Technische und organisatorische Maßnahmen

HEUBECK AG
Lösungen zur Altersvorsorge

1. Bezeichnung des Verfahrens und allgemeine Angaben

Bezeichnung des Verfahrens

Gutachten / Einzelfallberechnungen

Version 0.1

Abteilungen, in denen das Verfahren eingesetzt wird (Fachabteilungen / Sachgebiete)

Team Vz

Verantwortlich & nähere Auskunft erteilt:

Dr. Thilo Volz
t.volz@heubeck.de
+49 221 / 93 46 93 – 904

Datenschutzbeauftragter der Auftragnehmerin:

Thomas Wiedemann
t.wiedemann@heubeck.de
+49 221 / 93 46 93 – 909

2. Zweck und Rechtsgrundlagen der Erhebung, Verarbeitung oder Nutzung

Aufgaben, zu deren Erfüllung die personenbezogenen Daten erhoben, verarbeitet oder genutzt werden:	**Rechtsgrundlagen**
Erstellung von Gutachten / Beratung / Erstellung von Einzelfallberechnungen / Einzelfallberechnung	Art. 88 EU-DS-GVO § 26 BDSG, Art. 6 Abs. 1 Buchst. b), Buchst. c) Buchst. f) EU-DS-GVO / Art. 28 EU-DS-GVO

3. Art der gespeicherten Daten

Bezeichnung der Daten
Stammdaten / Gehaltsdaten / Betriebsrentenbezogene Daten / Sozialversicherungsdaten / Versorgungsausgleichsbezogene Daten / Lohnsteuerbezogene Daten

4. Kreis der Betroffenen

Anwärter (aktiv und unverfallbar ausgeschieden) / Rentner / Geschiedene von Anwärtern und Rentnern / Hinterbliebene von Anwärtern oder Rentnern / Anwärter und Leistungsbezieher von sonstigen Arbeitgeberleistungen

5. Art der regelmäßig zu übermittelnden Daten und deren Empfänger

Empfänger und Aufgabe, zu deren Erfüllung die Daten übermittelt werden, sowie weitere Angaben zum Empfänger *(z. B. öffentliche bzw. nicht-öffentliche Stelle, Personalabt. Kunde)*	**Rechtsgrundlage der Übermittlung**	**automatisiertes Abrufverfahren** *(ja/nein)*	**Anlass und Häufigkeit der Übermittlung**
Art der Daten s. Ziffer 3 Kunde / Gerichte / Wirtschaftsprüfer / Betriebsprüfer / ggf. Rückdeckungsversicherer / Steuerberater	Art. 88 EU-DS-GVO i.V.m. § 26 BDSG, Art. 6 Abs. 1 Buchst. b), Buchst. c), Buchst. f) EU-DS-GVO / Art. 28 EU-DS-GVO	nein	Vertragserfüllung / Weisung Auftraggeberin

6. Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung

Zeitraum:

Daten werden nur nach Weisung der Auftraggeberin gelöscht oder in der Verarbeitung eingeschränkt, soweit keine gesetzliche Aufbewahrungspflichten der Auftragnehmerin entgegenstehen.

7. Verarbeitungs- und nutzungsberechtigte Personengruppen

Team Vz

8. Bei Auftragsverarbeitung: Subunternehmer der Auftragnehmerin

Findet eine Auftragsverarbeitung statt:

Ja, es erfolgt eine Auslagerung des Rechenzentrums. Das Rechenzentrum liegt in Frankfurt am Main. Der untengenannte Dienstleister erhält nur im Einzelfall und auf Weisung der HEUBECK AG Zugriff auf die bei der HEUBECK AG gespeicherten Daten. Eine entsprechende Weisung wird nur erteilt, wenn die s zur Aufgabenerfüllung ausdrücklich erforderlich ist. Die unten genannten Subdienstleister haben keinen Zugriff auf die Daten.

Angaben zum Auftragnehmer:

MightyCare Solutions GmbH, Im Wiesengrund 27 53560 Vettelschoß

Subdienstleister:

Telehouse Deutschland GmbH, Kleyerstraße 75 - 87, 60326 Frankfurt (Bereitstellung der Räumlichkeiten)

23 Media GmbH, Johann-Krane-Weg 18, 48149 Münster (Bereitstellung der Infrastruktur innerhalb der Räumlichkeiten)

9. Empfänger vorgesehener Datenübermittlungen in Drittländer

(Staaten außerhalb der EU - Soweit es sich um regelmäßige Datenübermittlungen handelt, sind diese auch in Nr. 5 anzugeben.)

Nein

Empfängerstaat:

Empfänger oder Kategorien von Empfängern:

Art der Daten oder Datenkategorien:

Art der vertraglichen Regelungen mit dem Empfänger:

10. Allgemeine Beschreibung der Art der für das Verfahren eingesetzten Datenverarbeitungsanlagen und der genutzten Software

Netzwerkanbindung:	☒ lokales Netzwerk ☒ VPN ☐ Internet ☐ WAN / Dienstleister
Eingesetzte(s) Betriebssystem(e):	Windows Server 2012 Windows Server 2016 Windows 10 VMWare ESX / Horizon / VCenter Linux (Ubuntu / Debian) Server
Beschreibung der für die Erstellung bzw. dem Betrieb des Verfahrens genutzten Software (z. B. Angaben zu dem genutzten Datenbanksystem, Eigen- oder Fremdentwicklung, Programmiersprache)	Eingesetzte Software: Microsoft Office .NET Framework Visual Basic Microsoft SQL Datenbank Microsoft Exchange Crystal Reports

	Power BI Eigenprogrammierung: Rechenprogramm Standardgutachtenprogramm Altersteilzeitprogramm Office-VBA-Routinen und Funktionen Programmiersprachen: TSQL C C# Visual Basic Office-VBA

11. Schutzziele

Maßnahmen der Zugangskontrolle: *(Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte)*	Die verschiedenen Organisationsbereiche haben differenzierte Zutrittsberechtigungen. Die Eingänge zur Etage sind während der Geschäftszeiten verschlossen und durch ein Kartenlesegerät gesichert. Karten haben nur zutrittsberechtigte Mitarbeiter. Der Haupteingang zur Etage wird während der Geschäftszeiten durch einen ständig besetzten Empfang überwacht, der die Zutrittsberechtigung überprüft. Besucher werden nur in Begleitung eines Mitarbeiters in die Besprechungsräume geführt. Außerhalb der Geschäftszeiten sind die Gebäude verschlossen und werden durch einen Sicherheitsdienst gesichert. Die einzelnen Büros werden bei Abwesenheit der Mitarbeiter verschlossen. Es erfolgt eine Schlüsselvergabe nach einer Schlüsselliste. Bei Dienstschluss werden datenschutzrelevante Akten oder mobile Datenträger in den Schränken verschlossen. Der EDV-Bereich (Server) ist gesondert gesichert. Schlüssel besitzen nur wenige zutrittsberechtigte Mitarbeiter der EDV. Rechenzentrum: Der Zugang zum Rechenzentrum ist durch folgende Maßnahmen gesichert: • Elektronische Zugangssperre • Chipkarten / Transpondersystem • Besucher werden nur in Begleitung eines Rechenzentrum-Mitarbeiters eingelassen • Das Rechenzentrum wird von Wachpersonal überwacht • Es besteht ein Zugangskontrollsystem und ein definierter Zutrittsprozess (Anmeldelisten)

Maßnahmen der Datenträgerkontrolle: *(Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern)*	Vergabe von mobilen Datenträgern wird protokolliert. Mobile Datenträger werden verschlüsselt. Daten der eingehenden mobilen Datenträger werden unverzüglich in den entsprechenden Kundenordnern gespeichert. Mobile Datenträger werden anschließend entsprechend der Weisungen des Auftraggebers verwahrt oder vernichtet. Es gilt das kundenbezogene Berechtigungskonzept der Heubeck AG für auf den Servern gespeicherte Daten
Maßnahmen der Speicherkontrolle: *(Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten)*	Speicherung erfolgt in den Datenbanken. Es erfolgt eine Protokollierung der Änderungen in den Datenbanken. Desweiteren gilt das kundenbezogene Berechtigungskonzept der Heubeck AG
Maßnahmen der Benutzerkontrolle: *(Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte)*	Die Benutzerkontrolle erfolgt über ein Berechtigungskonzept. Der Zugriff wird eingeschränkt auf die verarbeitende Abteilung. Die Zugriffe auf das Datenaustauschportal erfolgt über SSL-VPN und Berechtigungskonzept. Internetzugriff der internen Mitarbeiter erfolgt über DatevNet, Sicherungsmaßnahmen erfolgen durch Datev. Der Zugriff auf Schnittstellen (USB, CD/DVD etc) der EDV-Einrichtungen ist eingeschränkt, es erfolgt ein kontrollierter und protokollierter Zugriff.

Maßnahmen der Zugriffskontrolle: *(Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben)*	Der Zugriff des jeweiligen Mitarbeiters erfolgt lediglich im Rahmen des ihm zugeordneten Benutzerprofils. Identifizierung erfolgt durch Eingabe Benutzername/Passwort. Bei Datenübertragungen verhindern verschiedene Verschlüsselungsverfahren einen unberechtigten Zugriff. Weiterhin gilt das kundenbezogene Berechtigungskonzept der Heubeck AG

Maßnahmen der Übertragungskontrolle: *(Gewährleistung, 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)*	Übermittlungsvorgänge werden protokolliert. Empfangsberechtigte sowie das Verfahren der Übermittlung sind in den Verträgen mit der Auftraggeberin definiert bzw. mit dieser abgestimmt. Bei Übermittlungen von Daten auf Grundlage gesetzlicher Bestimmungen wird der Datenschutzbeauftragte eingeschaltet. Weiterhin gilt das kundenbezogene Berechtigungskonzept der Heubeck AG
Maßnahmen der Eingabekontrolle: *(Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind)*	Es gilt das kundenbezogene Berechtigungskonzept der Heubeck AG für auf den Servern gespeicherte Daten Es werden Datenbanken mit Protokollierung der Eingaben (Zeit/ Benutzer) verwendet.

Maßnahmen der Auftragskontrolle: *(Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können)*	Die zur Verarbeitung oder Nutzung übergebenen Daten werden entsprechend der gesetzlichen Bedingungen nur im Rahmen der Weisungen der Auftraggeberin verarbeitet und nicht an unbefugte Dritte weitergegeben. Der Weisungsrahmen wird in schriftlichen Verträgen gemäß Art, 28 EU-DS-GVO eindeutig festgelegt. Ausnahmen vom konkreten Weisungsrahmen gelten für technisch bedingte Verarbeitungen, z.B. für die interne Datensicherung. Ist es der Auftragnehmerin gestattet, Unterauftragnehmer zu beauftragen wird durch vertragliche Vereinbarungen gemäß Art. 28 EU-DS-GVO sichergestellt, dass auch Subunternehmer die vertraglichen Vorgaben der Auftraggeberin umsetzen. Keine Unterauftragsverhältnisse im Sinne der Absätze 1 bis 2 sind solche Dienstleistungen, die Dritte als Nebenleistungen zur Unterstützung der Auftragsdurchführung bei der Auftragnehmerin erbringen. Hierzu zählen z.B. Telekommunikationsdienstleistungen, Wartung und Benutzerservice, Reinigungskräfte oder die Entsorgung von Datenträgern. Die Auftragnehmerin ist jedoch verpflichtet, auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

Maßnahmen der Transportkontrolle: *(Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden)*	Die Übermittlung personenbezogener Daten erfolgt je nach vertraglicher Vereinbarung entweder auf einem Datenträger auf dem Postweg, mittels Übertragung über das Internet oder über ein Datenaustauschportal. Die Daten werden durch geeignete Verschlüsselungsverfahren gesichert. Konkretes Übermittlungsverfahren wird mit der Auftraggeberin abgestimmt. Der zur Datenübermittlung und Datenannahme berechtigte Personenkreis ist definiert. Die zur Weitergabe berechtigten Personen werden der Auftraggeberin benannt. Protokollierung der Transferdaten auf Einrichtungen zur Datenübertragung Internetverbindung durch regelmäßig aktualisierte Firewalls und Virenscanner gesichert
Maßnahmen der Wiederherstellbarkeit: *(Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können)*	Die Datensicherung erfolgt im 3-2-1 Backupverfahren. Von allen Servern werden tägliche Imagesicherungen angefertigt und einen separaten Brandbereich ausgelagert. Hardwareserver sind durch mindestens doppelte Ausführung redundant ausgelegt und werden in zwei Brandbereichen des Rechenzentrums betrieben. Alle virtuellen Maschinen werden in einem Cluster betrieben. Zusätzlich wird ein monatliches Backup separat in einem Datensafe gelagert.
Maßnahmen der Zuverlässigkeit: *(Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden)*	Alle Systeme unterliegen einer permanenten Überwachung durch PRTG. Grenzwertüber- oder Unterschreitungen werden rechtzeitig erkannt und der Administration mitgeteilt. Die Systemadministration ist über mobile Anbindung an PRTG permanent über den Systemzustand informiert. Die Hardware im Rechenzentrum wird separat über den Dienstleister überwacht.
Maßnahmen der Datenintegrität: *(Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können)*	Entsprechend Backup- und Sicherheitskonzeptes der Heubeck AG, Unterschiedliche Gefahrenklassen (GK). Die Systeme der GK1 und GK2 sind grundsätzlich redundant ausgestattet, so dass typische Hardwaredefekte den Betrieb nicht beeinflussen können. Dies umfasst folgende Maßnahmen: • Die Hardwareserver werden in einem Cluster von zwei Brandabschnitten betrieben, der ausfallsicher ausgelegt ist. • Der Datenbestand wird täglich/wöchentlich/monatlich auf separaten Backupgeräten gesichert, eine dezentrale Aufbewahrung der Monatssicherungen findet auf einem transportablen Datenträger statt.

Maßnahmen zur Verfügbarkeitskontrolle: *(Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind)*	Entsprechend Backup- und Sicherheitskonzeptes der Heubeck AG, Unterschiedliche Gefahrenklassen (GK). Die Systeme der GK1 und GK2 sind grundsätzlich redundant ausgestattet, so dass typische Hardwaredefekte den Betrieb nicht beeinflussen können. Dies umfasst folgende Maßnahmen: • Die Hardwareserver werden in einem Cluster von zwei Brandabschnitten betrieben, der ausfallsicher ausgelegt ist. • Der Datenbestand wird täglich/wöchentlich/monatlich auf separaten Backupgeräten gesichert, eine dezentrale Aufbewahrung der Monatssicherungen findet auf einem transportablen Datenträger statt.
Maßnahmen zur Trennbarkeit: *(Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können)*	Es besteht ein kundenbezogenes Berechtigungskonzept. Der Zugriff des jeweiligen Mitarbeiters erfolgt lediglich im Rahmen des ihm zugeordneten Benutzerprofils t. Es besteht eine klar definierte und einheitliche kundenbezogene Datenablage.

	Köln,
Ort, Datum	Ort, Datum
	HEUBECK AG