Vereinbarung zur Auftragsverarbeitung

ePension Arbeitgeber-Portal

gemäß Art. 28 Datenschutz-Grundverordnung (DS-GVO)

Die **ePension GmbH & Co. KG,** Beim Strohhause 27, 20097 Hamburg (nachfolgend "die ePension KG oder „Auftragnehmer" genannt) vereinbart hiermit mit dem Arbeitgeber (nachfolgend auch: „der Auftraggeber“ genannt) gemäß Art. 28 DS-GVO folgende Regelungen zur Verarbeitung personenbezogener Daten durch das ePension Arbeitgeber-Portal:

1. Gegenstand und Dauer des Auftrags

1.1 Das ePension Arbeitgeber-Portal stellt Funktionalitäten zur elektronischen Beantragung und Verwaltung von Vorgängen und Verträgen zur betrieblichen Altersversorgung (bAV) bereit, die nach Maßgabe des deutschen Betriebsrentengesetzes (BetrAVG) konzipiert sind und bei denen sich Versicherer als Versorgungsträger oder zur Rückdeckung verpflichtet haben sowie gegebenenfalls zu sonstigen betrieblichen Vorsorgelösungen wie zum Beispiel der betrieblichen Krankenvorsorge (bKV).

Der Arbeitgeber hat sich gemäß den gesonderten „Allgemeinen Nutzungsbedingungen für das ePension Arbeitgeber-Portal“ (Grundversion oder Upgrade-Version) für die Nutzung des ePension Arbeitgeber-Portals registriert bzw. einen Aktivierungsantrag gestellt.

Zum Zweck der bAV bzw. der sonstigen betrieblichen Vorsorge (zum Beispiel bKV) verarbeitet das ePension Arbeitgeber-Portal personenbezogene Daten für den Arbeitgeber i.S.v. Art.4 Nr. 2 und Art.28 DS-GVO auf Grundlage dieses Auftrags.

1.2 Gegenstand und Dauer des Auftrags bestimmen sich nach der Registrierung des Auftraggebers für das ePension Arbeitgeber-Portal und den dabei vereinbarten „Allgemeinen Nutzungsbedingungen für das ePension Arbeitgeber-Portal“ (je nach Auftrag Grundversion oder Upgrade-Version). Das Recht beider Parteien zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien betroffener Personen

2.1 Der Auftrag erfasst alle Arten von Verarbeitungen im Sinne der Datenschutz-Grundverordnung (DS-GVO). Zweck der Verarbeitung ist die Erfüllung des Auftrags gemäß Ziffer 1.1.

2.2 Die Verarbeitungen des Auftragnehmers erfassen alle Arten von personenbezogenen Daten zu allen Kategorien betroffener Personen, die der Auftraggeber gemäß den vertraglich vereinbarten Funktionalitäten des ePension Arbeitgeber-Portals dem Auftragnehmer zur Erfüllung des Auftrags gemäß Ziffer 1.1 offenbart, zum Beispiel (aber nicht ausschließlich) Personenstammdaten, Vertragsdaten und Kontaktdaten der Beteiligten von bAV- und bKV-Verträgen, insbesondere Arbeitnehmer und sonstige Begünstigte einer bAV, bKV oder sonstigen betrieblichen Vorsorgelösung, Arbeitgeber und Versicherer (einschließlich deren Sachbearbeiter).

Die Entscheidung, welche Arten von personenbezogenen Daten zu welchen Kategorien betroffener Personen er vom Auftragnehmer im Rahmen des Auftrags gemäß Ziffer 1.1 verarbeiten lässt, trifft ausschließlich und in eigener Verantwortung der Auftraggeber.

3. Technische und organisatorische Maßnahmen

3.1 Der Auftragnehmer trifft alle technischen und organisatorischen Maßnahmen zum angemessenen Schutz der vereinbarungsgegenständlichen Daten gemäß der

Anlage zu 3.1: Technische und organisatorische Maßnahmen.

Dem Auftragnehmer ist es gestattet, die technischen und organisatorischen Maßnahmen nach Vertragsschluss zu ändern oder anzupassen, wobei er sicherstellt, dass das damit weiterhin das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3.2 Der Auftraggeber hat sich vor Erteilung des Auftrags gemäß Ziffer 1.1 über die technischen und organisatorischen Maßnahmen des Auftragnehmers anhand der vom Auftragnehmer bereitgestellten Informationen gemäß der Anlage 3.1 sowie Ziffer 9 dieser Vereinbarung informiert und wird dies nach Vertragsschluss in regelmäßigen Abständen tun. Der Auftraggeber trägt die Verantwortung dafür, dass die jeweils aktuell geltenden, vertraglich vereinbarten technischen und organisatorischen Maßnahmen für die Risiken der vom Auftraggeber bestimmten, zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

3.3 Wenn der Auftraggeber nach Abschluss dieser Vereinbarung entscheidet, dass die bislang vorhandenen technischen und organisatorischen Maßnahmen des Auftragnehmers zum Schutz bestimmter personenbezogener Daten unter Berücksichtigung der Kriterien des Art. 32 Absatz (1) DS-GVO nicht ausreichen, wird er dem Auftragnehmer vor der Offenbarung dieser bestimmten Daten die zusätzlich erforderlichen Maßnahmen benennen und mit dem Auftragnehmer eine Vereinbarung dazu treffen, welche Vertragspartei welche Maßnahmen zu welchen Kosten veranlassen wird.

4. Ort der Verarbeitung

Der Auftragnehmer verarbeitet die vereinbarungsgegenständlichen Daten in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum.

Der Auftragnehmer ist nur dann befugt, die Daten in einen Staat außerhalb der Europäischen Union bzw. außerhalb des Europäischen Wirtschaftsraums (sogenanntes „Drittland“) zu verlagern, sofern hierfür das in der Datenschutz-Grundverordnung festgelegte Schutzniveau für die vertragsgegenständlichen Daten gemäß den Art. 44 ff. DS-GVO gewährleistet wird.

5. Berichtigung, Einschränkung und Löschung von Daten; Anfragen von betroffenen Personen

5.1 Der Auftragnehmer darf die vereinbarungsgegenständlichen Daten nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Zur Weisungserteilung durch den Auftraggeber gilt Ziffer 10 dieser Vereinbarung (unten).

5.2 Für die Beantwortung von Anfragen Betroffener zur Geltendmachung ihrer Rechte, etwa auf Auskunftserteilung, Berichtigung, Einschränkung oder Löschung, ist ausschließlich der Auftraggeber zuständig und verantwortlich. Er ist befugt, dazu die mit dem Auftragnehmer vereinbarten Funktionalitäten des ePension Arbeitgeber-Portals zu nutzen.
Regelungen über eine Vergütung von Mehraufwendungen des Auftragnehmers, die durch dessen Mitwirkungsleistungen im Zusammenhang mit geltend gemachten Betroffenenrechten gegenüber dem Auftraggeber entstehen, bleiben unberührt. Für den Fall, dass der Auftraggeber das Ersuchen der betroffenen Person nicht, nicht richtig oder nicht fristgerecht beantwortet, haftet der Auftragnehmer nicht und der Auftraggeber stellt den Auftragnehmer von Ansprüchen Dritter frei und ersetzt ihm etwaige Schäden und Aufwendungen. Dies gilt nicht, soweit die unterbliebene, fehlerhafte oder nicht fristgerechte Antwort des Auftraggebers an die betroffene Person auf einer unterlassenen, fehlerhaften oder verspäteten Information vom Auftragnehmer an den Auftraggeber beruht.

5.3 Der Auftraggeber ist für die Datenportabilität in Bezug auf die betroffene Person verantwortlich. Soweit erforderlich, unterstützt der Auftragnehmer den Auftraggeber bei der Erfüllung der Datenportabilität, indem er im Rahmen des Zumutbaren und Erforderlichen gegen Kostenerstattung Daten in einem gängigen maschinenlesbaren Format überlässt, sofern der Auftraggeber diese nicht anderweitig beschaffen kann.

6. Verantwortlichkeit des Auftraggebers

6.1 Der Auftraggeber ist dafür verantwortlich, alle datenschutzrechtlichen Voraussetzungen dafür herzustellen und nachzuweisen, dass die Verarbeitung der personenbezogenen Daten, die der Auftragnehmer gemäß dieser Vereinbarung und dem Auftrag gemäß Ziffer 1.1 vornimmt, zulässig ist. Dies umfasst insbesondere, aber nicht ausschließlich die Einholung und Aufrechterhaltung etwa erforderlicher Genehmigungen von Aufsichtsbehörden oder Einwilligungen betroffener Personen. Insbesondere hat der Auftraggeber sicherzustellen, dass seine Weisungen den Datenschutzgesetzen und dem Auftrag gemäß Ziffer 1.1 entsprechen. Er ist für die Rechtmäßigkeit der Verarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DS-GVO). Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er im Hinblick auf die Verarbeitung bezüglich datenschutzrechtlicher Bestimmungen Fehler oder Unregelmäßigkeiten feststellt.

6.2 Der Auftraggeber ist dafür verantwortlich, die zu verarbeitenden personenbezogenen Daten rechtzeitig und gemäß den vereinbarten Funktionalitäten in das ePension Arbeitgeber-Portal einzugeben. Der Auftraggeber trägt weiter die Verantwortung für die Richtigkeit, Qualität, Rechtmäßigkeit und Verlässlichkeit der Daten, die er in das ePension Arbeitgeber-Portal eingibt oder dem Auftragnehmer in sonstiger Weise überlässt.

Soweit Daten zu bAV-, bKV- und sonstigen betrieblichen Vorsorgeverträgen des Auftraggebers von Versicherern im ePension Arbeitgeber-Portal eingegeben werden, wird hiermit klargestellt: Die Versicherer übermitteln diese Daten ihrerseits auf Anweisung des Auftraggebers an das ePension Arbeitgeber-Portal; der Auftragnehmer nimmt diese Daten im Auftrag des Auftraggebers entgegen und verarbeitet sie ausschließlich zu dem Zweck des Auftrags gemäß Ziffer 1.1 und den Weisungen des Auftraggebers.

6.3 Der Auftraggeber ist zur Vertraulichkeit verpflichtet zu allen Geschäftsgeheimnissen des Auftragnehmers und der Unterauftragnehmer, die ihm anlässlich dieser Vereinbarung oder des Nutzungsvertrags gemäß Ziffer 1 (oben) zur Kenntnis gelangen. Hiervon sind insbesondere die Informationen und Unterlagen zu technischen und organisatorischen Maßnahmen des Auftragnehmers (Anlage 3.1) und seiner Unterauftragnehmer erfasst, ebenso wie alle Informationen und Unterlagen, die dem Auftraggeber anlässlich Ziffer 9 dieser Vereinbarung zur Kenntnis gelangen.

6.4 Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Absatz (2) DS-GVO genannten Angaben zur Verfügung zu stellen, soweit sie ihm nicht bereits vorliegen.

7. Verantwortungsbereich des Auftragnehmers; Informationen bei der Verletzung des Schutzes personenbezogener Daten

7.1 Der Auftragnehmer setzt folgende Maßnahmen um:

7.1.1 Sofern der Auftragnehmer gemäß den Vorgaben dieses Vertrags Unterauftragnehmer außerhalb der Europäischen Union einsetzt (siehe oben Ziffer 4), trägt er dafür Sorge, dass jeder Unterauftragnehmer einen Vertreter nach Art. 27 Absatz (1) DS-GVO benennt.

7.1.2 Zur Wahrung der Vertraulichkeit gemäß den Art. 28 Absatz (3) Satz 2 lit. b, 29, 32 Absatz (4) DS-GVO wird der Auftragnehmer bei der Durchführung der Arbeiten nur Beschäftigte einsetzen, die auf die Vertraulichkeit verpflichtet und mit den für sie relevanten Bestimmungen zum Datenschutz vertraut sind. 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.

7.1.3 Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen und erteilen einander die hierzu erforderlichen Auskünfte; Aufwendungen, die dabei beim Auftragnehmer entstehen, hat der Auftraggeber auf Nachweis zu erstatten.

Die Parteien informieren sich wechselseitig unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

7.1.4 Für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten des Auftraggebers gemäß Art. 30 Absatz (1) DS-GVO ist ausschließlich der Auftraggeber verantwortlich; der Auftragnehmer unterstützt ihn dabei auf Anforderung durch Bereitstellung von Informationen, soweit dies die Verarbeitung personenbezogener Daten nach dieser Vereinbarung betrifft und die Bereitstellung vom Auftrag gemäß Ziffer 1.1 erfasst ist. Daten, die im ePension-Arbeitgeber-Portal gemäß den dort vorhandenen Funktionalitäten eingegeben werden, sind vom Auftraggeber durch Nutzung der Portal-Funktionalitäten abzurufen.

7.2.1 Falls dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, informiert er den Auftraggeber unverzüglich. Dabei teilt der Auftragnehmer auch Kontaktdaten mit, unter denen sich der Auftraggeber nach zusätzlichen Informationen zur Verletzung erkundigen kann.

7.2.2 Der Auftragnehmer ist verpflichtet, mit dem Auftraggeber zusammenzuarbeiten, um sämtliche Informationen zu erheben, die erforderlich sind, um den bzw. die betroffenen Personen bzw. die zuständige Datenschutzbehörde korrekt und vollständig über die Verletzung zu informieren.

7.2.3 Nach der Meldung einer Verletzung personenbezogener Daten durch den Auftragnehmer an den Auftraggeber entscheidet der Auftraggeber in alleiniger Verantwortung, ob die Voraussetzungen für eine Meldung an Behörden bzw. betroffene Personen vorliegen und nimmt die Meldungen in alleiniger Verantwortung vor.

8. Unterauftragsverhältnisse

8.1 Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, Unterauftragnehmer einzusetzen.

Der Auftragnehmer ist dabei verpflichtet, den Unterauftragnehmer

a) unter Berücksichtigung seiner technischen und organisatorischen Maßnahmen zum Datenschutz sorgfältig auszuwählen und

b) durch schriftlichen oder elektronischen Vertrag zu beauftragen und

c) in Bezug auf den Unterauftrag mindestens in demselben Umfang zur Erfüllung datenschutzrechtlicher Anforderungen zu verpflichten, wie dies in dieser Vereinbarung für den Auftragnehmer gilt.

d) Sofern eine Einbeziehung von Unterauftragnehmern in Drittländern erfolgen soll, stellt der Auftragnehmer sicher, dass beim jeweiligen Unterauftragnehmer ein angemessenes Datenschutzniveau im Sinne der Art. 44 ff. DS-GVO gewährleistet ist, zum Beispiel durch Abschluss einer Vereinbarung gemäß den von der EU-Kommission genehmigten EU-Standardvertragsklauseln. Der Unterauftragnehmer muss einen Vertreter in der EU bestellt haben.

8.2 Die Parteien stellen fest, dass die Voraussetzungen gemäß Ziffer 8.1 für die Unterauftragsverhältnisse vorliegen, die zum Zeitpunkt des Abschlusses dieser Vereinbarung bereits bestehen.

Die netcom7 GmbH mit Sitz in Überlingen (Deutschland) erbringt Programmierleistungen für den Auftragnehmer.

Die Hetzner Online GmbH ist für den Betrieb des Rechenzentrums zuständig, in dem das ePension Arbeitgeber-Portal gehostet ist. Der Unterauftragnehmer Hetzner Online GmbH arbeitet seinerseits wiederum mit weiteren Unterauftragnehmern zusammen. Eine produktspezifische Liste der eingesetzten Subunternehmer am jeweiligen Standort ist abrufbar unter: https://www.hetzner.com/AV/subunternehmer.pdf.

Die is2 Intelligent Solution Services AG, Am Bäckeranger 2, 85417 Marzling, erbringt, soweit vom Auftraggeber beauftragt, Leistungen im Zusammenhang mit dem elektronischen Abschluss von Verträgen.

8.3 Bevor der Auftragnehmer an den erteilten Unteraufträgen Änderungen vornimmt in Bezug auf die Hinzuziehung oder Ersetzung weiterer Unterauftragnehmer, teilt er dies dem Auftraggeber mit.

Der Auftraggeber kann in Bezug auf den weiteren Unterauftragnehmer innerhalb einer Frist von einer Woche seit Erhalt der Information gegen die Beauftragung des Unterauftragnehmers Einspruch erheben. Der Einspruch bedarf der Textform und ist zu begründen, er kann nur aus wichtigem Grund erhoben werden.

Nach einem Einspruch des Auftraggebers ist der Auftragnehmer berechtigt, diese Vereinbarung sowie den Auftrag gemäß Ziffer 1.1 mit einer Kündigungsfrist von zwei Wochen zum Ende eines Kalendermonats zu kündigen.

8.4 Ein Unterauftragsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste.

9. Nachweismöglichkeiten; Inspektionen und behördliche Kontrollen

9.1 Der Auftragnehmer weist dem Auftraggeber auf dessen Anfrage die Einhaltung der in dieser Vereinbarung geregelten Pflichten mit geeigneten Mitteln nach, wobei dem Auftragnehmer das Wahlrecht zwischen mehreren geeigneten Mitteln zusteht. Geeignet sind zum Beispiel

- eine Darstellung der aktuell getroffenen technischen und organisatorischen Maßnahmen über die Punkte gemäß der Anlage zu Ziffer 3.1 dieser Vereinbarung,
- Selbstauskünfte oder Prozessbeschreibungen des Auftragnehmers,
- Nachweise zur Durchführung von Selbstaudits,
- unternehmensinterne Verhaltensregelungen einschließlich eines externen Nachweises über deren Einhaltung,
- Zertifikate oder Testate zum Datenschutz und/oder zur Informationssicherheit,
- genehmigte Verhaltensregelungen gemäß Art. 40 DS-GVO,
- Zertifikate gemäß Art. 42 DS-GVO.

9.2 Die Nachweise gemäß Ziffer 9.1 sollen nach Möglichkeit Inspektionen (Vor-Ort-Kontrollen) beim Auftragnehmer vermeiden. Wenn im Einzelfall dennoch eine Inspektion beim Auftragnehmer erforderlich sein sollte, wird diese auf Kosten des Auftraggebers durch einen unabhängigen externen Prüfer / eine unabhängige externe Prüferin durchgeführt, den / die der Auftragnehmer benennt. Der Auftragnehmer darf nur solche Prüfer/Prüferinnen benennen, die gegenüber dem Auftraggeber ihre Unabhängigkeit vom Auftragnehmer versichert und sich zur Verschwiegenheit verpflichtet haben. Die Prüfung wird rechtzeitig mit angemessener Vorbereitungsfrist (bis zu 90 Tagen) abgestimmt und findet während der üblichen Geschäftszeiten des Auftragnehmers statt. Sie darf den Betriebsablauf des Auftragnehmers nicht beeinträchtigen.

Inspektionen sind nicht zulässig, soweit die Einhaltung der Pflichten nach dieser Vereinbarung anstelle einer Inspektion auch durch Vorlage von Unterlagen gemäß Ziffer 9.1 nachgewiesen wird. Die Parteien vereinbaren, dass der Nachweis durch Vorlage eines gültigen Zertifikats nach dem Standard ISO 27001 in der Regel erbracht ist.

9.3 Der Auftragnehmer hat in jedem Fall das Recht, die Duldung von Kontrollen und die Erteilung von Informationen insoweit und dann zu verweigern, wenn die Kontrolle bzw. Informationserteilung ein Risiko darstellen würde für die Sicherheit der Datenverarbeitungsanlagen oder der darauf befindlichen Daten des Auftragnehmers oder Dritter (zum Beispiel anderer Auftraggeber des Auftragnehmers).

9.4 Der Auftraggeber trägt neben den Kosten des Prüfers/der Prüferin die Aufwendungen des Auftragnehmers, die diesem im Rahmen der Inspektion entstehen; dies gilt auch für etwaige Prüfungen, die eine Datenschutz- oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers beim Auftragnehmer vornimmt.

9.5 Die Überprüfungen bei Unterauftragnehmern nimmt ausschließlich der Auftragnehmer bzw. ein vom Auftraggeber und Auftragnehmer gemeinsam Beauftragter vor. Sie werden dem Auftraggeber auf dessen Anforderung nachgewiesen. Sofern die Überprüfung eines Unterauftragnehmers auf Anforderung des Auftraggebers erfolgt, trägt der Auftraggeber die damit verbundenen Kosten, auch, soweit sie beim Unterauftragnehmer entstehen. Die Prüfung findet höchstens einmal pro Kalenderjahr statt, wobei der Auftragnehmer den Zeitpunkt bestimmt.

10. Weisungsbefugnis des Auftraggebers

10.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach den Weisungen des Auftraggebers. Die Weisungen des Auftraggebers müssen sich im Rahmen der geltenden Datenschutzgesetze, dieser Vereinbarung und des Auftrags gemäß Ziffer 1.1 halten.

10.2 Grundsätzlich erteilt der Auftraggeber seine Weisungen, indem er die vertraglich vereinbarten Funktionalitäten des ePension Arbeitgeber-Portals zur elektronischen Verwaltung und Verarbeitung der vereinbarungsgegenständlichen Daten nutzt.

Einzelweisungen, die von den vereinbarten Funktionalitäten des ePension Arbeitgeber-Portals abweichen, bedürfen der vorherigen Zustimmung des Auftragnehmers.

10.3 Falls der Auftragnehmer durch eine gesetzliche Vorschrift zu einer bestimmten Verarbeitung verpflichtet ist, zu welcher es keine Weisung des Auftraggebers gibt, teilt er dies dem Auftraggeber mit, sofern das betreffende Gesetz die Mitteilung nicht verbietet.

10.4 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung könnte gegen Datenschutzvorschriften verstoßen. Die Parteien sind sich einig, dass der Auftragnehmer in diesem Zusammenhang auf die Richtigkeit und Vollständigkeit der Informationen des Auftraggebers angewiesen ist.

10.5 Der Auftraggeber ist dafür verantwortlich, die für ihn weisungsberechtigten Personen durch die Nutzung der hierfür vom Auftragnehmer bereitgestellten Funktionalitäten zu definieren.

11. Löschung und Rückgabe von personenbezogenen Daten; Vertraulichkeit auch nach Vertragsende

11.1 Im Falle einer Verpflichtung zur Datenlöschung gewährleistet der Aufragnehmer eine datenschutzgerechte Löschung der vertragsgegenständlichen personenbezogenen Daten nach dem Stand der Technik.

11.2 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.

11.3 Auf Wunsch des Auftraggebers stellt der Auftragnehmer ihm gegen eine im Einzelfall vereinbarte Aufwandsentschädigung auf einem Datenträger oder per Datenfernübertragung die für ihm im ePension Arbeitgeber-Portal gespeicherten Daten in einem gängigen Dateiformat zur Verfügung, die zum Zeitpunkt der Vertragsbeendigung in Bezug auf den Arbeitgeber und die ihm zugeordneten bAV-Daten gespeichert sind.

Im Übrigen löscht der Auftragnehmer die Daten nach Maßgabe der datenschutzrechtlichen Vorgaben.

11.4 Der Auftragnehmer ist befugt, Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

11.5 Der Auftragnehmer ist verpflichtet, während und auch über das Ende des Vertrags hinaus die Vertraulichkeit aller vertragsgegenständlichen Informationen, Unterlagen und elektronischen Daten zu gewährleisten, soweit diese nicht auftragsgemäß vernichtet oder an den Auftraggeber zurückgegeben sind.

12. Vergütung

Sofern die Maßnahmen des Auftragnehmers gemäß dieser Vereinbarung nicht ausdrücklich vom Auftrag gemäß Ziffer 1.1 und der dort geregelten Vergütung erfasst sind, sind sie zu den aktuell geltenden Preisen des Auftragnehmers gesondert zu vergüten.

13. Haftung

13.1 Für die Haftung des Auftragnehmers nach dieser Vereinbarung gelten die Regelungen der Nutzungsbedingungen ePension Arbeitgeber-Portal gemäß Ziffer 1.1 (oben). Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

13.2 Der Auftraggeber ist verpflichtet, den Auftragnehmer auch von allen Geldbußen, die gegen den Auftragnehmer verhängt werden, auf erstes Anfordern in dem Umfang freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße verhängten Verstoß trägt.

14. Wirksamwerden des Vertrags und Schlussbestimmungen

14.1 Die Vereinbarung wird wirksam, wenn beim Auftragnehmer die Erklärung des Auftraggebers zur Zustimmung schriftlich oder in einem elektronischen Format eingegangen ist. Der Auftraggeber verzichtet auf den Zugang der Annahmeerklärung des Auftragnehmers gemäß § 151 Satz 1 BGB, wobei der Auftraggeber nicht befugt ist, Änderungen vorzunehmen an dem Vereinbarungstext, den er vom Auftragnehmer erhalten hat.

14.2 Für diese Vereinbarung gilt deutsches Recht.

14.3 Änderungen und Ergänzungen dieses Vertrags bedürfen der Schrift- oder der Textform. Dies gilt auch für die Aufhebung des Formerfordernisses.

14.4 Für etwaige Streitigkeiten zwischen den Parteien ist das Landgericht Hamburg zuständig.

V 21-08-001

Anlage 3.1

Vereinbarung zur Auftragsverarbeitung ePension Arbeitgeber-Portal

Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

A) Maßnahmen der ePension KG

Die ePension KG nimmt folgende technische und organisatorische Maßnahmen vor:

1.1 Vertraulichkeit (Artikel 32 Abs. 1 lit. b DSGVO)

1.1.1 Zutrittskontrolle

Die Zutrittskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Die Geschäftsräume der ePension GmbH & Co. KG sind verschlossen und können nur nach Maßgabe des Zutrittskontrollsystems geöffnet werden.
- Es wird ein dem Schutzbedarf der Daten angemessenes Schließsystem verwendet (Schlüssel, Codekarten).
- Es ist eine verantwortliche Person für die Verwaltung der Zutrittsmittel bestimmt.
- Eine Dokumentation der Zutrittsmittel wird geführt und laufend aktualisiert.
- Es gibt einen zentralen Besucherempfang. Die Büros sind nur darüber zu erreichen.
- Besucher halten sich ausschließlich in Begleitung eines Mitarbeiters in den Geschäftsräumen auf.
- Die Zutrittskontrolle zu den Serverräumen wird durch die räumliche Struktur des jeweiligen Rechenzentrums und die dort durch den Betreiber eingesetzten Kontrollsysteme gewährleistet.

1.1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Reduktion der zugriffsberechtigten Personen auf ein Minimum.
- Clientsysteme sind nur nach passwortgestützter Netzwerk-Authentifizierung nutzbar.
- Verbindliches Verfahren zur Vergabe von Berechtigungen.
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern.
- Eine Passwortrichtlinie mit ausreichendem Schutzstandard ist implementiert.
- Jeder Berechtigte verfügt über ein eigenes, nur ihm bekanntes Passwort, welches nicht weitergegeben werden darf. Bei eventuellem Bekanntwerden des Passwortes muss dieses umgehend geändert werden.
- Einsatz von Firewalls.

- Automatische Bildschirmsperren bei Verlassen des Arbeitsplatzes (passwortgeschützt).

1.1.3 Zugriffskontrolle

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

- Das unbefugte Lesen, Kopieren, Verändern und Löschen von Datenträgern wird verhindert durch
  - Datenträgerverwaltung-/Management,
  - Benennung eines Verantwortlichen für die Datenträger,
  - Softwareseitigen Ausschluss (Berechtigungskonzept)
  - Weitere Kontrollmechanismen des Rechenzentrums.
- Die Einschränkung der Zugriffsmöglichkeiten des zur Benutzung eines DV-Systems Berechtigten ausschließlich auf die seiner Zugriffsberechtigung unterliegenden Daten wird gewährleistet durch
  - automatische Prüfung der Zugriffsberechtigung mittels Passwort,
  - ausschließliche Menüsteuerung je nach Berechtigung,
  - differenzierte Zugriffsberechtigung auf Anwendungsprogramme,
  - differenzierte Verarbeitungsmöglichkeiten (Lesen/Ändern/Löschen) Führung eines Administrationskonzeptes,
  - Einsatz von Firewalls,
  - dem Schutzbedarf entsprechende Entsorgung und Vernichtung von Dokumenten und Datenträgern.

1.1.4 Trennungsgebot

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

- Personenbezogene Daten dürfen nur für den Zweck genutzt werden, für den sie ursprünglich erhoben wurden. Die unterschiedliche und getrennte Verarbeitung wird gewährleistet durch
  - Softwareseitigen Ausschluss (Mandantentrennung)
  - Das Datenbankprinzip, Trennung über Zugriffsregelung
  - Trennung von Test- und Produktivdaten
  - Trennung von Entwicklungs- und Produktionsprogrammen

1.2 Integrität (Artikel 32 Abs. 1 lit. b DSGVO)

1.2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Ein physischer Versand von Datenträgern ist nicht vorgesehen.
- Private Datenträger dürfen im Unternehmen nicht eingesetzt werden.
- Nicht mehr benötigte magnetische Datenträger werden durch mehrfaches Überschreiben gelöscht.
- Zugriff auf personenbezogene Daten nur über authentifizierte, verschlüsselte Verbindungen.
- Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten bei der Übertragung wird verhindert durch
  - SSL - Verschlüsselung der Datenübertragung,
  - Vollständigkeitsüberprüfung soweit relevant,
  - Aufbau einer Transportverbindung nur zwischen definierten und durch Zertifikate gesicherten Systemen.
- Die Weitergabe personenbezogener Daten erfolgt durch Dienste und Transportverfahren, die dem gewünschten Zweck und dem aktuellen Stand der Sicherheitstechnik äquivalent oder besser entsprechen.

1.2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Ob und von wem Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind, kann nachträglich überprüft und festgestellt werden durch
  - Benutzeridentifikation,
  - Protokollierung eingegebener Daten (Verarbeitungsprotokoll).

1.3 Verfügbarkeit und Belastbarkeit (Artikel 32 Abs. 1 lit. b und c DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

- Dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind, wird gewährleistet durch
  - Einsatz von RAID-Festplattensystemen,
  - Einsatz von USV und Notstromaggregat (an Serverstandorten, gegebenenfalls durch Unterauftragnehmer, siehe unten letzter Bullet-Point),
  - Feuer- und Rauchmeldeanlagen,
  - Feuerlöscheinrichtungen,
  - Einsatz einer Klimaanlage mit Raumtemperaturüberwachung an Serverstandorten (gegebenenfalls durch Unterauftragnehmer),
  - mehrfache inkrementelle Datenbank- und Systembackups,
  - Backups nach einem Zeitplan, der die Veränderungen der Daten durch Nutzung angemessen reflektiert,
  - Konzept zur Rekonstruktion der Datenbestände,
  - zusätzliche Maßnahmen durch die Unterauftragnehmer (Rechenzentrum).

1.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 25 Abs. 1 DSGVO; Art. 32 Abs. 1 lit. d DSGVO)

1.4.1 Datenschutz-Management

Die ePension GmbH & Co. KG wird von der Deutschen Datenschutzkanzlei (externer Datenschutzbeauftragter: Stefan Fischerkeller) betreut. Die Deutsche Datenschutzkanzlei nutzt ein eigens erstelltes Datenschutzmanagementsystem (DSMS), in dem alle Maßnahmen, Verfahren, Tätigkeiten etc. im Bereich Datenschutz abgebildet werden. Das DSMS beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen und beinhaltet darüber hinaus einen Maßnahmenplan zur rechtskonformen Umsetzung der EU-Datenschutzgrundverordnung (Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO).

1.4.2 Incident-Response-Management

Den Mitarbeitern ist bekannt, dass Sicherheitsvorfälle unverzüglich an den Datenschutzkoordinator zu melden sind. Dieser stimmt sich in diesem Fall mit dem Datenschutzbeauftragten und der Geschäftsführung ab. Erklärungen, Hinweise und Vorgaben sind darüber hinaus im Anwenderhandbuch implementiert.

1.4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftszwecke zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung- und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden. Bei der Datenverarbeitung handelt die ePension GmbH & Co. KG bzw. deren Dienstleister nach Kundenvorgabe und den gesetzlichen Vorschriften.

1.4.4 Auftragskontrolle

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

- Alle bei der Datenverarbeitung eingesetzten Mitarbeiter sind schriftlich auf das Datengeheimnis und zur Wahrung der Vertraulichkeit verpflichtet.
- Detaillierte Angaben über Zweck, Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers nach Vorgabe Art. 28 DS-GVO.
- Der Dienstleister hat einen externen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.
- Eine regelmäßige Prüfung der beauftragten Unternehmen wird durch den eigenen Datenschutzbeauftragten, bzw. die interne IT-Administration bzw. den IT-Sicherheitsbeauftragten vorgenommen und dokumentiert.
- Mündliche Aufträge müssen schriftlich bestätigt und dokumentiert werden.
- Vergabe von Einzelaufträgen nur über namentlich benannte Ansprechpartner.

1.5 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

Entsprechende Verschlüsselungssysteme für Datenträger und mobile Endgeräte sind implementiert. Verschlüsselungstechnologien bei der Übermittlung von Daten kommen ebenfalls zum Einsatz. Eine Richtlinie zum Umgang mit (mobilen) Datenträgern kommt zur Anwendung. Auch restriktive Zugriffsrechte beim Zugriff auf Server/Testdatenbanken/ Entwicklungssystem etc. werden angewandt.

1.6 Kooperation mit der Deutschen Datenschutzkanzlei

Zur Einhaltung der datenschutzrechtlichen Vorgaben nach der EU-Datenschutzgrundverordnung (DS-GVO), arbeitet ePension GmbH & Co. KG mit der Deutschen Datenschutzkanzlei zusammen. Neben der Erstellung von Richtlinien und Handlungshilfen, berät die Deutsche Datenschutzkanzlei ePension GmbH & Co. KG in allen Fragen rund um den Datenschutz und stellt mit Herrn Stefan Fischerkeller den externen Datenschutzbeauftragten nach Art. 37 DSGVO des Unternehmens.

Ansprechpartner der Deutschen Datenschutzkanzlei ist:
Stefan Fischerkeller
Diplomverwaltungswirt (FH), geprüfter fachkundiger Datenschutzbeauftragter (DESAG)

Deutsche Datenschutzkanzlei
Standort Tettnang
Dr.-Klein-Str. 29, 88069 Tettnang www.deutsche-datenschutzkanzlei.de

Kontakt Stefan Fischerkeller:
E-Mail: fischerkeller@ddsk.de
Tel. 07542 / 949 21 01

B) Maßnahmen des Unterauftragnehmers Hetzner Online GmbH

Der Unterauftragnehmer Hetzner Online GmbH verfügt über folgende technische und organisatorische Maßnahmen:

I. Vertraulichkeit

- Zutrittskontrolle,
  - Datacenter-Parks in Nürnberg und Falkenstein,
    - elektronisches Zutrittskontrollsystem mit Protokollierung,
    - Hochsicherheitszaun um den gesamten Datacenter-Park,
    - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation- Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack),
    - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude,
    - 24/7 personelle Besetzung der Rechenzentren,
    - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen,
    - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
- Verwaltung,
  - elektronisches Zutrittskontrollsystem mit Protokollierung,
  - Videoüberwachung an den Ein- und Ausgängen,
- Zugangskontrolle,
  - bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server",
    - Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind,
    - Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem Auftraggeber dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.
  - bei Hauptauftrag "Managed Server", "Webhosting", "Storage Box",

    - Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter vom Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert

- Zugriffskontrolle,
    - bei internen Verwaltungssystemen des Auftragnehmers.
        - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
        - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
- bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server",
    - Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.
- bei Hauptauftrag "Managed Server", "Webhosting", "Storage Box",
    - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
    - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers,
    - Für übertragene Daten/Software ist einzig der Auftraggeber in Bezug auf Sicherheit und Updates zuständig.
- Datenträgerkontrolle
    - Datacenter-Parks in Nürnberg und Falkenstein
        - Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
        - Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum (Falkenstein) zerstört (geschreddert).
- Trennungskontrolle
    - bei internen Verwaltungssystemen des Auftragnehmers
        - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
        - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
    - bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"

- Die Trennungskontrolle obliegt dem Auftraggeber.

- bei Hauptauftrag "Managed Server", "Webhosting", "Storage Box"
  - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
  - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

- Pseudonymisierung
  - Für die Pseudonymisierung ist der Auftraggeber verantwortlich

II. Integrität (Art. 32 Abs. 1 lit. b) DS-GVO)

- Weitergabekontrolle
  - Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
  - Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
  - Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.

- Eingabekontrolle
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
    - Änderungen der Daten werden protokolliert.
  - bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"
    - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
  - bei Hauptauftrag "Managed Server", "Webhosting", "Storage Box"
    - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
    - Änderungen der Daten werden protokolliert.

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DS-GVO)

- Verfügbarkeitskontrolle
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
    - Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
    - Einsatz von Festplattenspiegelung bei allen relevanten Servern.

- Monitoring aller relevanten Server.
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Dauerhaft aktiver DDoS-Schutz.

- bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"
  - Datensicherung obliegt dem Auftraggeber.
  - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
  - Dauerhaft aktiver DDoS-Schutz.
- bei Hauptauftrag "Managed Server", "Webhosting", "Storage Box"
  - Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
  - Einsatz von Festplattenspiegelung.
  - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
  - Einsatz von Softwarefirewall und Portreglementierungen.
  - Dauerhaft aktiver DDoS-Schutz.
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DS-GVO);
  - Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Das Datenschutz-Managementsystem und das Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.
- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).

- Auftragskontrolle
  - Die Mitarbeiter der Hetzner Online GmbH werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers.

- Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.