZDE
Kristian Jost	05231 3045-100	Projektleitung	Lohn, ZDE
Kai Kramm	05231 3045-100	Projektleitung	Lohn, ZDE
Sven Heiderich	05231 3045-440	Projektleitung / Entwicklung	Lohn, ZDE
Sabine Mellies	05231 3045-440	Projektleitung	Lohn, ZDE
Romana Kielmann	05231 3045-440	Projektleitung	Lohn, ZDE
Wenke Helle	05231 3045-100	Abteilungsleitung	Lohn
Susanne Therolf	05231 3045-100	Abteilungsleitung	Lohn
Frank Huppert	05231 3045-470	Abteilungsleitung	ERP
Frank Geisler	05231 3045-470	Abteilungsleitung	ERP

Kontakt
05231 3045-0
info@kdv-dt.de
www.kdv-dt.de

Anschrift
Sylbeckestr. 20
32756 Detmold

Geschäftsführer
Frank Greweling
Pierre Blidh

Steuer-Nr.
5313/5823/1169
Amtsgericht Lemgo
HRB 3405

Bankverbindung
Deutsche Bank
IBAN: DE 34 4767 0023 0418 0089 00
BIC: DEUTDE3B476