Allgemeine Geschäftsbedingungen
Datenschutz zur Auftragsverarbeitung gemäß Art. 28 DS-GVO
der ckn Computer GmbH & Co. KG

nachstehend Auftragnehmer genannt

Gegenstand der AGB

Gegenstand dieser AGB ist die schriftliche Vereinbarung von Datenschutzangelegenheiten beim Auftragnehmer. Sie findet Anwendung auf alle Tätigkeiten, die mit dem individuellen Kundenvertrag (»Dienstleistungsvertrag«) in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten (»Auftragsverarbeitung«).
Die detaillierten Verarbeitungsvereinbarungen werden durch den individuellen Kundenvertrag (Dienstleistungsvertrag) definiert.

Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1. In der Auftragsverarbeitung liegt der EDV-Betrieb inklusive der gesamten digitalen Datenverarbeitung, wobei der individuelle Vertrags-Gegenstand und die Dauer des Auftrags sich aus dem Hauptvertrag ergeben. Die Laufzeit dieser AGB richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser AGB nicht darüberhinausgehende Verpflichtungen ergeben.
2. Art und Zweck der Verarbeitung ergeben sich aus dem Umfang der individuellen Verarbeitungen des Kunden. Diese umfassen den Systembetrieb und die digitale Datenverarbeitung.
3. Der Betroffenenkreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags – wobei der Betroffenenkreis durch die Datenverarbeitungsprozesse des Auftraggebers bestimmt wird – umfasst:
i. Mitarbeiter des Auftraggebers
ii. Kunden des Auftraggebers
iii. Mandantendaten des Auftraggebers
iv. Mitarbeiterdaten des Kunden des Auftraggebers
4. Die Art der im Rahmen der Datenverarbeitung verarbeiteten Daten werden vom Auftraggeber selbst bestimmt. Beispiele für verarbeitete Daten sind:
i. Kundendaten des Auftraggebers
ii. Kundenadressen des Auftraggebers
5. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jegliche Verlagerung in ein Drittland bedarf der Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

Anwendungsbereich und Verantwortlichkeit

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im 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 den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

Verpflichtung auf die Vertraulichkeit

1. Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er 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. Er verpflichtet sich ferner, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen.
2. Der Auftragnehmer sichert zu, dass er bei der Verarbeitung die Vertraulichkeit streng wahren wird und die bei der auftragsgemäßen Datenverarbeitung beschäftigten Mitarbeiter schriftlich auf Vertraulichkeit verpflichtet und sie mit den

für sie maßgeblichen datenschutzrechtlichen Vorschriften vertraut gemacht hat. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.
3. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
4. Der Auftragnehmer verpflichtet sich und seine 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 des Auftragnehmers vertraulich zu behandeln.

Pflichten des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Datenverarbeitung / -erhebung / -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.
2. Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und vertraglich festzuhalten
3. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
4. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.
5. Der Auftraggeber benennt dem Auftragnehmer
a) den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen,
b) die weisungsberechtigten Personen, sowie
c) den Umfang, in dem diese Personen nach b) weisungsberechtigt sind.

Pflichten des Auftragnehmers

1. Der Auftragnehmer 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) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
2. Die Weisungen werden anfänglich durch eine Anlage zum Dienstleistungsvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle (Anhang 3) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Hauptvertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.
3. Der Auftragnehmer hat personenbezogene Daten zu berichtigen, löschen und zu sperren, wenn der Auftraggeber dies in der getroffenen Vereinbarung oder einer Weisung verlangt.
4. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.
5. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.
a. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.
b. Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO, die er 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 dem Auftragnehmer 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.
6. Sollten die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht mehr genügen, benachrichtigt er den Auftraggeber unverzüglich. Entsprechendes gilt für Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.
7. Der Auftragnehmer verwendet die vom Auftraggeber überlassenen Daten zu keinem anderen Zweck, als im Dienstvertrag oder dieser AGB festgelegt. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

8. Die Datenträger, die von Auftraggeber zur Verfügung gestellt bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden -automatisierten- Verwaltung. Eingang und Ausgang werden dokumentiert.
9. Der Auftragnehmer unterstützt, soweit vereinbart, den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. Für Unterstützungsleistungen, die nicht im Dienstleistungsvertrag enthalten oder auf ein Fehlverhalten des Auftraggeber zurückzuführen sind, kann der Auftragnehmer eine Vergütung verlangen.
10. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
11. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer 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.

Datenschutzbeauftrage(r) des Auftragnehmers

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.

Anfragen betroffener Personen

1. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer 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 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Für Unterstützungsleistungen, die nicht im Dienstleistungsvertrag enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung verlangen.
3. Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO gilt Nr. 2 entsprechend.

Nachweismöglichkeiten der Verpflichtungen

1. Der Auftragnehmer weist dem Auftraggeber auf Verlangen die Einhaltung der in diesem Vertrag niedergelegten Pflichten, insbesondere der technischen und organisatorischen Mittel nach § 3 Abs. 2 dieses Vertrages, mit geeigneten Mitteln nach. Der Nachweis über die die Umsetzung der technischen und organisatorischen Maßnahmen kann erfolgen durch
a) Zertifikat zum Datenschutz (ausgestellt durch den Datenschutzbeauftragten)
b) Aktuelle Berichte des Datenschutzbeauftragten
2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung und unter Berücksichtigung einer angemessenen Vorlaufzeit von mindestens 3 Wochen durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer

Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen.
Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Für Unterstützungsleistungen bei der Durchführung einer Inspektion, die nicht im Dienstleistungsvertrag enthalten sind, kann der Auftragnehmer eine Vergütung verlangen.
Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.
3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 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.

Subunternehmer (weitere Auftragsverarbeiter)

1. Mit Unterzeichnung dieses Vertrages stimmt der Auftraggeber zu, dass der Auftragnehmer Subunternehmer hinzuzieht (allgemeine schriftliche Genehmigung gem. Art. 28 Abs. 2 DS-GVO).
2. Die von dem Auftragnehmer hinzugezogenen Subunternehmer laut Anhang 2 (mit Vertragsgrundlage) zu diesen AGB gelten mit Vertragsunterzeichnung als genehmigt.
3. Änderungen (Hinzuziehung oder Ersetzung) der Subunternehmer werden durch Veröffentlichung mitgeteilt. Der Auftragnehmer 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.
4. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus dem Dienstleistungsvertrag und diesen AGB dem Subunternehmer zu übertragen.
Der Auftragnehmer überzeugt sich von der Einhaltung der vertraglich zugesicherten Sicherheitsmaßnahmen nachweislich und gewissenhaft.
5. Nicht als Untervertragsverhältnisse im Sinne dieser AGB sind solche Dienstleistungen zu verstehen, die der Auftragnehmer 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). Der Auftragnehmer 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.

Informationspflichten, Schriftformklausel, Zurückbehaltungsrecht, Rechtswahl

1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer 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 gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
5. Es gilt deutsches Recht.

Berichtigung, Löschung, Sperrung und Rückgabe der personenbezogenen Daten

1. Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen 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 der Auftragnehmer 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 Vertrag bereits vereinbart.
3. Sollten dem Auftragnehmer durch die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien Kosten entstehen, die der Auftragnehmer nicht zu verantworten hat, kann er 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 Vertrag bereits vereinbart.
5. Nach Auftragsende sind auf Verlangen des Auftraggebers sämtliche 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.

Vergütung

Die Vergütung wird durch den individuellen Dienstleistungsvertrag festgelegt.

Haftung und Schadensersatz

Die Haftung und der Haftungsrahmen werden durch die individuellen Kundenverträge festgelegt.

Anhang 1: Beschreibung der technischen und organisatorischen Maßnahmen – Datensicherungsmaßnahmen (TOM)

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität, Belastbarkeit und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Eingerichtete technische und organisatorische Maßnahmen:

Der Auftragnehmer bezieht über IT-Sourcing Rahmenverträge IT-Leistungen über die

DATEV eG
Baumgartnerstraße 6-14, 90429 Nürnberg

als DATEV Solution Partner. Mit diesem Partner liegen Rahmenverträge, Leistungsbeschreibungen, Service Level Agreements und Verträge nach §11 BDSG vor. Die entsprechenden Sicherungsmaßnahmen der DATEV werden an 1:1 an die Kunden des Auftragsnehmers durchgereicht. Der Zugang für den Auftragnehmer zu allen DATEV-bezogenen Ressourcen wird über eine 2-Faktor-Authentifizierung (Password und Hardware-Dongle) gesichert.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1. Zutrittskontrolle:
Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:
Das gesamte Gelände ist eingezäunt und mit einem Tor versehen. Dabei stellt das Tor die einzige Zutrittsmöglichkeit zum Gelände dar und ist nachts verschlossen. Es gibt ein Zutrittskontrollsystem sowie einen dafür benannten Verantwortlichen. Alle Personen müssen sich verbindlich authentisieren.
Der Außenbereich wird durch Bewegungsmelder überwacht, beziehungsweise beleuchtet. Eine Alarmanlage nach Stufe C des VdS (Verband der Schadenversicherer) ist in allen Räumen des Gebäudes installiert. Gemäß den Anforderungen an Stufe C verfügt die Anlage über einen erhöhten Schutz gegen Überwindungsversuche im scharfen sowie im unscharfen Zustand, die Melder verfügen über eine erhöhte Ansprechempfindlichkeit. Eine weitgehende Überwachung der sicherheitsrelevanten Funktionen ist vorhanden. Zur Alarmierung existiert eine Aufschaltung zu einem externen Wachdienst. Alle Türen und Fenster sind mit der Alarmanlage verbunden. Die Räume sind zusätzlich über Bewegungsmelder gesichert. Bei Alarmierung werden mehrere Ansprechpartner des Unternehmens, die beim externen Wachdienst in einer vorgegebenen Reihenfolge angegeben worden sind, nacheinander alarmiert. Für diesen Zweck werden Bereitschaftsdienste vergeben.
Für die interne Zugangsregelung gibt es einen benannten Verantwortlichen. Hierfür existiert ein Zutritts-Rollenkonzept mit entsprechenden Zuordnungen zu den Sicherheitsbereichen des Unternehmens. Die Rollen sind schriftlich natürlichen und bestimmbaren Personen zugeordnet (Schlüsselliste). Die Schlüsselvergabe wird nach einem Minimalberechtigungssystem durchgeführt und dokumentiert. Auch hierfür ist ein Verantwortlicher benannt.

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

Besucher werden an einem jederzeit besetzten, zentralen Eingangsbereich kontrolliert und im Anschluss ständig im Unternehmen beaufsichtigt. Am Ende des Besuchs melden sich die Besucher ab. Zur Sicherstellung der stetigen Besetzung des Empfangs während der Öffnungszeiten des Gebäudes sind Ablöse- Krankheits- und Urlaubsregelungen getroffen worden.
Der Bereich von Eingang und Lager wird Live-Videoüberwacht.

2. Zugangskontrolle
Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und
-verfahren benutzen:
Die Zugangsmöglichkeiten des Unternehmens zu allen Systemen sind durch Benutzerprofile mit User-ID und Passwort vor unberechtigtem Zugriff geschützt.
Die Zugangsberechtigungen sind stark eingeschränkt, werden flächendeckend eingesetzt und konsequent dokumentiert. Es gibt einen Verantwortlichen für die Vergabe und die Rücknahme von Berechtigungen. Es wird überprüft, ob Nutzer sich abmelden.
Alle Mitarbeiter sind aufgrund ihrer Qualifikationen mit den Grundlagen des sicheren Umgangs mit Datenverarbeitungssystemen, insbesondere mit der Vergabe von sicheren Passwörtern, vertraut oder in diesem Bereich nachweislich geschult worden. Die Mitarbeiter sind durch das Active Directory dazu verpflichtet, kryptische Passwörter zu verwenden: Maximales Alter 90 Tage, minimal 9 Zeichen, Sonderzeichen müssen enthalten sein, sowie Groß- und Kleinschreibung, Nachverfolgung von 4 Passwörtern gegen Wiederholung. Nutzeraccounts werden nach wiederholter fehlerhafter Eingabe falscher Passwörter gesperrt und erst durch einen Administrator händisch wieder freigegeben.

3. 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: Die Berechtigungen können auf Dateien, auf Datensätze, auf Anwendungsprogramme und das Betriebssystem differenziert werden und die Lese-, Änderungs- und Löschrechte einschränken. Es wird sichergestellt, dass jeder Benutzer nur auf die Daten zugreifen kann, zu denen er zugriffsberechtigt ist. Das Berechtigungskonzept, dass sich an den Stellungen der Mitarbeiter orientiert, ist schriftlich festgehalten (Dokumentation über das Active Directory). Verschiedene Zugriffsrechte werden durch vorgefertigte Benutzerprofile zusammengefasst. Weiterhin ist das Berechtigungskonzept programmtechnisch in der Anwendung, im Active Directory hinterlegt. Es gibt ein Berechtigungskonzept, das schriftlich fixiert ist (im AD hinterlegt) und auf Einhaltung überprüft wird. Hierzu ist ein Verantwortlicher auf der Ebene der Geschäftsführung definiert.
Die Vergabe und der Entzug von Rechten werden dokumentiert und an durch eine entsprechende organisatorische Einheit veranlasst.
Zugriffe werden protokolliert und diese Protokolle unterliegen einer regelmäßigen Überprüfung.
Um unbefugten Zugriff zu minimieren, sperren sich die PCs nach Ablauf einer bestimmten Zeitspanne von selbst.
Die Daten werden zentral vorgehalten und die Nutzer arbeiten ausschließlich mit virtuellen Maschinen.
Die durch Akten erhobenen, verarbeiteten oder genutzten personenbezogenen Daten werden in verschlossenen Schränken aufbewahrt, die sowohl während der Arbeitszeiten, als auch nach Dienstende beim Verlassen eines Büros abgeschlossen werden. Gleiches gilt für die Büroräume, in denen sich Schränke zur Aufbewahrung von Akten bzw. die Datenverarbeitungssysteme des Unternehmens befinden.

4. Trennungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:
Es erfolgt eine Trennung der Daten auf physikalischer, logischer und organisatorischer Ebene.

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a, Art. 25 Abs. 1 DS-GVO)
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 der Daten obliegt dem Auftraggeber.

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

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

Es gibt ein Konzept und einen benannten Verantwortlichen für die Berechtigung zur Weitergabe von personenbezogenen Daten. Dieses Konzept regelt die abgabe- und empfangsberechtigten Personen.
Die Weitergabe erfolgt hauptsächlich auf elektronischem Wege. Beteiligte werden durch persönlichen Kontakt oder Formulare und autorisierte Personen Identifiziert und Authentifiziert.
Im Zuge der Weitergabe personenbezogener Daten werden Übertragungsweg, die empfangende und sendende Stelle sowie Benutzer, Zeitstempel, protokolliert und diese Protokolle automatisiert in kurzen Abständen ausgewertet.
Für die Mail-Verschlüsselung wird die DATEV-Lösung „DATEVnet E-Mailverschlüsselung“ eingesetzt, sodass Mail-Inhalte gegen unbefugte Einsichtnahme zusätzlich gesichert werden.

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:

Alle Eingaben personenbezogener Daten werden mit Zeit, Stand vor und nach der Änderung, änderndem Benutzer und der Änderungsgrund protokolliert. Diese Protokolle werden ausgewertet.

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DS-GVO)

Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit

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

Daten werden über eine professionelle Backup-Software zentral gesichert und ein Verantwortlicher für die Datensicherung ist benannt. Dabei ist gewährleistet, dass alle Daten des Unternehmens gesichert werden (ausschließliches Arbeiten auf Virtuellen Maschinen). Es werden Restore-Tests durchgeführt.
Papiere und Akten werden in verschließbaren Behältern gesammelt und datenschutzkonform von einer externen, zertifizierten Firma vernichtet.
Für die ständige Verfügbarkeit wird eine USV eingesetzt, die regelmäßig nachweislich getestet wird.
Die eingesetzte Firewall wird von einer externen Firma im Rahmen eines Silber-Partner-Supportvertrags betreut und die ständige Verfügbarkeit ist sichergestellt.
Täglich aktualisierte Virenscanner überprüfen auf allen Servern und PCs Datenträger, Dateien und ein- und ausgehende Mails. Die Mitarbeiter sind über die Gefahren von Computerviren informiert.
Die eingesetzte Hard- und Software wird zentral beschafft und betreut. Für dienstliche Smartphones wird eine Software zum Mobile Device Management (MDM Software) mit App-Berechtigungssystem eingesetzt.
Fernwartung für Kunden wird über die Software Teamviewer realisiert. Damit ist sichergestellt, dass keine ungefragte Interaktion mit Kundensystemen möglich ist.

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

1. Datenschutz-Management

Die Datenschutz-Grundverordnung bringt für Unternehmen umfassende Nachweispflichten mit sich (sog. „accountability“). 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“).

- Jährliche Datenschutzaudits mit Überprüfung der Datenschutzverfahren
- Regelmäßige Schulungen und Unterweisungen der Mitarbeiter
- Richtlinien für die eigenen Mitarbeiter

2. Incident-Response-Management
Es muss eine Ablaufstrategie vorliegen, was zu tun ist, wenn eine Sicherheitsverletzung entdeckt wird

Es ist ein Prozess zum Umgang mit Sicherheitsvorfällen definiert und umgesetzt. Die Wirksamkeit wird überprüft. Meldungen und Ereignisse werden protokolliert.

3. Datenschutz durch Technikgestaltung und Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
Datenschutz durch Technikgestaltung: Schon bei der Planung und Gestaltung digitaler Technologien werden datenschutzrechtliche Probleme berücksichtigt.
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).

Es wird auf datenschutzfreundliche Voreinstellungen für den Kunden geachtet. Die Rechtmäßigkeit der Datenverarbeitung und des Umfangs der Datenverarbeitung obliegt dem Auftraggeber.

4. Auftragskontrolle
Ohne entsprechende Weisung des Auftraggebers darf der Auftragnehmer keine Auftragsdatenverarbeitung i.S.d. Art. 28 DS-GVO vornehmen (Beispiele: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen).

Die Auftragskontrolle beschreibt die Verantwortung des Auftragnehmers, die Schutzmaßnahmen anderer Unternehmen an die er Aufträge im Zuge der Auftragsdatenverarbeitung vergibt, genau zu prüfen.

Die Umsetzung der Sicherungsmaßnahmen bei unseren Dienstleistern stetig überwacht und vertraglich zugesichert. Weiterhin werden alle Schutzmaßnahmen durch einen benannten Verantwortlichen regelmäßig auditiert.

Anhang 2: Subunternehmer des Auftragnehmers

Firma	Adresse	Kontaktdaten	Art der Verarbeitung
DATEV eG	Baumgartnerstraße 6-14 | 90429 Nürnberg	E-Mail: info@datev.de	IT Sourcing
1&1 Internet SE	Elgendorfer Str. 57 | 56410 Montabaur	E-Mail: info@1und1.de	Hosting der Webseite
Sophos	Amtlich eingetragen in England und Wales, mit registrierten Geschäftsräumen in The Pentagon, Abingdon Science Park, Abingdon OX14 3YP, Vereinigtes Königreich, Ust-Id-Nr GB 991 2418 08	Karlsruhe 0800 2782761 (gebührenfrei aus Deutschland) +49 721 25516-0 (Ausland) Sophos Technology GmbH (Karlsruhe) Amalienbadstr. 41/ Bau 52 76227 Karlsruhe Deutschland Wiesbaden +49 800 2782761 (gebührenfrei aus Deutschland) +49 611 5858-0 (Ausland) Sophos Technology GmbH (Wiesbaden) Gustav-Stresemann-Ring 1 65189 Wiesbaden Deutschland	Firewall
Plusnet GmbH (Centraflex)	Mathias-Brüggen-Str. 55, 50829 Köln	Telefon: 0221 6698050	Telefonanlage
Herrmann, Hüther & Partner Steuerberatungs-gesellschaft	Willi-Melchers-Straße 17, 44534 Lünen	Telefon: 02306 7040	Buchhaltung
estos GmbH	Petersbrunner Str. 3a, 82319 Starnberg	Telefon: 08151 36856 177	Telefonanlage (CTI)
A. & P. Drekopf GmbH & Co. KG	Boettgerstraße 33 | 41066 Moenchengladbach	Telefon: 02161 6894-0 Telefax: 02161 6894-44 E-Mail: info@drekopf.de	Papiervernichtung / verschlossene Container zur Aktenvernichtung
multipack Werbe und Versandgesellschaft mbH	Fujistr. 1 | 47533 Kleve		multipack Werbe und Versandgesellschaft mbH

Anhang 3: Weisungsempfänger beim Auftragnehmer

Name	Kontaktdaten	Position	Weisungsbereich / Befugnisse
Stefan Koch-Niehus	Telefon: +49 2309 95190 E-Mail: info@ckn.de	Geschäftsführer	Vollumfänglich
Dipl.-Inf. Oliver Günter	Telefon: +49 2309 95190 E-Mail: info@ckn.de	Geschäftsführer	Vollumfänglich