Dienstleistungsvertrag

zwischen

Mustermakler, Musterstr. 2, 12345 Musterort

- nachfolgend **Auftraggeber** genannt -

und

dWERK GmbH & Co. KG, Darmstädter Str. 170, 64625 Bensheim

- nachfolgend **Auftragnehmer** oder **dWERK** genannt –

Präambel

dWERK ist ein unabhängiger IT-Dienstleister für einen automatisierten, digitalen Vertriebsprozess im Bereich der betrieblichen Altersvorsorge (bAV).

Der Auftraggeber berät Arbeitgeber in der Umsetzung betrieblicher Altersvorsorgekonzepte. Zur Vereinfachung des bAV-Beratungsprozesses mit den Arbeitnehmern und zur Senkung der Kosten und Steigerung der Effizienz beabsichtigt der Auftraggeber, sich des digitalisierten Beratungsprozesses (dBAV) des Auftragnehmers zu bedienen. Um den digitalisierten Beratungsprozess für seine Beratung nutzen zu können, bedarf der Auftraggeber der Beratung und Einweisung durch den Auftragnehmer.

Hierüber schließen die Vertragsparteien den nachfolgenden Dienstleistungsvertrag, der die gegenseitigen Rechte und Pflichten der Vertragsparteien regelt.

§ 1 - Gegenstand des Vertrages

1. Der Auftragnehmer erstellt für den Auftraggeber den digitalen Beratungsprozess. Der Auftraggeber ist dazu berechtigt, seine Kunden mit dem digitalisierten Beratungstool zu beraten, nicht jedoch dieses für eigene Zwecke zu nutzen.

2. Der Auftraggeber verpflichtet sich zur Zahlung der vertraglich vereinbarten Vergütung.

§ 2 - Pflichten des Auftraggebers

1. Der Auftraggeber erhält vom Auftragnehmer eine Checkliste, die dem Auftragnehmer als Grundlage für seine Entscheidung, ob das Projekt mit dem Kunden des Auftraggebers durchgeführt wird, dient. Der Auftraggeber hat dem Auftragnehmer die in der Checkliste genannten Unterlagen, insbesondere

   - einen unterzeichneten Kollektivvertrag und die
   - Unternehmensstammdaten, Unternehmensstrukturen

   vollständig zur Verfügung zu stellen. Der Auftragnehmer prüft, ob aufgrund der ihm vorgelegten Unterlagen der digitalisierte Beratungsprozess durchgeführt werden kann. Der vorliegende Dienstleistungsvertrag steht unter der auflösenden Bedingung einer positiven Entscheidung durch den Auftragnehmer.

2. Der Auftraggeber stellt nach Bedarf weitere Unterlagen zur Verfügung, zur Vereinfachung weiterer Prozessschritte ist hier eine enge Abstimmung und Zuarbeit notwendig.

3. Der Auftraggeber verpflichtet sich, dem Auftragnehmer wesentliche Anwendungsprobleme mitzuteilen und Verbesserungsvorschläge zu unterbreiten, damit der digitalisierte Beratungsprozess ständig verbessert und weiterentwickelt werden kann.

4. Der Auftraggeber ist für den Vertrieb des Produkts/der Tarife allein und ausschließlich verantwortlich, führt die Kundenakquise eigenverantwortlich durch, berät den Arbeitgeber und vereinbart – wie bisher auch ohne den digitalisierten Prozess – die Kollektivlösung.

5. Der Auftraggeber ist bei der Durchführung der Beratung zur Prüfung gesetzlicher Erfordernisse und Einhaltung der gesetzlichen Vorschriften eigenverantwortlich verpflichtet.

§ 3 - Pflichten des Auftragnehmers

1. Der Auftragnehmer verpflichtet sich, den Auftraggeber in die Anwendung des digitalisierten Beratungsprozesses einzuweisen und in der Vorarbeit zum Beratungsprozess zu schulen.

2. Zur ordnungsgemäßen Nutzung des Beratungstools verpflichtet sich der Auftragnehmer folgende weiteren Dienst- und Beratungsleistungen zu erbringen:

   - Projektierungsunterstützung, Fachadministration, Steuerung der digitalen Prozess-Software
   - Zugriff auf das Betriebsrentenportal
   - Erstellung von Beratungsprotokollen, Antragslisten, Arbeitgeberlisten
   - Bereitstellung der Funktion „Datenausgabe“ in Standard-Schnittstellen und/oder in Papierform

3. Des Weiteren kann der Auftragnehmer vorab den Beratungsprozess ergänzen, z.B. mit weiteren Unternehmensstammdaten sowie Lohn- und Gehaltsdaten und bei der Installation unterstützen. Besondere Vereinbarung: Der Auftraggeber kann die projektbezogene Unterstützung des Auftragnehmers innerhalb der ersten 12 Monate nach Vertragsunterschrift kostenfrei anfragen.

4. Nach abgeschlossener Projektierung und Installation des für den Kunden des Auftraggebers (dem „Arbeitgeber“) personalisierten „dCRYPT“ erhält der Arbeitnehmer einen automatisch generierten Log-in-Code der zur Nutzung des digitalisierten Beratungstools berechtigt. Zusätzlich erhält der Arbeitnehmer mit dem Log-in-Code automatisch einen Freischaltcode. Dieser Freischaltcode ermöglicht dem Arbeitnehmer eine persönliche Berechnung auf Basis eigener Lohn- und Gehaltsdaten und unter Berücksichtigung aller Zulagen und Steuer-, sowie Sozialversicherungsvorteilen.

5. Der Vertragspartner/Kunde des Auftraggebers erlangt keinen eigenen Anspruch auf Verschaffung des Log-in-Codes und des Freischaltcodes gegen den Auftragnehmer. Vertragliche Beziehungen zwischen dem Auftragnehmer und dem Vertragspartner/Kunden des Auftraggebers werden nicht begründet, sofern sich aus diesem oder einem gesonderten Vertrag nichts Abweichendes ergibt.

§ 4 - Schutz des Beratungstools, Schutz des Begleitmaterials

1. Die Parteien gehen davon aus, dass der Beratungsprozess in Deutschland zu Gunsten des Auftragnehmers als Rechteinhaber urheberrechtlich bzw. leistungsrechtlich geschützt ist. Dies gilt auch für weiter verwendete Informationen, Bilder, Präsentationen und weiteres Begleitmaterial. Die von dem Auftragnehmer in diesem Dokument verwendeten Informationen sind ebenfalls urheberrechtlich geschützt. Sämtliche Rechte bleiben vorbehalten.

2. Der Auftraggeber ist verpflichtet, die bestehenden Urheberrechte zu beachten und diese nicht zu verletzen. Der Auftraggeber ist nicht befugt, Informationen, und Daten zum Beratungsprozess zu ändern, zu vervielfältigen, zugänglich zu machen, weiterzuleiten, zu verkaufen oder in anderer Form kommerziell zu nutzen. Urheberrechtshinweise und Markenbezeichnungen dürfen weder verändert noch beseitigt werden. Verkaufsunterlagen sind nur im Original, ohne Veränderungen, einsetzbar. Sollten Veränderungen erforderlich sein, kann dies nur durch Absprache mit dem Auftragnehmer erfolgen.

3. Der Auftragnehmer ist gegenüber dem Auftraggeber nicht verpflichtet, den Source Code des Log-in-Codes oder des personalisierter den Freischaltcodes oder des Beratungstools offenzulegen. Der Auftraggeber hat keinen Anspruch auf Bearbeitung oder Ergänzung des Sourcecodes der genannten Software oder Algorithmen.

4. Für die Nutzung des Titels des Beratungstools oder der Dienstleistungen des Auftragnehmers zum Zwecke der Eigenwerbung durch den Auftraggeber bedarf dieser der vorherigen Zustimmung durch

den Auftragnehmer. Dies gilt ebenfalls für Namen/Kennzeichen/Logos/Abbildungen des Beratungstools oder Dienstleistungen des Auftragnehmers. Im Rahmen der Durchführung des vorliegenden Vertrages sichert der Auftragnehmer jedoch seine Unterstützung zu. Weitere Einzelheiten bedürfen einer gesonderten vertraglichen Vereinbarung.

§ 5 - Rechteeinräumung

1. Der Auftragnehmer ermöglicht dem Kunden des Auftraggebers die Generierung eines Log-in-Code. Gleichzeitig wird ein personalisierter Freischaltcode zur Berechnung erzeugt und dem Kunden des Auftraggebers zur Verfügung gestellt. Die Rechtseinräumung wird erst wirksam, wenn der Auftraggeber die geschuldete Vergütung gemäß § 11 dieses Vertrags und Anlage 1 vollständig geleistet hat. Der Auftragnehmer die Generierung eines Log-in-Codes und die Erzeugung eines personalisierter Freischaltcodes auch schon vor diesem Zeitpunkt vorläufig erlauben. Ein Übergang der Rechte oder die Einräumung weitergehende Rechte nach diesen Paragrafen finde durch eine solche vorläufige Erlaubnis nicht statt.

2. Der Log-in-Code ermöglicht die Nutzung des Beratungstools auf der Webseite „unsere-betriebsrente.de“ zum Zweck der Beratung von Arbeitnehmern im Bereich der betrieblichen Altersvorsorge. Der Freischaltcode legitimiert den jeweiligen Nutzer zur Darstellung der persönlichen Angebote. Sobald der jeweilige Nutzer den Log-in-Code und Freischaltcode erhalten hat, ist dieser maximal für eine Dauer von 7 - 14 Tagen nutzbar. Anschließend verlieren diese ihre Gültigkeit.

3. Der Auftraggeber verpflichtet sich, das Beratungstool ausschließlich für die oben genannten Zwecke zu verwenden. Die Einräumung eines weitergehenden Nutzungsrechts ist damit nicht verbunden. Insbesondere ist der Auftraggeber nicht dazu berechtigt, die Nutzungsrechte an den Log-in-Codes oder Freischaltcodes oder an der Nutzung des Beratungsportals zu vervielfältigen, der Öffentlichkeit zugänglich oder zum Download verfügbar zu machen.

4. Der Auftragnehmer versichert und steht dafür ein, dass er Inhaber des Beratungstools und der Software ist und in der vertragsgegenständlichen Form frei über sie verfügen kann. Der Auftragnehmer garantiert ferner, dass das dem Vertragspartner des Auftraggebers eingeräumte Nutzungsrecht frei von Rechten Dritter ist. Falls dem Auftragnehmer bekannt werden sollte, dass an irgendwelchen Bestandteilen der vertragsgegenständlichen Software Rechte Dritter bestehen, hat er den Auftraggeber hierauf unverzüglich hinzuweisen. Der Auftragnehmer stellt den Auftraggeber hiermit von jeglichen Ansprüchen Dritter in diesem Zusammenhang frei und ersetzt ihm die Kosten der Rechtsverteidigung.

5. Der Auftraggeber garantiert, sämtliche für die beabsichtigte Nutzung weiter erforderlichen Rechte selbst einzuholen bzw. bereits eingeholt zu haben und stellt den Auftragnehmer in diesem Zusammenhang von jeglichen Ansprüchen Dritter frei.

6. Der Auftragnehmer haftet dafür, dass das Beratungstool keinen gesetzeswidrigen oder gegen behördliche Vorschriften oder Auflagen verstoßenden Inhalt aufweist.

7. Die Rechtseinräumung umfasst alle derzeit bekannten und unbekannten Nutzungsarten, die zur Erreichung des Vertragszwecks erforderlich sind oder werden, auch wenn sie erst auf Grundlage neuer Gesetzeslage oder aus anderen Gründen nachträglich entstehen oder erst nachträglich bekannt werden. Für etwa von dieser Rechtseinräumung nicht erfasste Nutzungsarten räumt der Auftragnehmer dem Auftraggeber eine Option zu angemessenen Bedingungen ein.

8. Die vorliegende Rechtseinräumung ist territorial auf die Nutzung in der Europäischen Union beschränkt.

§ 6 - Weitere Rechte und Pflichten der Vertragsparteien

1. Der Auftraggeber ist verpflichtet, eine individuelle Beratung seiner Kunden zu gewährleisten, soweit dies noch erforderlich ist.

2. Der Auftragnehmer erhält Produkte und Tarife von Dritten (Versicherern und/oder eVorsorge). Der Auftragnehmer ist nicht verpflichtet, Inhalte und Qualität dieser Produkte und Tarife zu prüfen.

3. Die Nutzung des Beratungstools setzt eine Authentifizierung voraus. Der Auftragnehmer ist berechtigt, den Log-in-Code zur Nutzung des Beratungsprozesses zu individualisieren und zu kodieren, um eine unautorisierte Nutzung zu verhindern. Der Auftraggeber ist nicht berechtigt, diese Kodierungen zu beseitigen.

4. Der Auftragnehmer behält sich vor, das digitalisierte Beratungstool jederzeit ohne Angaben von Gründen einzustellen und nicht weiter zu pflegen. Gegebenenfalls hat eine Rückerstattung der Vergütung pro rata temporis zu erfolgen. Besondere Vereinbarung: Der Auftragnehmer sichert dem Auftraggeber eine 6-monatige Karenzzeit vor der Abschaltung des Systems zu.

5. Im Übrigen ist der Auftragnehmer verpflichtet, das Beratungstool während der Vertragslaufzeit laufend zu aktualisieren und zu pflegen.

§ 7 - Wettbewerbsverbot/Abwerbeverbot

Beide Vertragsparteien verpflichten sich ferner, während der Dauer dieses Vertrags und ein Jahr nach Beendigung, gegenseitig keine Mitarbeiter des jeweils anderen Vertragspartners aktiv abzuwerben. Für den Fall jeder Zuwiderhandlung ist eine Vertragsstrafe in Höhe von Euro 85.000 je Verstoß an den Geschädigten sofort zur Zahlung fällig.

§ 8 - Haftung

1. Der Auftragnehmer führt sämtliche Beratungsleistungen mit großer Sorgfalt durch, insbesondere um die Entwicklung der Branche und den Bedürfnissen des Auftraggebers in bester Weise gerecht zu werden. Der Auftragnehmer haftet dem Auftraggeber gegenüber nicht für Mängel der ihm von Dritten zur Verfügung gestellten Produkte und Tarife sowie den Erfolg aus der Nutzung des digitalisierten Beratungsprozesses. Die Haftung ist insbesondere dann ausgeschlossen, wenn Versicherungsvorschläge als Ergebnis der Nutzung des Beratungstools auf unrichtigen, unvollständigen oder nicht ordnungsgemäßen Angaben der Nutzer (Kunden des Auftraggebers) beruhen.

2. Der Auftragnehmer haftet nicht für Inhalt und Qualität der Beratung durch den Auftraggeber, ebenso wenig wie für eine fehlende Individualität des Beratungsgespräches und Beratungsprotokolls. Das vom Auftragnehmer im Rahmen des digitalisierten Beratungsprozesses angefertigte Protokoll gibt ausschließlich den Inhalt des standardisierten automatisierten Beratungsprozesses wieder.

3. Der Auftragnehmer haftet nicht dafür, dass die technische Anbindung eines Internet sowie die Herstellung der Dialogfähigkeit und Internet Konnektivität auf Seiten des Nutzers erfolgreich ist bzw. sein wird.

4. Bei Auftreten von Mängeln ist der Auftraggeber verpflichtet, dem Auftragnehmer nachprüfbare Unterlagen zur Verfügung zu stellen und bei der Eingrenzung von Fehlern mitzuwirken und diese umgehend mitzuteilen.

5. Im Übrigen haftet der Auftragnehmer im Falle von Arglist, Vorsatz oder grober Fahrlässigkeit nach Maßgabe der gesetzlichen Bestimmungen. Schäden, die durch leichte Fahrlässigkeit entstanden sind, werden nur ersetzt, wenn es sich dabei um die Verletzung einer wesentlichen Pflicht handelt. In Fällen einer leicht fahrlässigen Verletzung einer wesentlichen Pflicht ist die Haftung der Höhe nach beschränkt auf den bei vergleichbaren Aufträgen dieser Art typischen Schaden, der bei Beauftragung oder spätestens bei der Begehung der Pflichtverletzung vorhersehbar war, maximal jedoch auf die Höhe des Auftragswertes.

6. Schadensersatzansprüche nach dem Produkthaftungsgesetz und für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit bleiben durch die vorstehenden Haftungsbeschränkungen unberührt.

7. Die vorstehenden Haftungsbeschränkungen gelten auch zugunsten von eventuell eingebundenen gesetzlichen Vertretern und Erfüllungsgehilfen des Auftragnehmers.

§ 9 - Veröffentlichung

Der Rechteinhaber garantiert hiermit, dass das Beratungstool bereits veröffentlicht ist.

§ 10 - Vertrags- und Lizenzdauer, Laufzeit, Kündigung

1. Dieser Vertrag beginnt mit beiderseitiger Unterzeichnung und läuft auf die Dauer von 12 Monaten (Vertragsdauer). Der Vertrag verlängert sich stillschweigend um weitere 12 Monate, sofern keiner der Vertragsparteien eine ordentliche Kündigung ausgesprochen hat. Mit Ablauf der Vertragsdauer enden sämtliche Pflichten aus diesem Vertrag mit Ausnahme solcher Regelungen, die ersichtlich auch nach Vertragsende gelten sollen.

2. Dieser Vertrag kann von beiden Parteien aus wichtigem Grund vorzeitig gekündigt werden, insbesondere wenn der Auftraggeber seinen Mitwirkungspflichten gemäß § 2 dieses Vertrages nicht nachkommt, der Auftraggeber fällige Zahlungen gemäß § 13 dieses Vertrages trotz Mahnung und Nachfristsetzung nicht leistet oder die Kontrollrechte des Auftragnehmers gemäß § 7 dieses Vertrages nicht erfüllt. Eine fristlose Kündigung setzt grundsätzlich voraus, dass der andere Teil schriftlich gemahnt und aufgefordert wird, den vermeintlichen Grund zur fristlosen Kündigung in angemessener Zeit zu beseitigen, es sei denn, es liegen besondere Gründe im Sinne der §§ 314 Abs. 2, 323 Abs. 2 BGB vor, die dem Kündigenden ein Festhalten an dem Vertrag auch ohne vorherige Mahnung oder Abmahnung unzumutbar macht.

§ 11 - Vergütung

1. Registrierungsgebühr

Die einmalige Registrierungsgebühr i. H. v. 500,00 € zzgl. Umsatzsteuer ist zu Vertragsbeginn nach Rechnungsstellung an den Auftragnehmer zu zahlen. Soweit der Auftraggeber die angeführte Dienstleistung nicht oder nur eingeschränkt nutzt, berührt dies den Vergütungsanspruch des Auftragnehmers nicht.

Enthalten in der Dienstleistungsgebühr ist die Erstellung einer eigenen dWERK-Berater-Landingpage.

2. Courtagebeteiligungsmodell

Die Einnahmen entstehen bei der Vermittlung von Versicherungsanträgen. Hieraus erhält der AG Abschlusscourtagen, etwaige laufende Abschlusscourtagen, sowie etwaige Bestandspflegecourtagen.

Die damit einhergehenden Stornohaftungsregelungen sind AG und AN bekannt und werden von beiden Seiten akzeptiert. Somit unterliegen AG als auch AN für den jeweils erhaltenen Courtageanteil der Stornohaftung.

AG und AN entscheiden sich für das sogenannte Courtageteilungsmodell.

Die Courtagen werden im Verhältnis 70% AG / 30% AN geteilt.

Die Courtageaufteilung gilt sowohl für sämtliche Abschlusscourtagen, sowie laufende Abschlusscourtagen die dem AG vom jeweiligen Versicherer oder Maklerpool vergütet werden.
Die Bestandspflegecourtagen verbleiben zu 100% beim AG.

3. Individuelle Änderungen/Anpassungen/Erweiterungen

Bei weiterführenden individuellen Umsetzungen bedarf es einer schriftlichen Vereinbarung zwischen Auftraggeber und Auftragnehmer.

4. Zahlungsmodalitäten
Die Vergütung ist nach Rechnungsstellung sofort fällig. Der Zahlungseingang hat nach Rechnungsstellung – ab Eingang beim Auftraggeber spätestens innerhalb von 14 Tage auf das genannte Konto der Rechnung zu erfolgen. Bei weiterführenden individuellen Umsetzungen bedarf es einer schriftlichen Vereinbarung zwischen Auftraggeber und Auftragnehmer.

Die Preise (bis auf die Einnahmen aus dem Courtagebeteiligungsmodell) verstehen sich rein netto, d.h. zzgl. der jeweils geltenden Umsatzsteuer.

§ 12 - Vertraulichkeit/Geheimhaltung

1. Der Auftraggeber verpflichtet sich, das Webportal ausschließlich in vertragsgemäßem Umfang zu nutzen und alle zumutbaren Vorkehrungen zu treffen, die den Missbrauch oder unautorisierten Zugriff durch Dritte verhindern.

2. Die Vertragsparteien verpflichten sich hiermit, alle Informationen und Unterlagen des anderen Vertragspartners, die entweder offensichtlich als vertraulich anzusehen sind oder von anderem Vertragspartner als vertraulich bezeichnet werden, wie Betriebs- und Geschäftsgeheimnisse zu behandeln und nur im Zusammenhang mit diesem Vertrag zu verwenden.

3. Sie sichern sich gegenseitig zu, diese Informationen weder Dritten weiterzugeben, noch in anderer Form Dritten zugänglich zu machen und alle angemessenen Vorkehrungen zu treffen, um einen Zugriff Dritter auf diese Informationen zu vermeiden.

4. Die Geheimhaltungsvereinbarung bezieht sich auf alle Informationen, welche die jeweilige Vertragspartei oder einer ihrer Angestellten oder Erfüllungsgehilfen in Zusammenhang mit diesem Vertrag erlangt oder erlangen wird, insbesondere auf das Know-how und interne Unterlagen des anderen Vertragspartners.

5. Die Geheimhaltungsvereinbarung erstreckt sich auch auf sämtliche Mitarbeiter und beauftragende und beauftragte Vertragspartner ohne Rücksicht auf die Art und rechtliche Ausgestaltung der Zusammenarbeit.

6. Die Vertragsparteien verpflichten sich, diesem Personenkreis entsprechende Geheimhaltungsverpflichtungen aufzuerlegen.

7. Die Geheimhaltungsverpflichtungen nach diesem Vertrag bleiben über die Beendigung des Vertrages hinaus bestehen.

8. Den Vertragsparteien ist bekannt, dass die Verletzung von Betriebs- und Geschäftsgeheimnissen nach den §§ 17,18 UWG strafbar ist und mit Freiheitsstrafe bis zu fünf Jahren geahndet werden kann, und derjenige, der Geschäfts- und Betriebsgeheimnisse verletzt, zum Ersatz des daraus entstandenen Schadens insbesondere nach § 19 UWG verpflichtet ist. Die Vertragsparteien vereinbaren eine Anpassung der vorliegenden Regelung, sobald dies aufgrund gesetzlicher Änderungen, insbesondere des Inkrafttretens des Gesetzes zum Schutz von Geschäftsgeheimnissen, erforderlich wird.

§ 13 - Herausgabe- und Löschungspflichten

Der Auftraggeber verpflichtet sich, nach Beendigung der Vertragsdauer alle ihm einzeln in elektronischer Form vorliegenden vertragsgegenständlichen Informationen und Inhalte zu löschen. Informationen und Inhalte (auch Informationsmaterial und Ähnliches) die in verkörperter Form vorliegen, sind an den Auftragnehmer zurückzugeben oder auf dessen Verlangen hin oder bei Nichtannahme zu vernichten.

§ 14 - Exklusivität

Der Auftragnehmer ist berechtigt, anderen Versicherungsmaklern oder Dritten einen Zugang zur Nutzung des Beratungstools zu ermöglichen, selbst wenn diese zu dem Vertragspartner in einem direkten Konkurrenzverhältnis stehen.

Die ausschließliche Einräumung eines Nutzungsrechts für einen Berechtigten bedarf des gesonderten Abschlusses einer exklusiven Vereinbarung.

§ 15 - Datenschutz

1. Der Auftragnehmer verarbeitet lediglich Daten Dritter, insbesondere von Kunden des Auftraggebers. Ein eigenes Interesse an diesen Daten hat der Auftragnehmer nicht. Zweck und Mittel der Datenverarbeitung werden vom Auftraggeber bzw. dessen Kunden festgelegt. Der Auftragnehmer hat insoweit lediglich eine technische Hilfs- bzw. Unterstützungsfunktion. Die Parteien sind sich deshalb darüber einig, dass der Auftragnehmer als „Auftragsverarbeiter“ i.S. des § 4 Nr.8 DS-GVO anzusehen ist.
2. Im Übrigen verpflichten sich die Vertragsparteien personenbezogene Daten, die sie im Zusammenhang mit diesem Vertrag von der anderen Partei übermittelt erhalten, ausschließlich zum Zweck der Durchführung dieses Vertrages zu verarbeiten und zu nutzen. Näheres regelt die Anlage „Auftragsdatenverarbeitung“.

§ 16 - Anwendbares Recht

Dieser Vertrag unterliegt ausschließlich deutschem Recht unter Ausschluss des UN Kaufrechts.

§ 17 - Nebenabreden (Gerichtsstand, Schriftformklausel)

1. Soweit in diesem Vertrag nicht ausdrücklich etwas anderes angegeben ist, sind sämtliche Erklärungen in Schriftform oder per E-Mail abzugeben. Die E-Mail-Adresse des Auftragnehmers lautet: info@dwerk.de. Die postalische Anschrift des Auftragnehmers lautet: dWERK GmbH & Co. KG Darmstädter Str. 170, 64625 Bensheim.

2. Ausschließlicher Gerichtsstand für alle sich aus diesem Vertrag ergebenden Streitigkeiten ist, soweit eine solche Gerichtsstandvereinbarung zulässig ist, der Sitz des Auftragnehmers.

§ 18 - Salvatorische Klausel

Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden, bleibt die Rechtswirksamkeit der übrigen Bestimmungen hiervon unberührt. Anstelle der unwirksamen Bestimmung gilt eine wirksame Bestimmung als vereinbart, die der von den Parteien gewollten wirtschaftlich am nächsten kommt.

_____	_____
Ort,	Datum
_____	_____
Auftraggeber	dWERK GmbH & Co. KG

Vereinbarung über Auftragsverarbeitung

zwischen

Mustermakler, Musterstr. 1, 12345 Musterort
- Verantwortlicher - nachstehend Auftraggeber genannt -

und

dWERK GmbH & Co. KG, Darmstädter Str. 170, 64625 Bensheim
- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem Dienstleistungsvertrag zwischen Auftraggeber und Auftragnehmer vom TT.MM.JJJJ in ihren Einzelheiten abzuleitenden Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☒ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Erfassung/Import der zur bAV-Beratung relevanten Arbeitnehmer-/Gehaltsdaten in das Online-Beratungssystem der dWERK GmbH & Co.KG und damit verbundener Nebentätigkeiten, Angebotsanfrage und Antragstellung, Vertragsverwaltung

(2) Dauer

☒ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Dienstleistungsvereinbarung zwischen Auftraggeber und Auftragnehmer vom TT.MM.JJJJ.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

☒ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: Erfassung der Gehaltsdaten der bAV-zu-beratenden Arbeitnehmer des Auftraggebers von durch diesen zur Verfügung gestellten Gehaltsabrechnungen („Gehaltszettel“) oder Aufbereitung und elektronischer Import eben dieser auf Basis eines durch den Auftraggeber vorbereiteten Datenexports aus dessen Lohn-/Gehaltsprogramm; damit verbundene Nebentätigkeiten; die Tätigkeiten werden vor Ort in den Räumlichkeiten des Auftraggebers vorgenommen;

der Auftraggeber stellt dazu geeignete Hardware (Windows-PC, -Laptop) sowie eine geeignete Räumlichkeit zur Verfügung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich 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 Art. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

☒ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☒ Personenstammdaten (Adressen, Geburtsdatum, Bankverbindung)
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☒ Planungs- und Steuerungsdaten (Stundenpläne, Einsatzpläne)
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen → Bonitätsdaten)
- ☒ Gehaltsdaten zur Berechnung der Steuer-/Sozialversicherungsersparnis

(3) Kategorien betroffener Personen

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Kunden
- ☒ Interessenten
- ☐ Abonnenten
- ☒ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ Behörden (Finanzämter)
- ☐ SV-Träger
- ☐ Banken

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung,

insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a)

- ☐ Schriftliche Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
- ☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
- ☒ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Frank Berns, Konzept 17 GmbH, Westring 3, 24850 Schuby benannt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b)

☐ Der Auftragnehmer ist nicht zur Benennung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

c)

☐ Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

d)

Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

e)

Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

f)

Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

g)

Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

h)

Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

i)

Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

j)
Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☒ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
dWERK GmbH & Co. KG	Darmstädter Str. 170, 64625 Bensheim	gemäß 2.(1)
DATIS IT-Services GmbH	Weberstr. 2, 68165 Mannheim	gemäß Anlage TOM
eVorsorge Systems GmbH	Leopoldstraße 244, 80807 München	Angebotsabfrage, Antragstellung, Vertragsverwaltung (Arbeitgeber-, Arbeitnehmerportal)

c) ☐ Die Auslagerung auf Unterauftragnehmer

oder

☒ der Wechsel des bestehenden Unterauftragnehmers

sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe personenbezogener Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;

☒ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform).

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

☒ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

☐ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer

sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

_____	_____
Ort	Datum
_____	_____
Auftraggeber	dWERK GmbH & Co. KG

Anlagen

Technische und organisatorische Maßnahmen (TOM)

Technische und organisatorische Maßnahmen
der dWERK GmbH & Co. KG
gemäß Art. 32 Abs. 1 DS GVO für Verantwortliche (Art. 30 Abs. 1 lit. g)
und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

Die dWERK GmbH & Co KG, Anbieter von Digitalisierungsprozessen im Bereich betrieblicher Altersversorgung, trifft nachfolgende und technische organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.
Die nach den Maßnahmen genannten Referenzen in Klammern beziehen sich auf Anhang A der ISO 27001 als umzusetzende Pflichtmaßnahmen.

1. Pseudonymisierung

- Personenbezogene Daten werden unter einem Pseudonym abgelegt, erst bei Entschlüsselung werden diese Daten entschlüsselt.

2. Verschlüsselung

Die Übertragung sämtlicher personenbezogener Daten zwischen den einzelnen Anwendungen (crmLight, MS Dynamics, WebPortal) werden verschlüsselt und erfolgen durch verschlüsselte SSL-Verbindungen. Der Aufruf der Portalanwendung durch den Kunden, erfolgt über das HTTPS-Protokoll.

Alle Passwörter der Anwendungen werden verschlüsselt gespeichert, so dass weder der Betreiber der Anwendungen noch dWERK in Kenntnis der Klartextpasswörter gelangen können.

3. Vertraulichkeit

Sämtliche Daten werden auf Dedicated Servern bzw. Backup-Servern in einem Rechenzentrum der Firma Datis It - Services GmbH - Weberstr. 2 – DE-68165 Mannheim gespeichert.

Zugangskontrolle und Sicherheit

Folgende Maßnahmen wurden getroffen:

- Zugangssteuerungsrichtlinie (A.9.1.1)
- Zugang zu Netzwerken und Netzwerkdiensten nur durch die Personen möglich, die für die Nutzung befugt sind (A.9.1.2)
- Prozess zur Benutzerzugangsverwaltung (A.9.2)
- Regeln für den Umgang geheimer Authentisierungsinformationen (A.9.3.1)
- Zugangssteuerung für Systeme und Anwendungen (A.9.4)
- Definition von Sicherheitsbereichen mit physischer Zutrittssteuerung (A.11.1)
- Sichern von und Arbeiten in Büros, Räumen und Einrichtungen (A.11.1)
- Schutz vor externen und umweltbedingten Bedrohungen (A.11.1)
- Netzwerksicherheitsmanagement (A.13.1)

- Sicherheit in der Informationsübertragung (A.13.2)

Zugriffskontrolle

- Mandantenfähigkeit
- Trennung von Test- und Produktionssystem

im Testsystem befinden sich keine echten personenbezogenen Daten.

- Administrationskonzept nach dem Least-Privilege-Model (nur so viel Zugriffsrechte wie benötigt wird).

Jeder Mitarbeiter der Firma dWERK, der Zugang zu den Anwendungen CrmLight, und MS Dynamics (nachfolgend als Anwendungen benannt) hat, erhält eine eigene Benutzerkennung mit Passwort; es ist nur Ihnen bekannt.
Endanwender, also Kunden, die sich über das WEB-Portal beraten lassen, bekommen einen 16-stelligen Schlüssel und einen Freischaltcode, die ihnen in einem verschlossenen Umschlag von ihrem Firmenadministrator übergeben werden.

Trennung

Die Software ist eine mandantenfähige Software. Zur Trennung der Daten verschiedener Mandanten werden sämtliche Datensätze des Auftraggebers parametrisiert mit einer eindeutigen, dem Auftraggeber zugeordneten Kennung und können somit mandantenspezifisch gefiltert werden.

4. Gewährleistung der Integrität

Eingabekontrolle

Sämtliche Eingaben, Änderungen und Löschungen von personenbezogenen Daten in den Anwendungen werden protokolliert. Sofern der Zugriff auf die Anwendungen durch einen angemeldeten Benutzer erfolgt, wird die Eingabe, Änderung oder Löschung unter diesem angemeldeten Benutzer protokolliert. Diese Protokolle sind mit dem Datensatz über die jeweilige Person in der Datenbank assoziiert und werden vollständig und datenschutzgerecht gelöscht, wenn der zugehörige Personen/Mandanten-Datensatz gelöscht wird. Der Zugriff auf diese Protokolle ist für authorisierte Mitarbeiter des Auftraggebers (dWERK) und für befugte Supportmitarbeiter möglich. (dWERK, PTA).

Weitergabekontrolle

Die Übertragung sämtlicher personenbezogener Daten zwischen den einzelnen Anwendungen (crmLight, MS Dynamics, WebPortal) werden verschlüsselt und erfolgt durch verschlüsselte SSL-Verbindungen. Der Aufruf der Portalanwendung durch den Kunden, erfolgt über das HTTPS-Protokoll.
Alle Mitarbeiter von dWERK sind verpflichtet, den sicheren Umgang mit personenbezogenen Daten im Sinne des Artikel 32 Abs. 4 DS-GVO sicherzustellen.

5. Gewährleistung der Verfügbarkeit

- Platzierung und Schutz von Betriebsmitteln (A.11.2.1)
- Versorgungseinrichtungen (USV, Kälte, Notstrom, Rechenzentrums Infrastruktur) (A.11.2.2)
- Sicherheit der Verkabelung (Energie, Netze, Einspeisung, Redundanzen) (A.11.2.3)
- Instandhalten von Geräten und Betriebsmitteln (A.11.2.4)
- Schutz vor dem Entfernen von Werten (A.11.2.5)
- Schutz vor Missbrauch außerhalb der Firmengelände (A.11.2.6)
- Maßnahmen zur sicheren Entsorgung besonders von Datenträgern (A.11.2.7)
- Richtlinien für Arbeitsgeräte (A.11.2.8+9)
- Kapazitätssteuerung (A.12.1.3)
- Durchführung einer angemessenen Datensicherung (A.12.3)

6. Gewährleistung der Belastbarkeit der Systeme

- Permanente Überwachung der Auslastung von Kundensystemen (CPU, RAM, Festspeicher) mit automatischer Benachrichtigung bei Überschreitung von Schwellwerten
- Maßnahmen zur Anschaffung, Entwicklung und Instandhaltung von Systemen (A.14)
- Mit Kunden vereinbarte Verfahren im Fall von Kapazitätsüberschreitungen

7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

- Business Continuity Management: Planen, Umsetzen und Überprüfen von Maßnahmen zur Aufrechterhaltung der Informationssicherheit auch nach einem Notfall (A.17.1)
- Bereitstellung von Redundanzen (A.17.2)

8. Verfahren regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

- Handhabung technischer Schwachstellen (A.12.6)
- Audit von Informationssystemen (A.12.7.1)
- Handhabung von Informationssicherheitsvorfällen (A.16)
- Unabhängige Überprüfung der Informationssicherheit (A.18.2.1)
- Überprüfung der Einhaltung von Sicherheitsrichtlinien und –standards (A.18.2.2)
- Überprüfen der Einhaltung technischer Vorgaben (A.18.2.3)
- Risikomanagement
- Alle Mitarbeiter von dWERK werden über die Notwendigkeiten des vertraulichen Umgangs mit personenbezogenen Daten informiert und zu deren Einhaltung verpflichtet.

Die beschriebenen technischen und organisatorischen Maßnahmen werden quartalsweise durch dWERK geprüft und bewertet