**Vertrag zur Auftragsverarbeitung zwischen**

**Kunde**

**– nachfolgend Verantwortlicher genannt –**

**und**

**optovision GmbH**
**Heinrich-Hertz-Str. 17**
**63225 Langen**

**– nachfolgend Auftragsbearbeiter genannt –**

Diese Auftragsvereinbarung (AVV) regelt die Bearbeitung von Personendaten des Verantwortlichen und definiert Rechte und Pflichten in Bezug auf Datenschutzaspekte – gestützt auf das neue Schweizer Bundesgesetz über den Datenschutz (revDSG) und der Datenschutzgrundverordnung der Europäischen Union (EU-DSGVO).

## § 1 Gegenstand und Dauer des Auftrags

(1) Der Auftragsbearbeiter führt die im Anhang 1 beschriebenen Dienstleistungen für den Verantwortlichen durch. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen werden dort beschrieben.

(2) Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Unterzeichnung beider Parteien in Kraft und gilt, solange der Auftragsbearbeiter für den Verantwortlichen Personendaten verarbeitet. Er endet automatisch mit der Beendigung der Geschäftsbeziehung oder mit dem Ende des Hauptvertrags.

## § 2 Weisungen des Verantwortlichen

(1) Der Verantwortliche ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.

(2) Der Auftragsbearbeiter verarbeitet die ihm zur Verfügung gestellten Personendaten ausschließlich nach den Weisungen des Verantwortlichen und im Rahmen der getroffenen Vereinbarungen. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn der Verantwortliche dies anweist.

(3) Die Verarbeitung erfolgt nur auf Weisung des Verantwortlichen, es sei denn, der Auftragsbearbeiter ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsbearbeiter unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt der Auftragsbearbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(4) Grundsätzlich können Weisungen mündlich erteilt werden. Mündliche Weisungen sind anschließend vom Verantwortlichen zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn der Auftragsbearbeiter dies verlangt.

(5) Ist der Auftragsbearbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Vorschriften verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen.

## § 3 Technische und organisatorische Maßnahmen

(1) Der Auftragsbearbeiter verpflichtet sich, für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen zu treffen und im Anhang 3 dieses Vertrages zu dokumentieren. Die Sicherheitsmaßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. Der Auftragsbearbeiter darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss der Auftragsbearbeiter dem Verantwortlichen nur wesentliche Anpassungen mitteilen.

(3) Der Auftragsbearbeiter unterstützt den Verantwortlichen bei der Einhaltung aller gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. Der Auftragsbearbeiter hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Bearbeitungstätigkeiten dem Verantwortlichen mitzuwirken. Der Auftragsbearbeiter wirkt bei der Erstellung einer Datenschutz-Folgenabschätzung und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden mit. Er hat dem Verantwortlichen alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen.

**§ 4 Pflichten des Auftragsbearbeiters**

(1) Der Auftragsbearbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass er den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Der Auftragsbearbeiter bietet hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Rechten der betroffenen Person steht.

(3) Der Auftragsbearbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) Der Auftragsbearbeiter darf im Rahmen der Auftragsverarbeitung nur dann auf Personendaten des Verantwortlichen zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.

(5) Die Auftragsverarbeitung erfolgt grundsätzlich in der Schweiz, im Europäischen Wirtschaftsraum (EWR), oder in sonstigen Staaten, deren Datenschutzrecht nach Einschätzung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) oder des Schweizerischen Bundesrates einen angemessenen Datenschutz gewährleistet. Jegliche Verlagerung in andere Staaten darf nur mit Zustimmung des Verantwortlichen sowie unter den Bedingungen des Bundesgesetzes über den Datenschutz (DSG) und unter Einhaltung dieses Vertrags erfolgen.

(6) Der Auftragsbearbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen, damit der Verantwortliche seine bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann, z.B. die Information und Auskunft an die betroffene Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. Der Auftragsbearbeiter benennt einen Ansprechpartner, der den Verantwortlichen bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsverarbeitung entstehen, unterstützt und teilt dem Verantwortlichen dessen Kontaktdaten unverzüglich mit. Soweit der Verantwortliche besonderen gesetzlichen Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten unterliegt, unterstützt der Auftragsbearbeiter den Verantwortlichen hierbei. Auskünfte an die betroffene Person oder Dritte darf der Auftragsbearbeiter nur nach vorheriger Weisung des Verantwortlichen erteilen. Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber dem Auftragsbearbeiter geltend macht, wird der Auftragsbearbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

**§ 5 Berechtigung zur Begründung von Unterauftragsverhältnissen**

(1) Der Auftragsbearbeiter darf Unterauftragsbearbeiter nur beauftragen, wenn der Verantwortliche dies vorher schriftlich genehmigt hat.

(2) Ein Unterauftragsverhältnis liegt insbesondere vor, wenn der Auftragsbearbeiter weitere Auftragsbearbeiter in Teilen oder im Ganzen mit Leistungen beauftragt, auf die sich dieser Vertrag bezieht. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragsbearbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B.

Telekommunikationsleistungen oder Reinigungskräfte. Der Auftragsbearbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten dem Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) Ein Zugriff auf Daten darf durch den Unterauftragsbearbeiter erst dann erfolgen, wenn der Auftragsbearbeiter durch einen schriftlichen Vertrag sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den Unterauftragsbearbeiter gelten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den datenschutzrechtlichen Vorschriften erfolgt.

(4) Die Inanspruchnahme der in Anhang 2 zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragsbearbeiter gilt als genehmigt, sofern die in § 5 Abs. 3 dieses Vertrages genannten Voraussetzungen umgesetzt werden.

**§ 6 Kontrollrechte des Verantwortlichen**

Der Auftragsbearbeiter erklärt sich damit einverstanden, dass der Verantwortliche oder eine von ihm beauftragte Person 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 Anforderung von relevanten Unterlagen, die Einsichtnahme in die Verarbeitungsprogramme oder durch Zutritt zu den Arbeitsräumen des Auftragsbearbeiters zu den ausgewiesenen Geschäftszeiten nach vorheriger Anmeldung. Durch geeignete und gültige Zertifikate zur IT-Sicherheit (z.B. IT-Grundschutz, ISO 27001) kann auch der Nachweis einer ordnungsgemäßen Verarbeitung erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht die Pflicht des Auftragsbearbeiters zur Dokumentation der Sicherheitsmaßnahmen im Sinne des § 3 dieser Vereinbarung.

**§ 7 Mitzuteilende Verstöße des Auftragsbearbeiters**

Der Auftragsbearbeiter unterrichtet den Verantwortlichen unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Verantwortlichen mit sich bringen, sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten des Verantwortlichen. Gleiches gilt, wenn der Auftragsbearbeiter feststellt, dass die vom ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. Dem Auftragsbearbeiter ist bekannt, dass der Verantwortliche verpflichtet ist, umfassend alle Verletzungen des Schutzes Personendaten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person unverzüglich zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird der Auftragsbearbeiter den Verantwortlichen bei der Einhaltung seiner Meldepflichten unterstützen. Er wird die Verletzungen des Verantwortlichen unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

a) eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,

b) Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie

d) eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

**§ 8 Beendigung des Auftrags**

(1) Nach Abschluss der Auftragsverarbeitung hat der Auftragsbearbeiter alle Personendaten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der Personendaten besteht.

(2) Der Verantwortliche kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragsbearbeiter einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und der Verantwortliche aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

**§ 9 Schlussbestimmungen**

(1) Sollte das Eigentum des Verantwortlichen bei dem Auftragsbearbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige

Ereignisse gefährdet werden, so hat der Auftragsbearbeiter den Verantwortlichen unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Verantwortlichen ausgeschlossen.

(2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was ab dem 25.05.2018 auch in einem elektronischen Format erfolgen kann.

(3) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

**Anhang 1: Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten**

| | |
|---|---|
| Gegenstand der Verarbeitung | • Die Vereinbarung gilt für alle Leistungen, bei denen der Verantwortliche für die Dauer der Auftragsabwicklung Personendaten an Auftragsbearbeiter übermittelt, die für die Durchführung des jeweiligen Auftrags erforderlich sind. Sie umfasst alle Tätigkeiten, die im Zusammenhang mit dem zugrundeliegenden Auftrag stehen und bei denen Mitarbeiter des Auftragsbearbeiters oder von ihm beauftragte Dritte mit Personendaten des Verantwortlichen in Berührung kommen können. |
| Art und Zweck der Verarbeitung | • Art und Zweck der Verarbeitung von Personendaten durch den Auftragsbearbeiter für den Verantwortlichen sind alle Dienstleistungen, die optovision für den Kunden erbringt. Diese Dienstleistungen können unter anderem die folgenden Tätigkeiten und Ziele umfassen:<br>- Erhebung und Verarbeitung personenbezogener Daten, die im Zusammenhang mit der Abwicklung von Bestellungen von Brillengläsern und optischen Produkten übermittelt werden.<br>- Einrichtung, Bereitstellung und Betreuung (vor-Ort-Service sowie Fernwartung) der Geräte wie Vision Excellence Tower 4.0 usw.<br>- Bereitstellung eines Kunden-Supports (u.a. Fernwartung)<br>- Bereitstellung und Durchführung von Werbedienstleistungen |
| Art der personenbezogenen Daten | • Daten des Verantwortlichen (Nutzers), z.B. Anrede, Name, Vorname, Firma, Adressdaten, E-Mail-Adresse, Telefon- und Faxnummern, Geburtsdatum, Gesundheitsdaten, Funktion<br>• Kundendaten des Verantwortlichen, z.B. Anrede, Name, Vorname, Geschlecht, Adressdaten, E-Mail-Adresse, Telefonnummer, Gesundheitsdaten (u.a. fotografische Aufnahmen des Augenhintergrundes, Analyseauswertungen, Kommentierung) |
| Kategorien betroffener Personen | • Kunden und seine Mitarbeiter<br>• Kunden des Verantwortlichen |

| | |
|---|---|
| Name und Kontaktdaten des Datenschutzbeauftragten des Verantwortlichen (sofern benannt) | |
| Name und Kontaktdaten des Datenschutzbeauftragten des Auftragsbearbeiters (sofern benannt) | optovision GmbH<br>z.Hd. Datenschutzbeauftragter<br>Heinrich-Hertz-Str. 17<br>63225 Langen<br>E-Mail: datenschutz@optovision.com |

**Anhang 2: Liste der beauftragten Unterauftragsbearbeiter einschließlich der Verarbeitungsstandorte**

| **Unterauftragsbearbeiter** (Name, Rechtsform, Sitz der Gesellschaft) | **Verarbeitungsstandort** | **Art der Dienstleistung** |
|---|---|---|
| WACON Internet GmbH | Nollenweg 2,<br>D-65510 Idstein | Pflege der Unternehmenswebsite |
| CLDES | Sonnenberger Str. 52B,<br>D-65193 Wiesbaden | Kreation und Produktion von Mailings |

**Anhang 3: Technisch-organisatorische Sicherheitsmaßnahmen**

In diesem Anhang werden die technisch-organisatorischen Maßnahmen dokumentiert, die durch den Auftragsbearbeiter zur ordnungsgemäßen Erfüllung der erbrachten Dienstleistung umgesetzt werden.

Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

| **Maßnahmen** | **Umsetzung der Maßnahme** |
|---|---|
| **A. Maßnahmen zur Pseudonymisierung**<br><br>Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren | • Pseudonymisierung Personendaten im Rahmen der Marktforschung |
| **B. Maßnahmen zur Verschlüsselung**<br><br>Maßnahmen oder Vorgänge, bei denen ein klar lesbarer Text/ Information mit Hilfe eines Verschlüsselungsverfahrens (Krypto System) in eine unleserliche, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird | • Client VPN Verschlüsselung TLS> 1.1<br>• Site2Site VPN Verschlüsselung AES256, 3DES<br>• Webseiten mit Benutzeranmeldung sind TLS verschlüsselt<br>• Verschlüsselte Kennwortspeicherung in zentralem System |
| **C. Maßnahmen zur Sicherung der Vertraulichkeit**<br><br>**1. Zutrittskontrolle**<br><br>Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen Personendaten verarbeitet werden, sowie zu vertraulichen Akten und Datenträgern physisch verwehren | • PC's werden beim Verlassen des Arbeitsplatzes mit einer Desktop-Sperre belegt<br>• Türsicherung (elektronischer Türöffner, etc.)<br>• gesicherter Serverraum<br>• Zutritt zum Firmengelände: Zaun<br>• Zutritt zum Firmengebäude: Chipkarte, Ausweisleser, kontrollierte Schlüsselvergabe<br>• Zutritt zum Serverraum: Chipkarte nur für ausgewählte Mitarbeiter<br>• Zutritt zur Datensicherung nur durch autorisierte Personen (zutrittsgeschützter Bereich)<br>• Werksüberwachung durch Videoaufzeichnung |

| | |
|---|---|
| **2. Zugangskontrolle**<br><br>Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können | • Zugangswege sind SSL oder AES256 verschlüsselt<br>• Verzeichnisdienst (Active Directory)<br>• Regelmäßig aktualisierte Antiviren- und Spyware Filter<br>• Rechtesystem: Begrenzung der Zahl der berechtigten Mitarbeiter<br>• Firewall-Appliance<br>• Gäste WLAN ist außerhalb des Firmennetzes<br>• Mitarbeiter / Geräte WLAN mit persönlichem PSK (Personal Security Key) geschützt<br>• Virenschutz wird bei Installation der Rechner installiert und regelmäßig aktualisiert. |
| **3. Zugriffskontrolle**<br><br>Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Personendaten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können | • Benutzeranlagen und Rollenänderungen werden vom Fachbereich beantragt. Die Prüfung erfolgt durch den Kostenstellenverantwortlichen, die Umsetzung durch IT-Administratoren.<br>• Active Directory Server: zentrale Rechtevergabe am jeweiligen Standort durch IT-Personal<br>• Es gibt die Anweisung an alle Mitarbeiter vor der Nutzung von USB-Sticks diese aufSchadsoftware zu prüfen.<br>• Zutritt zur Datensicherung nur durch autorisierte Personen (zutrittsgeschützter Bereich) |
| **4. Trennungsgebot**<br><br>Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist | • Tätigkeitsspezifische Rollen für den Filezugriff<br>• Die einzelnen Systeme (ERP/Fileserver/DB) sind auf jeweils getrennten Systemen installiert<br>• Trennung von Test- und Produktivsystemen<br>• Berechtigungskonzepte |
| **D. Maßnahmen zur Sicherung der Integrität**<br><br>**1. Datenintegrität**<br><br>Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden | • Funktionstest bei Installation und Releases/Patches durch IT-Abteilung<br><br>• Das Einspielen von Releases und Patches erfolgt im ERP mit dem Ticketsystem Redmine. Es erfolgt immer erst eine Installation in den Test-Systemen.<br><br>• Client- und Server-Patch-Management auf Microsoft-Systemen wird mit Hilfe |

| | |
|---|---|
| | von Matrix-42durchgeführt.<br><br>• DB-Patches werden auf Basis von Meldungen der Hersteller zyklisch von den Adminseingespielt. Hierbei erfolgt immer zuerst das Ausrollen auf den Test-Systemen. Es werden vor einer Produktiv-Installation Tests durchgeführt.<br><br>Besondere Merkmale der Verfahrensanweisung:<br>• Dokumentation<br>Anforderungen, Risiken, Testvorgaben, Testergebnisse, Architektur, Installationen und Updates werden schriftlich und revisionssicher dokumentiert.<br><br>• Prozesse<br>Definierte Prozesse und Verantwortlichkeiten für Neuentwicklungs- und Wartungsaufgaben.<br><br>• Risiko<br>Alle die Datenintegrität betreffenden Funktionalitäten müssen ein Testverfahrendurchlaufen, abhängig vom Risiko bezüglich der Datenintegrität werden Maßnahmen zur Sicherstellung getroffen. |
| **2. Übertragungskontrolle**<br><br>Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen Personendaten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können. | • Logging<br>• Benutzerberechtigung für die jeweiligen Systeme |
| **3. Transportkontrolle**<br><br>Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden | • VPN Tunnel innerhalb der Unternehmens-Gruppe (MPLS)<br>• Zutritt zur Datensicherung nur durch autorisierte Personen (zutrittsgeschützter Bereich)<br>• Transportprozesse mit individueller Verantwortlichkeit<br>• Verschlüsselungsverfahren die Datenveränderungen während des Transports aufdecken |
| **4. Eingabekontrolle**<br><br>Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann,ob und von wem personenbezogene Daten in DV-Systeme | • Änderungsprotokollierung und Aufbewahrung dieser Protokolle (ERP System) |

| | |
|---|---|
| eingegeben, verändert oder entfernt worden sind. | |
| **E. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit**<br><br>**1. Verfügbarkeitskontrolle**<br><br>Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind | • Wichtige Server sind grundsätzlich redundant ausgelegt. Das gilt auch für HW-Raid-Platten-Systeme.<br>• Wichtige Systeme sind auf räumlich getrennte Rechenzentren verteilt.<br>• Redundante USV's mit Redundanten Unterverteilungen in beiden Rechenzentren vorhanden<br>• Notstromdieselanlagen in beiden Rechenzentren vorhanden<br>• Brandmeldeanlage in beiden Rechenzentren vorhanden<br>• Redundante Klimatisierung der Rechenzentren.<br>• Virtualisierte Systeme mit VMWare<br>• Spezieller Zutrittsschutz zu den Rechenzentren, Bandsicherung und den Tresoren<br>• Monitoring von kritischen Systemen<br>• Rechenzentrum IBM getrennt in 2 RZ-Standorten |
| **2. Rasche Wiederherstellbarkeit**<br><br>Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. | • Notfallplan inkl. Notfallhandbuch<br>• Datensicherungsverfahren<br>• Regelmäßige Tests der Datenwiederherstellung durch Neuaufbau von Testsystemen<br>• Virtualisierte Systeme mit VMWare<br>• Redundantes IBM SAN (Stretched Cluster) |
| **3. Zuverlässigkeit**<br><br>Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden | • Automatisches Monitoring mit E-Mail-Benachrichtigung<br>• Notfallpläne mit Verantwortlichkeiten<br>• IT-Notdienst Bereitschaft |
| **F. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung**<br><br>**1. Überprüfungsverfahren**<br><br>Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen. | • Datenschutzmanagement<br>• Formalisierte Prozesse für Datenschutzvorfälle<br>• Jährliche IT-Prüfung durch externe Wirtschaftsprüfung<br>• Bestellung eines betrieblichen Datenschutzbeauftragten<br>• Datenschutz-Vorfälle: Info an Datenschutzbeauftragten, IT-Leitung und Führungskräfte<br>• Regelmäßige Wartung der technischen Einrichtungen/Wartungsverträge<br>• Testläufe der Notstromdiesel |
| **2. Auftragskontrolle**<br>Maßnahmen, die gewährleisten, dass Personendaten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können | • Weisungen des Verantwortlichen werden dokumentiert (siehe AVV) |