Auftragsverarbeitungsvereinbarung zur Nutzung von meinMVP

Zwischen

_____
Name

_____
Straße/Hausnummer

_____
Postleitzahl/Ort

(im Folgenden „Auftraggeber“) und der digital broking GmbH, Constantinstraße 90, 30177 Hannover, (im Folgenden „Auftragnehmer“) wurde eine Vereinbarung über die Nutzung der Plattform „meinMVP“ geschlossen. Der Auftraggeber beabsichtigt, auf Grundlage der Nutzungsvereinbarung mit Hilfe von meinMVP Kunden- und Versicherungsvertragsdaten elektronisch zu verwalten. Die Speicherung, Verarbeitung und Nutzung der betreffenden Daten wird dabei auf Computersystemen des Auftraggebers erfolgen. Vor diesem Hintergrund vereinbaren die Parteien die Geltung folgender Regelungen zur Auftragsverarbeitung:

1. Gegenstand des Auftrags, Begriffsbestimmungen

1.1. Der Gegenstand des Auftrags ergibt sich aus Ziffer 3 der Allgemeinen Nutzungsbedingungen für die Online-Plattform meinMVP, auf denen Grundlage die Parteien die Nutzungsvereinbarung geschlossen haben.

1.2. „Nutzungsvereinbarung“ im Sinne dieser Auftragsverarbeitungsvereinbarung ist die zwischen den Parteien auf Grundlage der Allgemeinen Nutzungsbedingungen für die Online-Plattform meinMVP geschlossene Vereinbarung über die Nutzung der Online-Plattform meinMVP.

1.3. „Allgemeine Nutzungsbedingungen“ im Sinne dieser Auftragsverarbeitungsvereinbarung sind die Allgemeinen Nutzungsbedingungen für die Online-Plattform meinMVP des Auftragnehmers.

1.4. „Auftraggeber“ im Sinne dieser Auftragsverarbeitungsvereinbarung ist der „Nutzer“ der Plattform meinMVP im Sinne der Allgemeinen Nutzungsbedingungen.

1.5. „Auftragnehmer“ im Sinne dieser Auftragsverarbeitungsvereinbarung ist der in den Allgemeinen Nutzungsbedingungen als „digital broking“ bezeichnete Vertragspartner.

1.6. Sofern in dieser Vereinbarung nicht anders angegeben, gelten die in den Allgemeinen Nutzungsbedingungen vorgesehenen Begriffsbestimmungen auch für diese Auftragsverarbeitungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

2.1. Zweck der Erhebung, Verarbeitung und/oder Nutzung der personenbezogenen Daten ist die Verwaltung von Kunden- und Vertragsdaten im Rahmen der Plattform meinMVP im Auftrag des Auftraggebers. Der genaue Umfang der Verarbeitung wird durch die konkrete Nutzung des Auftraggebers bestimmt.

2.2. Inhalt des Auftrags ist zudem die freiwillige Inanspruchnahme von Support-Leistungen (insbesondere in Form von Fernwartungs-Leistungen) durch den Auftraggeber nach Ziffer 8 der Allgemeinen Nutzungsbedingungen und Ziffer 9 der Nutzungsvereinbarung.

2.3. Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenarten bzw. -kategorien:

- Versicherungsvertragsdaten (z. B. GDV-Daten, Vertragsbeziehung, Produkt- bzw. Vertragsinteresse, Gesundheitsdaten),
- Personenstammdaten (z. B. Name, Adresse, Geburtsdatum) und weitere Kommunikationsdaten (z. B. Telefonnummer, Telefaxnummer, E-Mail-Adresse, IP-Adresse),
- Abrechnungs- und Zahlungsdaten zu Versicherungsverträgen und Vermittlungsverträgen (z. B. Rechnungen, Bankverbindung).

2.4. Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst:

- Kunden des Auftraggebers (Versicherungsnehmer),
- potentielle Kunden des Auftraggebers,
- sonstige im Zusammenhang mit der Kunden-, Vertrags- und Schadenverwaltung des Auftraggebers betroffene Personen,
- den Auftraggeber selbst, soweit es sich um eine natürliche Person handelt,
- Mitarbeiter und sonstige Beschäftigte des Auftraggebers.

2.5. Die Verarbeitung und Nutzung der Daten findet ausschließlich auf Systemen des Auftragnehmers im Gebiet der Bundesrepublik Deutschland oder in einem Mitgliedsstaat der Europäischen Union statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

3. Technisch-organisatorische Maßnahmen

3.1. Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen

Datensicherheitsmaßnahmen. Die in der Anlage beschriebenen technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt.

3.2. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses entsprechend der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.

3.3. Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den vereinbarten Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt er den Auftraggeber unverzüglich.

4. Weisungsrecht des Auftraggebers

4.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und entsprechend den dokumentierten Weisungen des Auftraggebers.

4.2. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate 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.

4.3. Von den vorstehenden Ziffern 4.1 und 4.2 ausgenommen ist die Verarbeitung von Daten durch den Auftragnehmer, um eine Pflicht aus dem Recht der Union oder der Mitgliedstaaten im Sinne des § 28 Abs. 3 a) DSGVO, dem der Auftragnehmer unterliegt, zu erfüllen. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit. Eine Mitteilung erfolgt nicht, wenn das betreffende Recht diese wegen eines wichtigen öffentlichen Interesses verbietet.

4.4. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung des Auftraggebers verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

4.5. Die Ausübung des Weisungsrechts erfolgt durch Benutzung und Einrichtung des Services meinMVP durch den Auftraggeber oder durch grundsätzlich schriftlich zu erteilende Einzelweisungen. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

5. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat personenbezogene Daten zu berichtigen, zu löschen und zu sperren, wenn der Auftraggeber dies in einer Weisung verlangt, sofern der Auftraggeber dies nicht mit Hilfe die Funktionen der Plattform selbst umsetzen kann.

6. Pflichten des Auftragnehmers

6.1. Der Auftragnehmer hat darüber hinaus folgende Pflichten:

- Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Aufgaben gemäß Art. 39 DSGVO erfüllen kann, und Bekanntgabe der Person des Datenschutzbeauftragten auf Anforderung des Auftraggebers.
- Die Gewährleistung der Vertraulichkeit gemäß Art. 28 Abs. 3 b) DSGVO. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.
- Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) vorlegen.

6.2. Der Auftragnehmer unterstützt den Auftraggeber angemessen mit geeigneten technischen und organisatorischen Maßnahmen dabei, dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in den Artikeln 12 bis 23 DSGVO genannten Rechte der betroffenen Person nachzukommen.

6.3. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen dabei, die in den Artikeln 32 bis 36 genannten Pflichten zu erfüllen.

6.4. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

6.5. An der Erstellung der Verfahrensverzeichnisse bzw. des Verarbeitungsverzeichnisses des Auftraggebers im Sinne des Art. 30 Abs. 1 DSGVO hat der Auftragnehmer mitzuwirken. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten. Der Auftragnehmer führt sein Verarbeitungsverzeichnis gem. Art. 30 Abs. 2 DSGVO. Der Auftraggeber hat ein Einsichtsrecht.

7. Unterauftragsverhältnisse

7.1. Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

- Die Einschaltung von Unterauftragnehmern ist grundsätzlich gestattet. Der Auftragnehmer kann zur Vertragsdurchführung unter Wahrung seiner unter Ziffer 6 dieses Vertrages erläuterten Pflicht zur Auftragskontrolle Unterauftragnehmer einsetzen, wenn er dem Auftraggeber die beabsichtige Hinzuziehung oder Ersetzung eines Unterauftragnehmers binnen angemessener Frist vor Beginn der Verarbeitung oder Nutzung mitteilt. Erhebt der Auftraggeber Einspruch gegen die beabsichtigte Änderung, erfolgt sie nicht (Art. 28 Abs. 2 Satz 2 DSGVO).
- Der Auftragnehmer versichert, dass er Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat.
- Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Unterauftragnehmern entsprechend gelten. Dabei muss der Unterauftragnehmer insbesondere hinreichende Garantien dafür bieten, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Zudem vereinbart der Auftragnehmer mit dem Unterauftragnehmer, und dieser rekursiv mit weiteren Unterauftragnehmern, dass jeder Unterauftragnehmer dem Auftraggeber für die Verletzung von Datenschutzrecht unmittelbar haftet. Der Auftragnehmer hat die Einhaltung der Pflichten regelmäßig zu überprüfen. Das Ergebnis ist entsprechend zu dokumentieren.

7.2. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

7.3. Zurzeit sind folgende mit Namen, Anschrift und Auftragsinhalt bezeichneten Unterauftragnehmer mit der Verarbeitung von personenbezogenen Daten in dem wie folgt genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden:

Name, Anschrift	Auftragsinhalt
adesso AG, Stockholmer Allee 20, 44269 Dortmund	Betrieb, Entwicklung
TREND Services GmbH, In der Fleute 100, 2389 Wuppertal	Service Desk, First Level Support
adesso as a service GmbH Stockholmer Allee 24 44269 Dortmund	Betrieb, Second Level Support
VHV Holding AG, VHV-Platz 1, 30177 Hannover	Betrieb, First und Second Level Support
VHV Vereinigte Hannoversche Versicherung a.G., VHV-Platz 1, 30177 Hannover	Betrieb, First und Second Level Support
VHV Allgemeine Versicherung AG, VHV-Platz 1, 30177 Hannover	Betrieb, First und Second Level Support
VHV Solutions GmbH, VHV-Platz 1, 30177 Hannover	Betrieb, First und Second Level Support
conventic GmbH, Burgstraße 79, 53177 Bonn – Bad Godesberg	Betrieb, Infrastruktur
FINCON Unternehmensberatung GmbH, Dorotheenstr. 64, 22301 Hamburg	Infrastruktur , Entwicklung
Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn	Hosting, e-mail Service
T-Systems International GmbH, Hahnstraße 43 d, 60528 Frankfurt am Main	Subunternehmen, Anbieter der Cloud
Deutsche Telekom Regional Services and Solutions GmbH, Friedrich-Ebert-Allee 71, 53113 Bonn	First Level Support
IT Services Hungary, Neumann Janos u 1/C, H-1117 Budapest	Betrieb, First und Second Level Support
STRATO AG Deutschland, Pascalstraße 10, 10587 Berlin	Service Desk
Axivas Deutschland GmbH, Carl-Benz-Straße 9-11, 68723 Schwetzingen	Service Desk

8. Überprüfungen, Inspektionen

8.1. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO oder dieser Vereinbarung niedergelegten Pflichten zur Verfügung. Er weist dem Auftraggeber insbesondere auf Anfrage die Umsetzung der nach dieser Vereinbarung festgelegten technischen und organisatorischen Maßnahmen nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-

Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) erbracht werden.

8.2. Der Auftragnehmer ermöglicht Überprüfungen – einschließlich Inspektionen – im Sinne des Art. 28 Abs. 3 h) DSGVO, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt hierzu angemessen bei.

9. Mitteilung bei Verstößen des Auftragnehmers

9.1. Der Auftragnehmer erstattet dem Auftraggeber in allen Fällen Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Störungen oder Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

9.2. Es ist bekannt, dass nach Art. 33 und Art. 34 DSGVO Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach Art. 33 und Art. 34 DSGVO treffen, hat der Auftragnehmer ihn bei der Erfüllung angemessen zu unterstützen, insbesondere indem er ihm, soweit möglich, unverzüglich die Informationen gem. Art. 33 Abs. 3 DSGVO, im Falle des Art. 34 DSGVO zusätzlich die Informationen gem. Art. 34 Abs. 2 DSGVO zur Verfügung stellt.

10. Pflichten des Auftraggebers

10.1. Der Auftraggeber ist gemäß Art. 4 Nr. 7 DSGVO Verantwortlicher im datenschutzrechtlichen Sinne für die bei dem Auftragnehmer vertragsgemäß verarbeiteten personenbezogenen Daten.

10.2. Der Auftraggeber ist bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für ihn einschlägigen Datenschutzgesetze verantwortlich.

10.3. Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z. B. durch Einholung von Einwilligungserklärungen) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtverletzungsfrei erbringen kann.

10.4. Der Auftraggeber hat den Auftragnehmer über entdeckte Fehler oder Unregelmäßigkeiten bei Datenverarbeitungsvorgängen unverzüglich in Textform zu informieren.

11. Laufzeit

11.1. Die Dauer des Auftrages entspricht der Dauer der Nutzungsvereinbarung.

11.2. Die Möglichkeit zur fristlosen Kündigung bleibt unberührt. Ein Grund zur fristlosen Kündigung liegt insbesondere vor, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieser Auftragsverarbeitungsvereinbarung vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers vertragswidrig verweigert.

12. Löschung von Daten nach Ende der Vereinbarung

12.1. Nach Beendigung des Auftrages werden die personenbezogenen Daten auf Weisung des Auftraggebers gelöscht. Der Auftragnehmer ist grundsätzlich auch ohne gesonderte Zustimmung des Auftraggebers berechtigt, nach Beendigung der Nutzungsvereinbarung die Daten des Auftraggebers zu löschen.

12.2. Eine Pflicht des Auftragnehmers zur Löschung von Daten besteht nicht, sofern nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten im Sinne des Art. 28 Abs. 3 g) DSGVO besteht.

13. Haftung

Die Haftungsregelungen aus der Nutzungsvereinbarung gelten auch für diese Vereinbarung zur Auftragsdatenverarbeitung, soweit nicht eine Haftungsbeschränkung nach Maßgabe der jeweils einschlägigen geltenden rechtlichen Bestimmungen zugunsten des Auftragnehmers greift.

14. Sonstiges

14.1. Verweise auf die Datenschutzgrundverordnung (DSGVO) sind bis zum 24.05.2018 als Verweise auf die entsprechende Regelung im Bundesdatenschutzgesetz (BDSG) auszulegen. Sofern es keine entsprechende Regelung im BDSG gibt, entfällt die genannte Verpflichtung bis zum 24.05.2018 und findet erst mit Wirkung ab dem 25.05.2018 Anwendung.

14.2. Ist der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit dieser Auftragsverarbeitungsvereinbarung Hannover.

14.3. Es gilt das Recht der Bundesrepublik Deutschland.

14.4. Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten wird ausgeschlossen.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Auftraggeber	digital broking GmbH

Technische und organisatorische Datenschutzmaßnahmen der digital broking GmbH für die Plattform „meinMVP“

Stand: 27. April 2018

A. Organisation

Die technischen und organisatorischen Datenschutzmaßnahmen entsprechen den Anforderungen gemäß Art. 32 DSGVO bzw. § 64 Abs. 3 BDSG (neu).

Die innerbetriebliche Organisation der digital broking GmbH und der durch sie beauftragten Dritten, ist durch Maßnahmen so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Zu diesen Maßnahmen zählen:

- schriftliche Arbeitsanweisungen, Richtlinien, Merkblätter;
- Programme/Verfahren sind ordnungsgemäß dokumentiert;
- Aufbewahrung und Zugriffsmöglichkeit maschinell erzeugter Protokolle/Logs ist geregelt;
- Programmfreigabeverfahren ist eingerichtet;
- Benachrichtigungen, Auskunftsersuchen, Anliegen bzgl. Berichtigung, Löschung oder Sperrung werden dokumentiert.

B. Sicherungsmaßnahmen

Die Datensicherung (Backup) wird bei der digital broking GmbH betrieben und gewartet. Die Server für das Online-System und Datenbanken sind bei T-Systems International GmbH als Cloud Service gehostet.

Die Unterbeauftragten werden sorgfältig ausgewählt und hinsichtlich ihres Sicherheitsbewusstseins und ihrer Fachkompetenz überprüft.

Einige diesen Bereich betreffenden Sicherungsmaßnahmen sind an dieser Stelle nicht gesondert ausgewiesen, da sie in die Verantwortung der Unterbeauftragten fallen oder aus Gründen der Aufrechterhaltung der Sicherheit durch Vertraulichkeit nicht detailliert veröffentlicht werden.

1. Zugangskontrolle:

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte.

Die Verwehrung des Zugangs zur Verarbeitungsanlagen für Unbefugte wird durch folgende Maßnahmen gewährleistet:

1.1 Die Zugangskontrolle zu den Serverräumen wird durch die räumliche Struktur des Rechenzentrums und die eingesetzten Kontrollsysteme gewährleistet.

Der Cloud Anbieter T-Systems International GmbH ist ISO 27001 zertifiziert und erfüllt die Sicherheitsvorgaben an Zutrittskontrolle (Siehe Zertifikats-Registrier-Nr.: DS-1215044).
Der zertifizierte Bereich ist: Bereitstellung von Informationstechnologie-, Telekommunikations- und Cloud-Lösungen für eine vernetzte Geschäftswelt und Gesellschaft für interne und externe Kunden einschließlich Servicemanagement und Bereitstellung von dynamischen Applikations-Services & Infrastrukturen, Rechenzentrums-Services, Softwareentwicklung, ICT Security, Projektmanagement, Produktmanagement und Beratungsdienstleistungen

1.2 Zudem ist T-Systems International GmbH als „Trusted Cloud-Datenschutzprofil für Cloud-Dienste“ zur Erfüllung der Datenschutzanforderungen für die Auftragsdatenverarbeitung gemäß dem TCDP, Version 1.0, Schutzklasse III Wiederherstellbarkeitsniveau sehr hoch zertifiziert.

Prüfgegenstand ist der Dienst Open Telekom Cloud (OTC) v2.0 ein Infrastructure-as-a-Service-Angebot auf der Basis von OpenStack. Einzelne Komponenten zur Rechenleistung, Speicher, Netzwerk & Sicherheitskomponenten sind in einer einheitlichen Managementoberfläche abrufbar. Der Dienst wird ausschließlich in Rechenzentren an deutschen Standorten bereitgestellt. (Siehe Zertifikats-Registrier-Nr.: DS-0817020-1)

1.3 Die Zugangskontrolle zu den Arbeitsräumen der digital broking GmbH ist durch eine personifizierte Zutrittskarte gewährleistet. Die Vergabe der Zutrittskarte erfolgt nach einem Vergabe- und Genehmigungsprozess.

2. Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.

Das unbefugte Lesen, Kopieren, Verändern Löschen von Datenträgern wird durch folgende Maßnahmen gewährleistet:

2.1 Die Nutzung von externen Speichern zur Verwaltung von personenbezogenen Daten ist Mitarbeitern der digital broking GmbH nicht gestattet.

2.2 Der Cloud-Anbieter T-Systems International GmbH ist ISO 27001 zertifiziert und erfüllt die Sicherheitsvorgaben an Datenträgerkontrolle. Er hat im Rahmen der Etablierung des Standards ISO 27001 gemäß Anhang „A.8.3 Umgang mit Medien“ Maßnahmen zur Verwaltung, Entsorgung und physische Weitergabe von Wechselmedien umgesetzt.

3. Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

Die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten wird verhindert durch:

3.1 Registrierungsprozess inkl. Prüfung der Nutzer-Identität.

3.2 Individuelle Nutzer-Kennung und Passwort-Vergabe. 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.

3.3 Passwort-Sicherheit und -Komplexität.

3.4 Erforderliche Nutzung eines zweiten Faktors zur Authentifizierung.

3.5 Protokollierung bzw. Auswertung der Logdateien.

3.6 Mandantenfähigkeit der Plattform.

3.7 Für administrative Tätigkeiten wurde ein Berechtigungskonzept nach dem Minimum-Prinzip etabliert.

4. Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

Die Benutzerkontrolle ist durch folgende Maßnahmen umgesetzt:

4.1 Registrierungsprozess inkl. Prüfung der Nutzer-Identität.

4.2 Individuelle Nutzer-Kennung und Passwort-Vergabe. 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

4.3 Erforderliche Nutzung eines zweiten Faktors zur Authentifizierung.

4.4 Unbefugte Nutzer werden durch das System automatisch abgewiesen.

4.5 Berechtigungskonzept inkl. Prozess zur Vergaben der Berechtigungen administrativer Tätigkeiten.

4.6 Einsatz von Verschlüsselungsverfahren mit Stand der Technik (z.B. SSH, TLS 1.2, AES128, AES256, SHA2, etc.).

4.7 Einsatz vom Nutzerverwaltungssystem sowohl für administrative Benutzerkonten als auch für die Nutzer der Plattform meinMVP (LDAP und Key Cloak).

5. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

Die Zugriffskontrolle wird durch folgende Maßnahmen gewährleistet:

5.1 Das unbefugte Lesen, Kopieren, Verändern oder Löschen von Produktivdaten wird verhindert durch:

- Softwareseitigen Ausschluss (Berechtigungskonzept).
- Softwareseitige Überwachung nichtplausibler Nutzung (Monitoring).
- Gesicherte Schnittstellen.
- Weitere Kontrollmechanismen des Rechenzentrums.

5.2 Die Einschränkung der Zugriffsmöglichkeit des zur Benutzung eines DV-Systems Berechtigten ausschließlich auf die seiner Zugriffsberechtigung unterliegenden Daten wird gewährleistet durch:

- Automatische Prüfung der Zugriffsberechtigung mittels Passwort.
- Erforderliche Nutzung eines zweiten Faktors zur Authentifizierung.
- Ausschließliche Menüsteuerung je nach Berechtigung.
- Mandantenfähigkeit der Plattform.
- Differenzierte Zugriffsberechtigung auf Anwendungsprogramme.
- Differenzierte Verarbeitungsmöglichkeiten (Lesen/Ändern/Löschen).

5.3 Es wurden Maßnahmen getroffen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass gespeicherte oder in Verarbeitung befindliche Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Dokumentierter, technisch unterstütztes On-/Off-Boarding, Changeprozess-Workflow.
- Zugriff durch personalisierte Accounts auf Basis eines Berechtigungskonzepts.
- Zugriffe werden protokolliert.

6. 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

Die Übertragungskontrolle ist durch folgende Maßnahmen gewährleistet:

6.1 Die Übertragung von personenbezogenen an Dritte ist im Datenschutzkonzept (im Confluence) detailliert beschrieben.

6.2 Es werden nur Daten an berechtigte Empfänger zur Erfüllung der Aufgabe elektronisch übermittelt.

6.3 Die Übertragung der Daten wird protokolliert.

6.4 Die Daten werden mit Stand der Technik verschlüsselt übertragen. Unbefugte Personen haben keine Möglichkeit die Daten zu lesen oder zu verändern.

6.5 Automatischer Rückruf des Servers auf bekannte IP des Nutzers.

6.6 Überprüfung bekannter öffentlicher Schlüssel bei Kontaktaufnahme.

6.7 Protokollierung der Systemnutzung und Protokollauswertung.

7. 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.

Ob und von wem Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind, kann nachträglich überprüft und festgestellt werden durch:

7.1 Benutzeridentifikation.

7.2 System- und Anwendungslogfiles werden gespeichert und administrative Tätigkeiten aufgezeichnet (Protokollierung).

8. Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

Die Transportkontrolle wird durch folgende Maßnahmen gewährleistet:

8.1 Ein physischer Versand von Datenträgern ist nicht erlaubt.

8.2 Private Datenträger dürfen nicht im Rechenzentrum eingesetzt werden (Regelung durch das Rechenzentrum).

8.3 Daten auf nicht mehr benötigten magnetischen Datenträgern werden durch mehrfaches Überschreiben oder Schreddern zerstört (Regelung durch das Rechenzentrum).

8.4 Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten bei der Übertragung wird verhindert durch:

- Aktuelle Verschlüsselung der Datenübertragung.
- Vollständigkeitsüberprüfung, soweit relevant.
- Aufbau der Transportverbindung nur zwischen definierten und durch Zertifikate gesicherten Systemen.

8.5 Die Transportverfahren bestätigen den Empfang der Daten softwareseitig automatisch.

8.6 Alle zum Transport vorgesehenen sensitiven Daten werden verschlüsselt.

8.7 Die Weitergabe personenbezogener Daten erfolgt durch Nutzung folgender Dienste:

- WWW (HTTPS);
- andere Dienste und Transportverfahren, die dem gewünschten Zweck und dem aktuellen Stand der Sicherheitstechnik äquivalent oder besser entsprechen.

8.8 Folgende Sicherheitsmaßnahmen existieren:

- Hardware- und Software-Firewall-Regeln.
- Technische Vorkehrungen, die das Eindringen von Viren erkennen, die Ausführung von Malware verhindern bzw. die Weitergabe von infizierten Inhalten vermeiden helfen.

8.9 Schnittstellen zu anderen Systemen, Diensten und Datenquellen sind dokumentiert, bewertet und durch angemessene Maßnahmen abgesichert.

8.10 Während des Betriebs der Hosting-Plattform wurden unter anderem die folgenden Maßnahmen ergriffen, um zu gewährleisten, dass Daten bei der elektronischen Übertragung, während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung von Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Der Zugriff auf die Systeme unterliegt der Zugriffskontrolle.
- Der Umgang mit Datenträgern ist formalisiert und in verbindlichen Anweisungen geregelt:
  - Verschlüsselung von Festplatten der Arbeitsrechner.
  - Verschlüsselung externer Datenträger.
  - Sicherstellung der ordnungsgemäßen Vernichtung physischer Datenträger durch zertifizierte Entsorgungsunternehmen bzw. Aktenvernichter.
  - Schutz der Netzwerke gegen Kompromittierung der Übertragung durch Firewalls.

9. Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Die Wiederherstellbarkeit wird durch folgende Maßnahmen realisiert:

9.1 Installation und Pflege der Systeme und Anwendung sind in Betriebsdokumentationen beschrieben worden. Zudem erfolgt die Installation der Systeme und Anwendungen voll automatisiert (per Ansible Scripts).

9.2 Gemäß Support- und Lösungsverantwortungs-Prozess wird um die Störungen und Vorfälle aktiv gekümmert. Es ist ein zweistufiges Support-Konzept umgesetzt worden. Der First Level Support besteht aus Mitgliedern der Gruppe BA (Business Analyst). Der Second Level Support besteht aus Mitgliedern der Gruppen "Anwendungsentwicklung" und "Infrastruktur".

9.3 Im Rahmen der Datensicherung werden Backups von Nutzerdaten und die einzelnen kritischen Server als Snapshot durchgeführt.

9.4 Die Wiederherstellung der Systeme und Anwendungen ist im Confluence dokumentiert.

9.5 Regelmäßiger Test der Datenwiederherstellung.

9.6 Regelmäßige Notfallübungen.

9.7 Zusätzliche Maßnahmen des Rechenzentrums.

10. Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Es wird die Zuverlässigkeit durch folgende Maßnahmen gewährleistet:

10.1 Die Nutzung einer Known Error Database auf System- und Anwendungsebene.

10.2 Überwachung (Monitoring & Logging), Fehlersuche, Fehlerbehebung und Eskalation.

10.3 Gemäß Change-Management-Prozess werden Änderungen an System, Anwendung oder Netzwerk durchgeführt.

10.4 Es werden regelmäßige Schwachstellen- und Penetrationstests durchgeführt.

11. Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Die Datenintegrität wird durch den Change-Management-Prozess und Abnahmeprozess gewährleitet. Im Einzelnen durch die folgenden Ansätze wird es realisiert:

11.1 Jede Änderung am System wird im Vorfeld durch Business Analysten und Software Architekt evaluiert.

11.2 Es werden ausführliche Tests, wie funktionale Test, Last-, Performance- und Penetrationstests durchgeführt.

11.3 Nach dem Abnahme-Prozess werden Releases gebaut und in der Produktion eingespielt.

11.4 Durch Monitoring und Überwachung der Funktionalitäten können rechtzeitig Auffälligkeiten entdeckt und an Support Mitarbeiter gemeldet.

12. Auftragskontrolle

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

Die Auftragskontrolle wird durch folgende Maßnahmen gewährleistet:

12.1 Es existieren Verträge für folgende Formen der Auftragsverarbeitung:

- Wartung/Fernwartung.
- Administration/Fernadministration.
- Cloud-Service-Anbieter.
- Dritte wie z. B. Franke und Bornberg für die Nutzung des Services Angebot- und Antragserstellung.

12.2 Die Verarbeitung personenbezogener Daten im Auftrag erfolgt nur entsprechend den Weisungen des Auftraggebers. Es bestehen schriftliche Vereinbarungen zum Datenschutz zwischen Auftraggeber und Auftragnehmer bzw. Unterauftragnehmern. Alle Mitarbeiter sind der Wahrung des Datengeheimnisses entsprechend § 53 BDSG (neu) verpflichtet, es finden regelmäßig Datenschutzschulungen statt.

12.3 Über gravierende Änderungen im Verfahrensablauf bzw. Störungen wird der Auftraggeber durch den Auftragnehmer informiert.

13. Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

Der Schutz personenbezogener Daten gegen Zerstörung oder Verlust wird durch folgende Maßnahmen gewährleistet:

13.1 Dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind, wird durch Maßnahmen auf RZ-Ebene bzw. innerhalb der Produktivumgebung beispielsweise gewährleistet durch:

- Unterbrechungsfreie Stromversorgung (durch Rechenzentrum gewährleistet).
- Einteilung der Betriebsflächen des Rechenzentrums in Brandabschnitte und Einsatz von Brandfrüherkennung, Brandmeldeanlage, Brandlöschsystem und Feuerlöscher.
- Automatisiertes Monitoring, Alarmierung.
- Berechtigungskonzept für Infrastrukturumgebung.
- Datensicherung gemäß Datensicherungskonzept, z. T. mehrfache, getrennte Ablage von Backup-Daten.
- Redundante Auslegung von Datenverarbeitungssystemen.
- Regelmäßiger Test der Datenwiederherstellung.
- Regelmäßige Notfallübungen.
- Zusätzliche Maßnahmen des Rechenzentrums.
- Regelmäßige Prüfung der Server auf Schwachstellen (Security-Scans).

13.2 Eine Planung für den Katastrophenfall des RZs liegt vor.

14. Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

Die Trennbarkeit wird durch folgende Maßnahmen gewährleistet:

14.1 Personenbezogene Daten dürfen nur für den Zweck genutzt werden, für den sie ursprünglich erhoben wurden.

14.2 Dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können, wird gewährleistet durch:

- softwareseitigen Ausschluss (z. B. Mandantentrennung durch differenzierte Zugriffsregelung und verschlüsselte Dokumentenablage gemäß Verschlüsselungskonzept).
- Verarbeitung erfolgt auf Systemen, die durch logische und physische Zugriffskontrollen im Netzwerk getrennt sind.
- Trennung von Test- und Produktivdaten.
- Trennung von Entwicklungs-, Test- und Produktionssystemen.