Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitungsvertrag – AVV)

zwischen

Nutzer gemäß Nutzungsvereinbarung CNXT

nachstehend **„Auftraggeber“**

und

Rodenstock GmbH
Elsenheimerstr. 33
80687 München

nachstehend **“Rodenstock“**

Präambel

Rodenstock kommt mit der Erfüllung seiner Services für den Auftraggeber in Berührung mit personenbezogenen Daten. In dieser Vereinbarung werden Regelungen festgelegt, die gewährleisten, dass Rodenstock sorgsam mit den Daten umgeht und somit ein hoher Datenschutzstandard bei dem Auftraggeber und Rodenstock sichergestellt wird.

§ 1 Gegenstand und Geltungsbereich

Zwischen dem Auftraggeber und Rodenstock besteht ein Auftragsverhältnis. Dieser Auftragsverarbeitungsvertrag einschließlich aller Anlagen (nachfolgend gemeinsam als **Vereinbarung** bezeichnet) konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien aus dem zugrundeliegenden Vertrag, der Leistungsvereinbarung und/oder Auftragsbeschreibung einschließlich aller Anlagen (nachfolgend gemeinsam als **Vertrag** bezeichnet). Diese Vereinbarung gilt **für sämtliche Services** bei denen der Auftraggeber Rodenstock zur Durchführung des jeweiligen Auftrages erforderliche personenbezogene Daten für die Dauer der Auftragsabwicklung überlässt oder bei denen es zu einer Verarbeitung oder Wahrnehmung von personenbezogenen Daten durch Rodenstock kommen kann. Der Vertrag, sowie Bestandteile des Vertrages werden auf der CNXT Webseite unter der Rubrik Trust-Center veröffentlicht und können dort jederzeit eingesehen werden.

§ 2 Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung

Gegenstand des Auftrags sind alle Services, welche Rodenstock gegenüber dem Auftraggeber erbringt. Diese können u.a. folgende Tätigkeiten und Zwecke erfassen:

Bereitstellung des Portals CNXT zu folgenden Zwecken:

- Vernetzung verschiedener optischer bzw. medizintechnischer Messgeräte mit diversen Endgeräten (PC's, Tablets, etc.) zum Zweck des Datenaustausches.
- Reduzierung administrativer und manueller Tätigkeiten bezüglich der Datenerfassung für eine Brillenglasberatung und/oder -bestellung.
- Zusammenführung und Speicherung aller erfassten Kunden- und Messdaten, um diese an allen angeschlossenen Geräten verfügbar zu machen.
- Die Daten können über die CNXT Bedienoberfläche editiert werden.
- Auswertung der Daten zum Zwecke der Optimierung und Weiterentwicklung unserer Produkte sowie der Entwicklung neuer Services.

Im Übrigen ergeben sich Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten durch Rodenstock aus dem zugrundeliegenden Nutzungsvertrag. Rodenstock verarbeitet hierbei die personenbezogenen Daten, welche im Rahmen der oben genannten Leistungen genutzt werden. Hierbei kann es sich um folgende Daten handeln:

- Daten des Auftraggebers (Nutzers), z.B. Anrede, Name, Vorname, Firma, Adressdaten, E-Mail-Adresse, Telefon- und Faxnummern, Funktion
- Kundendaten des Auftraggebers, z.B. Anrede, Name, Vorname, Geschlecht, Adressaten, E-Mail-Adresse, Telefonnummer, Gesundheitsdaten (u.a. fotografische Aufnahmen des Augenhintergrundes, Analyseauswertungen, Kommentierung).

Die Vereinbarung endet automatisch bei Beendung der Geschäftsbeziehung bzw. am Ende der Laufzeit des Nutzungsvertrages.

§ 3 Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie zur Wahrung der Rechte der Betroffenen ist allein der Auftraggeber zuständig und somit für die Verarbeitung Auftraggeber im Sinne des Art. 4 Nr.7 DSGVO.

(2) Der Auftraggeber ist berechtigt, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen sind auf Verlangen des Auftraggebers unverzüglich von Rodenstock schriftlich oder in Textform (z.B. per E-Mail) zu bestätigen.

(3) Soweit es der Auftraggeber für erforderlich hält, können weisungsberechtigte Personen benannt werden. Diese wird der Auftraggeber Rodenstock schriftlich oder in Textform mitteilen. Für den Fall, dass sich diese weisungsberechtigten Personen bei dem Auftraggeber ändern, wird dies dem Rodenstock unter Benennung der jeweils neuen Person schriftlich oder in Textform mitgeteilt.

(4) Der Auftraggeber informiert Rodenstock unverzüglich, wenn Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch Rodenstock festgestellt werden.

§ 4 Pflichten von Rodenstock

(1) Datenverarbeitung

Rodenstock wird personenbezogene Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des zugrundeliegenden Hauptvertrages sowie nach den Weisungen des Auftraggebers verarbeiten.

(2) Betroffenenrechte

a. Rodenstock wird den Auftraggeber bei der Erfüllung der Rechte der Betroffenen, insbesondere im Hinblick auf Berichtigung, Einschränkung der Verarbeitung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen seiner Möglichkeiten unterstützen. Sollte Rodenstock die in § 2 dieser Vereinbarung genannten personenbezogenen Daten im Auftrag des Auftraggeber verarbeiten und sind diese Daten Gegenstand eines Verlangens auf Datenportabilität gem. Art. 20 DSGVO, wird Rodenstock dem Auftraggeber den betreffenden Datensatz innerhalb einer angemessen gesetzten Frist, im Übrigen innerhalb von sieben Arbeitstagen, in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen.

b. Rodenstock hat auf Weisung des Auftraggebers die in § 2 dieser Vereinbarung genannten Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder die Verarbeitung einzuschränken. Das Gleiche gilt, wenn diese Vereinbarung eine Berichtigung, Löschung oder Einschränkung der Verarbeitung von Daten vorsieht.

c. Soweit sich ein Betroffener unmittelbar an Rodenstock zwecks Berichtigung, Löschung oder Einschränkung der Verarbeitung der in § 2 dieser Vereinbarung genannten Daten wendet, wird Rodenstock dieses Ersuchen unverzüglich nach Erhalt an den Auftraggeber weiterleiten.

(3) Kontrollpflichten

a. Rodenstock stellt durch geeignete Kontrollen sicher, dass die im Auftrag verarbeiteten personenbezogenen Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des Hauptvertrages und/oder den entsprechenden Weisungen verarbeitet werden.

b. Rodenstock wird sein Unternehmen und seine Betriebsabläufe so gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

c. Rodenstock bestätigt, dass gem. Art. 37 DSGVO und, sofern anwendbar, gemäß § 38 BDSG ein Datenschutzbeauftragter bestellt und die Einhaltung der Vorschriften zum Datenschutz und zur Datensicherheit unter Einbeziehung des Datenschutzbeauftragten überwacht werden. Unseren Datenschutzbeauftragten erreichen Sie wie folgt:

Rodenstock GmbH
z.Hd. Datenschutzbeauftragter
Elsenheimerstr. 33
80687 München

e-Mail: datenschutz@rodenstock.com

(4) Informationspflichten

a. Rodenstock wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine von dem Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Rodenstock ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

b. Rodenstock wird den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützen.

(5) Ort der Datenverarbeitung

Die Verarbeitung der Daten findet grundsätzlich 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 darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(6) Löschung der personenbezogenen Daten nach Auftragsbeendigung

Nach Beendigung des Hauptvertrages wird Rodenstock alle im Auftrag verarbeiteten personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen oder zurückgeben, sofern der Löschung dieser Daten keine gesetzlichen Aufbewahrungspflichten der Rodenstock entgegenstehen. Die datenschutzgerechte Löschung ist zu dokumentieren und gegenüber dem Auftraggeber auf Anforderung zu bestätigen.

§ 5 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, nach rechtzeitiger vorheriger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Geschäftsbetriebes von Rodenstock oder Gefährdung der Sicherheitsmaßnahmen für andere Auftraggeber und auf eigene Kosten, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen

Umfang selbst oder durch Dritte zu kontrollieren. Die Kontrollen können auch durch Zugriff auf vorhandene branchenübliche Zertifizierungen des Unternehmens Rodenstock, aktuelle Testate oder Berichte einer unabhängigen Instanz (wie z.B. Wirtschaftsprüfer, externer Datenschutzbeauftragter, Revisor oder externer Datenschutzauditor) oder Selbstauskünfte durchgeführt werden. Rodenstock wird die notwendige Unterstützung zur Durchführung der Kontrollen anbieten.

(2) Rodenstock wird den Auftraggeber über die Durchführung von Kontrollmaßnahmen der Aufsichtsbehörde informieren, soweit die Maßnahmen oder Datenverarbeitungen betreffen können, die Rodenstock für den Auftraggeber erbringt.

§ 6 Unterauftragsverhältnisse

(1) Der Auftraggeber ermächtigt Rodenstock weitere Unternehmen gemäß den nachfolgenden Absätzen in § 6 dieser Vereinbarung in Anspruch zu nehmen. Diese Ermächtigung stellt eine allgemeine schriftliche Genehmigung i. S. d. Art. 28 Abs. 2 DSGVO dar.

(2) Rodenstock arbeitet derzeit bei der Erfüllung des Auftrags mit den in der **Anlage 2** benannten Unterauftragnehmern zusammen, mit deren Beauftragung sich der Auftraggeber einverstanden erklärt.

(3) Rodenstock ist berechtigt, weitere Unternehmen zu beauftragen oder bereits beauftragte zu ersetzen. Rodenstock wird den Auftraggeber vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines weiteren Unternehmens informieren. Der Auftraggeber kann gegen eine beabsichtigte Änderung Einspruch erheben.

(4) Der Einspruch gegen die beabsichtigte Änderung ist innerhalb von 2 Wochen nach Zugang der Information über die Änderung gegenüber Rodenstock zu erheben. Im Fall des Einspruchs kann Rodenstock nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder – sofern die Erbringung der Leistung ohne die beabsichtigte Änderung dem Unternehmen nicht zumutbar ist, etwa aufgrund von damit verbundenen unverhältnismäßigen Aufwendungen für Rodenstock – diese Vereinbarung sowie den Hauptvertrag ohne Einhaltung einer Frist kündigen.

(5) Bei Einschaltung eines weiteren Unternehmens muss stets ein Schutzniveau, welches mit demjenigen dieser Vereinbarung vergleichbar ist, gewährleistet werden. Rodenstock ist gegenüber dem Auftraggeber für sämtliche Handlungen und Unterlassungen der von ihm eingesetzten weiteren Unternehmen verantwortlich.

§ 7 Vertraulichkeit

(1) Rodenstock ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit verpflichtet.

(3) Rodenstock verpflichtet sich bei der Erfüllung des Auftrags nur Mitarbeiter oder sonstige Erfüllungsgehilfen einzusetzen, die auf die Vertraulichkeit im Umgang mit überlassenen personenbezogenen Daten verpflichtet und in geeigneter Weise mit den Anforderungen des Datenschutzes vertraut gemacht worden sind. Die Vornahme der Verpflichtungen wird Rodenstock dem Auftraggeber auf Nachfrage nachweisen.

(4) Sofern der Auftraggeber anderweitigen Geheimnisschutzregeln unterliegt, wird er dies Rodenstock mitteilen. Rodenstock wird seine Mitarbeiter entsprechend den Anforderungen des Auftraggebers auf diese Geheimnisschutzregeln verpflichten.

§ 8 Technische und organisatorische Maßnahmen

(1) Die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen werden als angemessen vereinbart. Rodenstock kann diese Maßnahmen aktualisieren und ändern, vorausgesetzt dass das Schutzniveau durch solche Aktualisierungen und/oder Änderungen nicht wesentlich herabgesetzt wird.

(2) Rodenstock beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung gemäß Art 32 i. V. m. Art. 5 Abs. 1 DSGVO. Rodenstock gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen. Rodenstock wird alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Standes der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene, ergreifen. Die zu treffenden Maßnahmen umfassen insbesondere Maßnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Maßnahmen, die die Kontinuität der Verarbeitung nach Zwischenfällen gewährleisten. Um stets ein angemessenes Sicherheitsniveau der Verarbeitung gewährleisten zu können, wird Rodenstock die implementierten Maßnahmen regelmäßig evaluieren und ggf. Anpassungen vornehmen.

§ 9 Haftung/ Freistellung

(1) Rodenstock haftet gegenüber dem Auftraggeber gemäß den gesetzlichen Regelungen für sämtliche Schäden durch schuldhafte Verstöße gegen diese Vereinbarung sowie gegen die das Unternehmen treffenden gesetzlichen Datenschutzbestimmungen, die Rodenstock, seine Mitarbeiter bzw. die von Rodenstock mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung verursachen. Eine Ersatzpflicht von Rodenstock besteht nicht, sofern Rodenstock nachweist, dass die dem Unternehmen überlassenen Daten des Auftraggebers ausschließlich nach den Weisungen des Auftraggebers verarbeitet und seinen speziell Rodenstock auferlegten Pflichten aus der DSGVO nachgekommen ist.

(2) Der Auftraggeber stellt Rodenstock von allen Ansprüchen Dritter frei, die aufgrund einer schuldhaften Verletzung der Verpflichtungen aus dieser Vereinbarung oder geltenden datenschutzrechtlichen Vorschriften durch den Auftraggeber gegen Rodenstock geltend gemacht werden.

§ 10 Sonstiges

(1) Im Falle von Widersprüchen zwischen den Bestimmungen in dieser Vereinbarung und den Regelungen des Hauptvertrages gehen die Bestimmungen dieser Vereinbarung vor.

(2) Änderungen und Ergänzungen dieser Vereinbarung setzen die beidseitige Zustimmung der Vertragsparteien voraus unter konkreter Bezugnahme auf die zu ändernde Regelung dieser Vereinbarung. Mündliche Nebenabreden bestehen nicht und sind auch für künftige Änderungen dieser Vereinbarung ausgeschlossen.

(3) Diese Vereinbarung unterliegt dem Recht des Staates mit dem Sitz von Rodenstock.

(4) Als ausschließlicher und internationaler Gerichtsstand gegenüber Kaufleuten im Sinne des Handelsrechts, juristischen Personen des öffentlichen Rechts oder öffentlich-rechtlichen Sondervermögen ist der Sitz von Rodenstock.

(5) Sofern der Zugriff auf die Daten, die der Auftraggeber Rodenstock zur Datenverarbeitung übermittelt hat, durch Maßnahmen Dritter (z.B. Maßnahmen eines Insolvenzverwalters, Beschlagnahme durch Finanzbehörden, etc.) gefährdet wird, hat Rodenstock den Auftraggeber unverzüglich hierüber zu benachrichtigen.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift (Auftraggeber)	Unterschrift (Rodenstock)

Anlagenverzeichnis

Anlage 1 Technische und organisatorische Maßnahmen Rodenstocks zur Gewährleistung der Sicherheit der Datenverarbeitung

Anlage 2 Unterauftragsverhältnisse gemäß § 6 der Vereinbarung zur Auftragsverarbeitung

Anlage 1

Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung

Rodenstock sichert zu, folgende technische und organisatorische Maßnahmen getroffen zu haben:

A. Maßnahmen zur Pseudonymisierung

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.

Beschreibung der Pseudonymisierung:

- Pseudonymisierung personenbezogener Daten im Rahmen der Marktforschung

B. Maßnahmen zur Verschlüsselung

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
- Site2Site VPN Verschlüsselung AES256, 3DES
- Webseiten mit Benutzeranmeldung sind TLS verschlüsselt
- Verschlüsselte Kennwortspeicherung in zentralem System

C. Maßnahmen zur Sicherung der Vertraulichkeit

1. Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie zu vertraulichen Akten und Datenträgern physisch verwehren:

Beschreibung des Zutrittskontrollsystems:

- PC's werden beim Verlassen des Arbeitsplatzes mit einer Desktop-Sperre belegt.
- Gültigkeit von Accounts von externen Mitarbeitern wird auf 12 Monate beschränkt.
- Türsicherung (elektronischer Türöffner, etc.)
- Werkschutz/Pförtner
- Überwachungseinrichtung (Alarmanlagen)
- gesicherter Serverraum
- Kontrollsystem für Besucher
- Firmentelefone durch MDM (Mobile Device Management) geschützt

• Zutritt zum Firmengelände: Zaun, Drehkreuz, Schranke
• Zutritt zum Firmengebäude: Chipkarte, Ausweisleser, kontrollierte Schlüsselvergabe,
• Zutritt zum Rechenzentrum durch externen Dienstleister ISAE3402
• Zutritt zum Serverraum: Chipkarte nur für ausgewählte Mitarbeiter
• Zutritt zur Datensicherung nur durch autorisierte Personen (zutrittsgeschützter Bereich)
• Werkschutz an allen Wochentagen (inkl. Wochenende)
• Werksüberwachung durch Videoaufzeichnung

2. **Zugangskontrolle**

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können.

Beschreibung des Zugangskontrollsystems:

• Zugangswege sind SSL oder AES256 verschlüsselt
• Verzeichnisdienst (Active Directory)
• Regelmäßig aktualisierte Antiviren- und Spyware Filter
• Rechtesystem: Begrenzung der Zahl der berechtigten Mitarbeiter
• Firewall- und UTM-Appliance
• Gäste WLAN mit Voucher geschützt.
• Mitarbeiter / Geräte WLAN mit persönlichem PSK (Personal Security Key) geschützt
• Virenschutz wird bei Installation der Rechner installiert und regelmäßig aktualisiert.

3. **Zugriffskontrolle**

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Beschreibung des Zugriffskontrollsystems:

• Benutzeranlagen und Rollenänderungen werden vom Fachbereich beantragt. Die Prüfung erfolgt durch den Kostenstellenverantwortlichen, die Umsetzung durch IT-Administratoren.
• Windows Active Directory Server: zentrale Rechtevergabe am jeweiligen Standort durch IT Personal
• Es gibt die Anweisung an alle Mitarbeiter vor der Nutzung von USB-Sticks diese auf Schadsoftware zu prüfen.
• Zutritt zur Datensicherung nur durch autorisierte Personen (zutrittsgeschützter Bereich)
• Berechtigungs-Anträge über SharePoint mit Genehmigungsworkflow

4. Trennungsgebot

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.

Beschreibung des Trennungskontrollvorgangs:

• Tätigkeitsspezifische Rollen für den Filezugriff

• Die einzelnen Systeme (SAP/Fileserver/DB) sind auf jeweils getrennten Systemen installiert
• Trennung von Test- und Produktivsystemen
• Berechtigungskonzepte

D. Maßnahmen zur Sicherung der Integrität

1. Datenintegrität

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden:

Beschreibung der Datenintegrität im Allgemeinen:

• Funktionstest bei Installation und Releases/Patches durch IT-Abteilung
• Im SAP gibt es einen geregelten Transport-Ablauf mit 4 Augen-Prinzip
Das Einspielen von Releases und Patches erfolgt im SAP-mit dem Ticketsystem SAP Solution Manager. Es erfolgt immer erst eine Installation in den Test-Systemen. Zusammen mit Key Usern werden vor einer Produktiv-Installation Tests durchgeführt. Ein 4-Augen-Prinzip ist sichergestellt.
• Client- und Server-Patch-Management auf Microsoft-Systemen wird mit Hilfe von MS-WSUS durchgeführt. Für die Produktionsbereiche werden hierbei zuerst Testgruppen bei IT und einzelne User in Fachabteilungen mit den Patchen versorgt und ein mehrwöchiger Testbetrieb durchgeführt. Erst dann erfolgt ein flächendeckendes Ausrollen.
• SAP und DB-Patche werden auf Basis von Meldungen der Hersteller zyklisch von den Admins gepatcht. Hierbei erfolgt immer zuerst das Ausrollen auf den Test-Systemen. Zusammen mit Key Usern werden vor einer Produktiv-Installation Tests durchgeführt.

Zusätzliche Maßnahmen, ausschließlich für CNXT:

• Während des gesamten Lifecycles (Konzept, Entwicklung, Wartung, Ausserbetriebsetzung) findet eine Qualitätssicherung nach den Regeln der Computerized System Validation (CSV) statt.
• Das Qualitätsmanagement von Rodenstock hat eine Verfahrensanweisung zu CSV erlassen und überwacht deren Einhaltung.
• Die Sicherung der Datenintegrität ist ein zentrales Anliegen der CSV-Methodik.

Besondere Merkmale der Verfahrensanweisung:

- Dokumentation
  Anforderungen, Risiken, Testvorgaben, Testergebnisse, Architektur, Installationen und Updates werden schriftlich und revisionssicher dokumentiert.
- Prozesse
  Definierte Prozesse und Verantwortlichkeiten für Neuentwicklungs- und Wartungsaufgaben.
- Risiko
  Alle die Datenintegrität betreffenden Funktionalitäten müssen ein Risiko-Assessment durchlaufen, abhängig vom Risiko bezüglich der Datenintegrität werden Maßnahmen zur Sicherstellung getroffen.

2. Übertragungskontrolle

Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können:

Beschreibung der Übertragungskontrolle:

• Logging

• Benutzerberechtigung für die jeweiligen Systeme

3. Transportkontrolle

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

Beschreibung der Transportkontrolle:

• VPN Tunnel innerhalb der Unternehmens-Gruppe (MPLS)
• Zutritt zur Datensicherung nur durch autorisierte Personen (zutrittsgeschützter Bereich)
• Transportprozesse mit individueller Verantwortlichkeit
• Verschlüsselungsverfahren die Datenveränderungen während des Transports aufdecken

4. 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.

Beschreibung des Eingabekontrollvorgangs:

• Protokollierung sämtlicher Systemaktivitäten und Aufbewahrung dieser Protokolle (SAP System)
• Änderungsbelege im SAP HCM-System

Besonderheit des Eingabekontrollvorgangs bei CNXT:

• Die Daten in CNXT werden durch den Auftraggeber eingegeben, verändert oder entfernt.
• Der Auftraggeber benutzt CNXT mittels seiner Zugangskontrolle.

E. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

1. **Verfügbarkeitskontrolle**

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beschreibung des Verfügbarkeitskontrollsystems:

• Wichtige Server sind grundsätzlich redundant ausgelegt. Das gilt auch für HW-Raid-Platten-Systeme.
• Wichtige Systeme sind auf räumlich getrennte Rechenzentren verteilt.

• Redundante USV's mit Redundanten Unterverteilungen in beiden Rechenzentren vorhanden
• Notstromdieselanlagen in beiden Rechenzentren vorhanden.
• Brandmeldeanlage in beiden Rechenzentren vorhanden
• Gaslöschanlage in beiden Rechenzentren vorhanden.
• Redundante Klimatisierung der Rechenzentren auch bei Stromausfall.
• Virtualisierte Systeme mit VMWare
• Spezieller Zutrittsschutz in den Rechenzentren als auch zur Bandsicherung und den Tresoren.
• Monitoring von kritischen Systemen
• SAP Hochverfügbare Datenbanken
• Rechenzentrum IBM getrennt in 2 RZ-Standorten

2. Rasche Wiederherstellbarkeit

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beschreibung der Maßnahmen zur raschen Widerherstellbarkeit:

• Notfallplan inkl. Notfallhandbuch
• Datensicherungsverfahren
• Regelmäßige Tests der Datenwiederherstellung durch Neuaufbau von Testsystemen (SAP)
• Virtualisierte Systeme mit VMWare
• SAP Hochverfügbare Datenbanken (IBM Redundant an zwei Standorten)

3. Zuverlässigkeit

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

Beschreibung der Maßnahmen zur Zuverlässigkeit:

• Automatisches Monitoring mit E-Mail-Benachrichtigung
• Notfallpläne mit Verantwortlichkeiten
• IT-Notdienst Bereitschaft

F. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

1. Überprüfungsverfahren

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen.

Beschreibung der Überprüfungsverfahren:

• Datenschutzmanagement
• Formalisierte Prozesse für Datenschutzvorfälle
• Jährliche IT-Prüfung durch externe Wirtschaftsprüfung

- Datenschutzbeauftragter
- Datenschutz-Vorfälle Info an Datenschutzbeauftragten, IT-Leitung und Führungskräfte
- Regelmäßige Wartung der technischen Einrichtungen / Wartungsverträge
- Testläufe der Notstromdiesel

2. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

Beschreibung der Maßnahmen zur Auftragskontrolle:

- Weisungen des Auftraggebers werden dokumentiert (siehe AVV)

Anlage 2

Unterauftragsverhältnisse gemäß § 6 der Vereinbarung zur Auftragsverarbeitung

Rodenstock arbeitet derzeit bei der Erfüllung des Auftrags mit den folgenden weiteren Unternehmen zusammen, mit deren Beauftragung sich der Auftraggeber einverstanden erklärt.

1. SpaceNet AG, Joseph-Dollinger-Bogen 14, 80807 München,
   Leistungen: Betreiber externer RZ-Dienstleistungen
2. EasyScan GmbH, Kasinostraße 19-21, D-42103 Wuppertal,
   Leistungen: Lieferung, Installation und Support des Rodenstock FundusScanners
3. ARS Computer und Consulting GmbH, Garmischer Straße 7, 80339 München,
   Leistungen: Unterstützung im Bereich Backend Wartung und Entwicklung.
4. freed Interactive BV, Lauwersweg 9, 9231 GR Surhuisterveen Achtkarspelen, Friesland
   Leistungen: Unterstützung im Bereich Frontend Wartung und Entwicklung.