Allgemeine Geschäftsbedingungen Datenschutz

der

KDV Kanne Datenverarbeitung GmbH

Sylbeckestraße 20

32756 Detmold

- nachstehend Auftragnehmer genannt–

Gegenstand der Vereinbarung

Gegenstand des Auftrages ist die schriftliche Vereinbarung von Datenschutzgegebenheiten beim Auftragnehmer. Die detaillierten Verarbeitungsvereinbarungen werden durch den individuellen Kundenvertrag (Dienstleistungsvertrag) definiert.

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

Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, 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 erfüllt sind.

Art der Daten

Im Rahmen der Datenverarbeitung werden nur Lohn- und Gehaltsdaten verarbeitet.

Kreis der Betroffenen

Der Betroffenenkreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags - wobei der

GDI
Datenschutz mit Augenmaß

Beratung für:
- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

Anschrift
Fleyer Straße 61
D - 58097 Hagen

Kontakt
Tel: +49 (0) 2331 356 832 - 0
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu
www.gdi-mbh.eu

Geschäftsführer
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01
Amtsgericht Hagen
HRB 8805

Bankverbindung
Sparkasse HagenHerdecke
Konto-Nr.: 100 2012 02
BLZ.: 450 5000 1
IBAN: DE14450500010100201202
BIC: WELADE3HXXX

Deutsche Bank AG Hagen
Konto-Nr.: 710 25 1000
BLZ.: 450 700 24
IBAN: DE20450700240710251000
BIC: DEUTDEDB450

Betroffenenkreis durch die Datenverarbeitungsprozesse des Auftraggebers bestimmt wird - umfasst:

- Mitarbeiter des Auftraggebers

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 informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
4. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er hat personenbezogene Daten zu berichtigen, löschen und zu sperren, wenn der Auftraggeber dies in der getroffenen Vereinbarung oder einer Weisung verlangt.
   Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.
2. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden - automatisierten - Verwaltung. Eingang und Ausgang werden dokumentiert.
3. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
4. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden

GDI
Datenschutz mit Augenmaß

Beratung für:
- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

Anschrift
Fleyer Straße 61
D - 58097 Hagen

Kontakt
Tel: +49 (0) 2331 356 832 - 0
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu
www.gdi-mbh.eu

Geschäftsführer
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01
Amtsgericht Hagen
HRB 8805

Bankverbindung
Sparkasse HagenHerdecke
Konto-Nr.: 100 2012 02
BLZ.: 450 5000 1
IBAN: DE14450500010100201202
BIC: WELADE3HXXX

Deutsche Bank AG Hagen
Konto-Nr.: 710 25 1000
BLZ.: 450 700 24
IBAN: DE20450700240710251000
BIC: DEUTDEDB450

Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

5. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit nach Absprache und mindestens 14 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 die Datenverarbeitungsprogramme sowie Betreten und Besichtigung der Räumlichkeiten des Auftragnehmers, welche die Leistungserbringung für den Auftraggeber betreffen unter Übernahme der für den Auftragnehmer nachweisbaren Kosten berechtigt ist. Der Auftragnehmer verpflichtet sich insoweit dem Auftraggeber oder von diesem beauftragten Dritten (Auditoren) zu diesem Zwecke Zugang zu den Firmenräumen zu gewähren.

6. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich zu bestätigen.

7. Die beauftragten Subunternehmer sind mit Vertragsgrundlage in der Anlage dieser Vereinbarung angegeben. Der Auftragnehmer hat in diesem Falle vertraglich sicherzustellen, dass die vereinbarten Regelungen auch gegenüber Subunternehmern gelten. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Weiterleitung von Daten ist erst zulässig, wenn der Subunternehmer die Verpflichtung nach § 11 BDSG erfüllt hat.

   Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, 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.

8. Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, 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 erfüllt sind.

GDI
Datenschutz mit Augenmaß

Beratung für:
- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

Anschrift
Fleyer Straße 61
D - 58097 Hagen

Kontakt
Tel: +49 (0) 2331 356 832 - 0
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu
www.gdi-mbh.eu

Geschäftsführer
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01
Amtsgericht Hagen
HRB 8805

Bankverbindung
Sparkasse HagenHerdecke
Konto-Nr.: 100 2012 02
BLZ.: 450 5000 1
IBAN: DE14450500010100201202
BIC: WELADE3HXXX

Deutsche Bank AG Hagen
Konto-Nr.: 710 25 1000
BLZ.: 450 700 24
IBAN: DE20450700240710251000
BIC: DEUTDEDB450

Falls ein Subunternehmer beauftragt werden soll, gelten diese Anforderungen zusätzlich.

Datenschutzbeauftragte des Auftragnehmers

Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz

Herr Olaf Tenti
GDI Gesellschaft für Datenschutz und Informationssicherheit mbH
Fleyer Str. 61
58097 Hagen

Tel.-Nr.: 0 23 31 / 35 68 32 0
Fax-Nr.: 0 23 31 / 35 68 32 1

E-Mail-Adresse: info@gdi-mbh.eu
Website: www.gdi-mbh.eu

bestellt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

Datengeheimnis

1. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis zu wahren. Er verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen.
2. Geheimhaltung Auftragnehmer:
   Der Auftragnehmer verpflichtet sich, über nicht allgemein bekannte, geschäftlich relevante und bedeutsame Angelegenheiten des Auftraggebers (Geschäftsgeheimnisse) Verschwiegenheit zu wahren. Er wird auch seine Mitarbeiter zur Verschwiegenheit verpflichten.
3. Geheimhaltung Auftraggeber:
   Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datengeheimnissen des Auftragnehmers vertraulich zu behandeln.
4. Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und sie auf das Datengeheimnis schriftlich verpflichtet. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

GDI
Datenschutz mit Augenmaß

Beratung für:
- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

Anschrift
Fleyer Straße 61
D - 58097 Hagen

Kontakt
Tel: +49 (0) 2331 356 832 - 0
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu
www.gdi-mbh.eu

Geschäftsführer
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01
Amtsgericht Hagen
HRB 8805

Bankverbindung
Sparkasse HagenHerdecke
Konto-Nr.: 100 2012 02
BLZ.: 450 5000 1
IBAN: DE14450500010100201202
BIC: WELADE3HXXX

Deutsche Bank AG Hagen
Konto-Nr.: 710 25 1000
BLZ.: 450 700 24
IBAN: DE20450700240710251000
BIC: DEUTDEDB450

5. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

Datensicherungsmaßnahmen nach der Anlage zu § 9 BDSG (Erläuterungen siehe Anhang)

1. Die im Anhang beschriebenen technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt.
2. An der Erstellung der Verfahrensverzeichnisse hat der Auftragnehmer mitzuwirken. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.
3. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.
4. Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht 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.

Vertragsdauer

Die Vertragslaufzeiten werden durch die individuellen Kundenverträge festgelegt.

Vergütung

Die Vergütung wird durch die individuellen Kundenverträge festgelegt.

Haftung

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

GDI
Datenschutz mit Augenmaß

Beratung für:
- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

Anschrift
Fleyer Straße 61
D - 58097 Hagen

Kontakt
Tel: +49 (0) 2331 356 832 - 0
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu
www.gdi-mbh.eu

Geschäftsführer
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01
Amtsgericht Hagen
HRB 8805

Bankverbindung
Sparkasse HagenHerdecke
Konto-Nr.: 100 2012 02
BLZ.: 450 5000 1
IBAN: DE14450500010100201202
BIC: WELADE3HXXX

Deutsche Bank AG Hagen
Konto-Nr.: 710 25 1000
BLZ.: 450 700 24
IBAN: DE20450700240710251000
BIC: DEUTDEDB450

Sonstiges

1. Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
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. Es gilt deutsches Recht
5. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

GDI
Datenschutz mit Augenmaß

Beratung für:
- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

Anschrift
Fleyer Straße 61
D - 58097 Hagen

Kontakt
Tel: +49 (0) 2331 356 832 - 0
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu
www.gdi-mbh.eu

Geschäftsführer
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01
Amtsgericht Hagen
HRB 8805

Bankverbindung
Sparkasse HagenHerdecke
Konto-Nr.: 100 2012 02
BLZ.: 450 5000 1
IBAN: DE14450500010100201202
BIC: WELADE3HXXX

Deutsche Bank AG Hagen
Konto-Nr.: 710 25 1000
BLZ.: 450 700 24
IBAN: DE20450700240710251000
BIC: DEUTDEDB450

Erläuterungen zu VI - Datensicherungsmaßnahmen

In dem Vertrag müssen die technischen und organisatorischen Maßnahmen festgelegt werden, die bei der Datenverarbeitung umzusetzen sind.

Rechtsgrundlage ist § 11 Abs. 2 BDSG, in dem beschrieben ist, welche Prüfungen ein Auftraggeber vor einer Auftragsvergabe durchzuführen hat. So muss der Auftragnehmer unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt werden. Im Auftrag sind insbesondere die technischen und organisatorischen Maßnahmen schriftlich festzulegen. Auch hat der Auftraggeber zu prüfen, ob beim Auftragnehmer die nach der Anlage zu § 9 BDSG erforderlichen Maßnahmen getroffen werden.

Werden personenbezogene Daten verarbeitet, deren Verarbeitung für die Betroffenen keine besonderen Risiken erwarten lässt, so bietet das Grundschutzhandbuch des BSI für bestimmte technische Konstellationen einen Katalog an Sicherheitsmaßnahmen. (Das Handbuch, in dem die Maßnahmen erläutert werden, kann auf Datenträgern beim BSI (www.bsi.de) bestellt werden.)

Wenn der Auftragnehmer ein Datensicherheitskonzept besitzt, muss der Auftraggeber prüfen und schriftlich festlegen, ob es seinen Anforderungen entspricht. Die Sicherheitsziele sind in der Anlage zu § 9 BDSG genannt. Ist das Konzept nicht ausreichend, sind ergänzende Maßnahmen zu vereinbaren. Das daraus resultierende Sicherheitskonzept sollte zum Vertragsbestandteil gemacht werden. In diesem Fall kann darauf verzichtet werden, im Sicherheitskonzept genannte Maßnahmen im Vertrag zu wiederholen.

Wenn der Auftragnehmer kein Datensicherheitskonzept vorlegen kann, müssen die Maßnahmen im Vertrag vereinbart werden. Dabei sind wiederum die in der Anlage zu § 9 BDSG genannten Sicherheitsziele zu erreichen. Aus dem Katalog sollten die einzelnen Maßnahmen in den Vertrag übernommen werden. Es handelt sich um keinen abschließenden Maßnahmenkatalog. Insbesondere bei der Verarbeitung sensibler Daten sind in der Regel zusätzliche Maßnahmen erforderlich.

Besonders wichtig sind Regelungen zu folgenden Sachverhalten:

- Verantwortlichkeiten: Aus unklaren Aufgabenverteilungen, beispielsweise bei der Vergabe von Zugriffsrechten, resultieren Schwachstellen mit hohen Risiken.
- Abschottung von Netzen: Es müssen Maßnahmen ergriffen werden, um ein unberechtigtes Eindringen in Rechnernetze soweit möglich zu verhindern. Da meist keine absolute Sicherheit zu erreichen ist, müssen derartige Versuche erkannt werden. Technische Komponenten, die in Betracht kommen, sind Firewalls, Intrusion Detection Systeme und insbesondere dem Stand der Technik entsprechende Verschlüsselungsverfahren.
- Abhören der Kommunikation: Zum Schutz gegen unberechtigtes Abhören bietet es sich an, die Daten entsprechend dem Stand der Technik zu verschlüsseln.
- Abmeldeprozeduren: Die Abmeldung am System oder Anwendung stellt die erste und wichtigste Hürde dar, die unbefugte Personen überwinden müssen. An dieser Stelle müssen qualitativ hochwertige Maßnahmen ergriffen werden.

GDI
Datenschutz mit Augenmaß

Beratung für:
- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

Anschrift
Fleyer Straße 61
D - 58097 Hagen

Kontakt
Tel: +49 (0) 2331 356 832 - 0
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu
www.gdi-mbh.eu

Geschäftsführer
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01
Amtsgericht Hagen
HRB 8805

Bankverbindung
Sparkasse HagenHerdecke
Konto-Nr.: 100 2012 02
BLZ.: 450 5000 1
IBAN: DE14450500010100201202
BIC: WELADE3HXXX

Deutsche Bank AG Hagen
Konto-Nr.: 710 25 1000
BLZ.: 450 700 24
IBAN: DE20450700240710251000
BIC: DEUTDEDB450

Anhang I: Beschreibung der technischen und organisatorischen Maßnahmen – Datensicherungsmaßnahmen

1. Zutrittskontrolle:

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

Der Zutritt in das Unternehmen erfolgt über einen Schlüssel, der sich im zugehörigen, zentralen Schließkreis befindet. Bei Verlust eines dieser Schlüssel wird die zentrale Schließanlage ausgetauscht, sodass der verlorengegangene Schlüssel keine Zutrittsmöglichkeit in das Gebäude darstellt. Das Gebäude verfügt über einen Haupteingang und mehrere Fluchttüren. Lediglich der Haupteingang dient dem Zutritt in das Gebäude. In dem Gebäude sind mehrere Unternehmen eingemietet. Der Schließkreis zum Zutritt in das Gebäude ist allen Mietern gemeinsam. Die Zutritte in die Räumlichkeiten der einzelnen Unternehmen sind durch die Treppenhäuser und die damit verbundenen separaten Schließkreise voneinander differenziert.
Durch einen externen Wachschutz wird in unregelmäßigen und undefinierten Abständen das Gebäude außerhalb der Betriebsstunden geprüft. Hierbei wird besonders auf die Anwesenheit von betriebsfremden Personen und den ordnungsgemäßen Zustand aller Türen und Fenster an den äußeren Seiten des Gebäudes geachtet. Die Zustandsprüfung der Türen und Fenster bezieht sich auf den Verschluss, sowie auf eventuelle Beschädigungen. Zusätzlich ist das gesamte Gebäude durch eine Brandmeldeanlage mit einer direkten Verbindung zur Feuerwehr gesichert. Diesbezüglich sind alle Räumlichkeiten mit Bewegungsmeldern ausgestattet.
Firmenfremde werden am zentralen Empfang des Unternehmens abgeholt und innerhalb des Unternehmens begleitet. Besuchern ist es durch die verschlossenen Bereiche des Unternehmens und durch die verschlossenen Etagen nicht möglich sich 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 einzelne Räume/ Bereiche durch vier verschiedene Schließsysteme vor unbefugten Zutritt geschützt. Für alle unterschiedlichen Zutrittsbereiche wird zusätzlich ein Chip mit zugehörigen Berechtigungen benötigt. Für die Vergabe der verschiedenen Zutrittsbefugnisse (Ausgabe der Schlüssel und der Chips) ist die Geschäftsführung zuständig. Die Dokumentation aller vergebenen Zutrittsmöglichkeiten wird ebenfalls durch die Geschäftsführung geführt, so dass die aktuellen Zutrittsbefugnisse der eigenen Mitarbeiter immer bekannt sind. Die Vergabe der einzelnen Zutrittsmöglichkeiten orientiert sich an den verschiedenen Stellungen der Mitarbeiter. Es wird auf eine minimale Vergabe geachtet. Dies trifft auch auf die Schlüsselkarten zu. 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.

Beratung für:
- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

Anschrift
Fleyer Straße 61
D - 58097 Hagen

Kontakt
Tel: +49 (0) 2331 356 832 - 0
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu
www.gdi-mbh.eu

Geschäftsführer
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01
Amtsgericht Hagen
HRB 8805

Bankverbindung
Sparkasse HagenHerdecke
Konto-Nr.: 100 2012 02
BLZ.: 450 5000 1
IBAN: DE14450500010100201202
BIC: WELADE3HXXX

Deutsche Bank AG Hagen
Konto-Nr.: 710 25 1000
BLZ.: 450 700 24
IBAN: DE20450700240710251000
BIC: DEUTDEDB450

In dem Unternehmen gibt es zwei Serverräume: Einen Serverraum im ersten Obergeschoss für das Backup und die Sicherung der Produktionsdaten. Die Tür zu diesem Serverraum befindet sich in einem gesonderten Schließbereich: kaufmännischen Abteilung. Auch die Telefonanlage steht im ersten Stock in einem Serverschrank.
Ein weiterer Serverraum ist im dritten Obergeschoss. Dieser Serverraum verfügt über die Daten zur Bearbeitung des Bereiches Fullservice. Zusätzlich ist in diesem Raum ein Backup-Rechner untergebracht, der im Notfall als Rechenzentrum agieren kann. Dieser Serverraum befindet sich hinter dem Messeraum. Sowohl der Messeraum, als auch der Serverraum sind gesondert im Zutritt beschränkt. In Persona sind der IT-Hauptadministrator und die Geschäftsführung zutrittsberechtigt für den Serverraum im dritten Stock. In dem Serverraum im dritten Stock ist eine Klimaanlage, in dem Serverraum im ersten Stock sind zwei, redundant geschaltete Klimaanlagen installiert. Für die Wartung und die Reinigung der Klimaanlage in den Serverräumen ist eine spezialisierte Wartungsfirma über Wartungsverträge verantwortlich.
Die Haustechnik des Unternehmens sind im Keller hinter einer Stahl- bzw. Tresortür untergebracht. Der gesamte Kellerbereich verfügt über keine Fenster. Die Schlüsselbefugnisse zum Öffnen dieser Tür sind nicht im Schließkreis des Generalschlüssels. Zutrittsberechtigt sind wiederum der IT-Hauptadministrator, sowie die Geschäftsführung. Hinter der Stahltür zum Kellerbereich befindet sich auch der sogenannte Datenschutzbunker. Der Datenschutzbunker ist ein Raum, der komplett von nicht brennbaren Materialen umgeben ist. Die Feuertür zu diesem Raum trägt das Siegel F90. Zutrittsberechtigt zur diesem Raum, indem die Bänder der Datensicherung aufbewahrt werden, sind über einen separaten Schlüssel für die Sicherheitstür der IT-Hauptadministrator und die Geschäftsführung.
Der Internetübergang mit der Hauptleitung und der Back-Up-Leitung (Sicherheitskonzept der Telekom), Hauptanbindung nach Bielefeld, Back-Up-Anbindung nach Paderborn, sind ebenfalls im Datenschutzbunker untergebracht und damit besonders gesichert.
Ebenso ist der Zutritt zu dem Archiv, zum Maschinenraum, zum Bereich Fullservice und zu den Büroräumen der Geschäftsführung des Unternehmens durch gesonderte Berechtigungen abgegrenzt.

2. Zugangskontrolle

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

Der Serverraum, das Archiv, der Kellerraum, der Maschinenraum, der Bereich Fullservice und die Räume der Geschäftsleitung sind im Zugang beschränkt. Über vier verschiedene Schließsysteme werden verschiedenen Berechtigungsgruppen realisiert.
Alle Türen, hinter denen sich personenbezogene Daten befinden, sind immer abgeschlossen oder zusätzlich durch Chips gesichert.
Die Rechner des Unternehmens sind durch Benutzerprofile mit User-ID und Passwort vor unberechtigtem Zugriff geschützt.
Alle Mitarbeiter sind aufgrund ihrer Qualifikationen mit den Grundlagen des sicheren Umgangs mit Datenverarbeitungssystemen, insbesondere

Beratung für:
- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

Anschrift
Fleyer Straße 61
D - 58097 Hagen

Kontakt
Tel: +49 (0) 2331 356 832 - 0
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu
www.gdi-mbh.eu

Geschäftsführer
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01
Amtsgericht Hagen
HRB 8805

Bankverbindung
Sparkasse HagenHerdecke
Konto-Nr.: 100 2012 02
BLZ.: 450 5000 1
IBAN: DE14450500010100201202
BIC: WELADE3HXXX

Deutsche Bank AG Hagen
Konto-Nr.: 710 25 1000
BLZ.: 450 700 24
IBAN: DE20450700240710251000
BIC: DEUTDEDB450

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, die eine Mindestlänge von zehn Zeichen haben und eine Kombination aus Buchstaben, Zahlen und Sonderzeichen darstellen. Durch das Active Directory wird ebenfalls kontrolliert, dass bereits verwendete Passwörter nicht erneut eingesetzt werden können und dass alle Passwörter mindestens alle 42 Tage gewechselt werden. 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.

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. Sämtliche Zugriffe der Benutzer werden protokolliert.
Zum Schutz gegen unberechtigten Zugriff im Arbeitsalltag ist bei allen Benutzerkonten durch das Active Directory der Bildschirmschoner aktiviert. Jedes Konto wird nach zehn Minuten der Inaktivität durch eine erneut erforderliche Eingabe des Passwortes gesichert.
Alle Benutzergeräte zur Verarbeitung personenbezogener Daten sind durch eine Inventarnummer eindeutig gekennzeichnet, werden zentral gewartet und konfiguriert.
Die durch Akten erhobenen, verarbeiteten oder genutzten personenbezogenen Daten werden in verschlossenen Schränken aufbewahrt. Die Schränke werden sowohl während der Arbeitszeiten, als auch nach Dienstende beim Verlassen eines Büros abgeschlossen. Gleiches gilt für die Büroräume, in denen sich Schränke zur Aufbewahrung von Akten bzw. die Datenverarbeitungssysteme des Unternehmens befinden.

4. Weitergabe Kontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer

GDI
Datenschutz mit Augenmaß

Beratung für:
- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

Anschrift
Fleyer Straße 61
D - 58097 Hagen

Kontakt
Tel: +49 (0) 2331 356 832 - 0
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu
www.gdi-mbh.eu

Geschäftsführer
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01
Amtsgericht Hagen
HRB 8805

Bankverbindung
Sparkasse HagenHerdecke
Konto-Nr.: 100 2012 02
BLZ.: 450 5000 1
IBAN: DE14450500010100201202
BIC: WELADE3HXXX

Deutsche Bank AG Hagen
Konto-Nr.: 710 25 1000
BLZ.: 450 700 24
IBAN: DE20450700240710251000
BIC: DEUTDEDB450

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:

Personenbezogene Daten des Unternehmens werden zur Erfüllung der angebotenen Dienstleistungen und zum Nachkommen der gesetzlichen Vorschriften an folgende externe Stellen übermittelt: Krankenkasse, Finanzamt, betroffene Kunden, Sozialversicherung.
Zur Übertragung der Daten wird der Postweg, Fax oder Mail genutzt. Die Berechtigungsstrukturen zum Senden und Empfangen bestimmter Datenkategorien sind durch Zusatzvereinbarungen zu den Dienstleistungsverträgen in jedem Fall schriftlich definiert.

5. 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 mitgebrachen Log Mechanismen und Transaktionsprotokolle, zur Protokollierung aller Eingaben für alle Anwendungen, vorhanden.

6. Verfügbarkeitskontrolle

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

Die Daten auf dem Server werden zentral durch den Systemadministrator gesichert. Die Datensicherung ist konzeptionell durch die ISO 9000 schriftlich definiert. Auch das Testen einer Wiedereinspielung einer Datensicherung ist durch das Konzept gewährleistet. Es ist eine Mehrfachsicherung aller Daten vorhergesehen. Die Backup-Datenträger sind durch die Aufbewahrung im Datenschutzbunker zugriffsbeschränkt und gesondert gesichert. Das Unternehmen setzt eine unterbrechungsfreie Stromversorgung ein, in der Blitz- und Überspannungseinrichtungen integriert sind. Die unterbrechungsfreie Stromversorgung wird automatisch einmal jährlich hinsichtlich ihrer Wirksamkeit getestet. Bei einem Stromausfäll werden alle wichtigen Geräte (Server etc.) automatisch heruntergefahren.
Das Unternehmen verfügt weiterhin über folgende Speichermedien: Diskette, CD-R, CD-RW, DVD, USB und Streamer).
Es wird ein regelmäßig, automatisiert aktualisierter Virenscanner und eine regelmäßig kritisch überprüfte Firewall eingesetzt. Die Konfiguration der Regeln, den Aufbau und das regelmäßige Testen der Firewall wird nach dem Dienstleistungsvertrag von der Firma teuto.net übernommen. Der Betrieb der Firewall wird ständig durch den IT-Hauptadministrator überwacht, sodass 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. Die verschiedenen

Beratung für:
- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

Anschrift
Fleyer Straße 61
D - 58097 Hagen

Kontakt
Tel: +49 (0) 2331 356 832 - 0
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu
www.gdi-mbh.eu

Geschäftsführer
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01
Amtsgericht Hagen
HRB 8805

Bankverbindung
Sparkasse HagenHerdecke
Konto-Nr.: 100 2012 02
BLZ.: 450 5000 1
IBAN: DE14450500010100201202
BIC: WELADE3HXXX

Deutsche Bank AG Hagen
Konto-Nr.: 710 25 1000
BLZ.: 450 700 24
IBAN: DE20450700240710251000
BIC: DEUTDEDB450

Bereiche der EDV arbeiten komplett eigenständig und sind voneinander getrennt: Der Programmierungsbereich und der Bereich Fullservice sind lediglich über Glasfaserkabel mit dem übrigen Rechenzentrumsbereich verbunden. Hier erfolgt also ebenfalls eine galvanische Trennung, um übergreifende Kurzschlüsse zu vermeiden.

7. Trennungskontrolle

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

Es wird eine physikalische Trennung von verschiedenen speichernden Stellen realisiert. Weiterhin wird eine Trennung organisatorisch und logisch durchgeführt.

8. Auftragskontrolle

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

Die Schutzmaßnahmen externer Dienstleister werden durch einen benannten Verantwortlichen regelmäßig auditiert.

GDI
Datenschutz mit Augenmaß

Beratung für:
- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

Anschrift
Fleyer Straße 61
D - 58097 Hagen

Kontakt
Tel: +49 (0) 2331 356 832 - 0
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu
www.gdi-mbh.eu

Geschäftsführer
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01
Amtsgericht Hagen
HRB 8805

Bankverbindung
Sparkasse HagenHerdecke
Konto-Nr.: 100 2012 02
BLZ.: 450 5000 1
IBAN: DE14450500010100201202
BIC: WELADE3HXXX

Deutsche Bank AG Hagen
Konto-Nr.: 710 25 1000
BLZ.: 450 700 24
IBAN: DE20450700240710251000
BIC: DEUTDEDB450