



## Vereinbarung zur Auftragsdatenverarbeitung gemäß Artikel 28 DSGVO

zwischen

Vorname

Nachname

Firmierung

Straße

PLZ

Ort

- *nachstehend Auftraggeber genannt* -

und

degenia Versicherungsdienst AG / DMU Deutsche Makler Union GmbH | Brückes 63-63a | 55545 Bad Kreuznach

- *nachstehend Auftragnehmer genannt* -

### Präambel

Versicherungsvermittlung ohne personenbezogene Daten ist nicht möglich. Mit dieser Vereinbarung tragen wir den Anforderungen der ab dem 25.05.2018 gültigen Fassung der Datenschutzgrundverordnung (DSGVO) Rechnung. Die Verordnung enthält in Art. 28 DSGVO verbindliche Vorgaben, wenn personenbezogene Daten im Auftrag durch andere Stellen verarbeitet werden.

Die Auftragsverarbeitung soll nach Art 28 Abs. 3 DSGVO auf Grundlage eines Vertrages erfolgen und die dort festgelegten Inhalte berücksichtigen.

Neben der „klassischen Verarbeitung“ von personenbezogenen Daten im Auftrag, bei der personenbezogene Daten an den Auftragsverarbeiter übermittelt werden, kann Gegenstand des Vertrages zwischen dem Verantwortlichen und dem Auftragsverarbeiter die IT-Wartung oder Fernwartung sein, z. B. Fehleranalysen oder Support-Arbeiten in Systemen des Verantwortlichen. Besteht dabei für den Auftragsverarbeiter die Notwendigkeit oder zumindest die Möglichkeit des Zugriffs auf personenbezogene Daten, so handelt es sich ebenfalls um eine Form oder Teiltätigkeit einer Auftragsverarbeitung und die Anforderungen des Art. 28 DSGVO, wie etwa der Abschluss eines Vertrages zur Auftragsverarbeitung, sind umzusetzen.

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem mit Ihnen geschlossenen Maklervertrag (Courtagevereinbarung) ergeben.

### § 1 Gegenstand und Dauer des Auftrages

(1) Gegenstand

Der Auftrag umfasst Folgendes: (Gegenstand des Auftrags, konkrete Beschreibung der Tätigkeit)

Art und Zweck der Datenverarbeitung

Zweck der Datenverarbeitung durch den Auftragnehmer ist die Unterstützung des Auftraggebers bei der Vermittlung von Verträgen zu Versicherungs-, und/oder Finanz-, und/oder Versorger-Produkten für die DMU Deutsche Makler Union GmbH, sowie der kompletten Antragsverarbeitung (Policierung, Vertragsverwaltung, Inkasso) für die degenia Versicherungsdienst AG.

Dies geschieht auf folgende Weise:



# Vereinbarung zur Auftragsdatenverarbeitung gemäß Artikel 28 DSGVO

## Begrifflichkeiten

### Personenbezogene Daten

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

### Verarbeitung von personenbezogenen Daten

Jeder, mit oder ohne Hilfe automatisierter Verfahren, ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

### Verantwortlicher

Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein, oder gemeinsam mit anderen, über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche, beziehungsweise die bestimmten Kriterien seiner Benennung, nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

### Auftragsverarbeiter

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

- Bereitstellung von Vergleichsrechnern
- Zugang zum internen Bereich inkl. Funktionen zur Kundenverwaltung Prüfung und ggfls. Optimierung eingereicherter Anträge
- Prüfung, inwieweit eingereichte Anträge die Annahmerichtlinien der degenia Versicherungsdienst AG bzw. der übrigen Produktpartner (DMU) erfüllen.
- Weiterleitung eingereicherter Anträge an Produktgeber
- Unterstützung im Antragsprozess per Telefon, Chat oder E-Mail
- Bereitstellung einer Vermittlerhomepage (optional)
- Provisionierung des Auftraggebers
- Speicherung von Daten zu Anfragen (vor und während des Beratungs- und Entscheidungsprozesses)
- Speicherung von Daten zu bestätigten Abschlüssen im Rahmen der steuergesetzlichen Anforderungen

## (2) Dauer

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 3 Monaten gekündigt werden. 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 der Verantwortliche und darf nur erfolgen, wenn die besonderen Voraussetzungen des Art. 44 ff. DSGVO erfüllt sind.

## § 2 Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

### (1) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende:

Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

Personenstammdaten (z.B. Mitarbeiter, Bewerber, Kunden, Lieferanten, Interessenten) Kommunikationsdaten (z.B. Telefon, E-Mail) Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse) Vertragsabrechnungs und Zahlungsdaten Firmenstammdaten Lohn und Gehaltsdaten Bewerbungsunterlagen Daten von Beschäftigten (z.B. Lohn und Gehaltsdaten, Arbeitszeugnisse, Leistungsdaten, Beurteilungen, An- und Abwesenheitsdaten) Daten für Finanzbehörden, Krankenkassen, Berufsgenossenschaften, Sozialversicherungsträger Daten von Gerichten oder Behörden (z.B. bezgl. Pfändung und Insolvenz) Auskunftangaben von Dritten, z.B. Auskunftsteien zur Bonität) Gesundheitsdaten zur Antragserfassung / -Prüfung.



## Vereinbarung zur Auftragsdatenverarbeitung gemäß Artikel 28 DSGVO

### (2) Kategorien betroffener Personen

Die Kategorien, der durch die Verarbeitung betroffenen Personen umfassen:

- Versicherungsnehmer
- Makler
- Interessenten
- Beschäftigte
- Lieferanten

### § 3 Technisch-organisatorische Maßnahmen

(1) Der Auftragsverarbeiter 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 Verantwortlichen zur Prüfung zu übergeben. Bei Akzeptanz durch den Verantwortlichen werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2.) Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen.

(3.) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Die konkrete Beschreibung der technischen und organisatorischen Maßnahmen erfolgt in einer separaten Anlage 1 zu dieser Vereinbarung.

### § 4 Berichtigung, Einschränkung und Löschung von Daten

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, das Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen.

### § 5 Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat, zusätzlich zu der Einhaltung der Regelungen dieses Auftrags, gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO. Insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, soweit gesetzlich vorgeschrieben.

Für den Auftragsverarbeiter ist als Datenschutzbeauftragte(r) bestellt:

**GINDAT GmbH**  
**Herr Arndt Halbach**  
**42897 Remscheid**  
**Tel. 02191 909 430**  
**E-Mail: datenschutz@degenia.de**

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragsverarbeiter 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 Auftragsverarbeiter verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Verantwortlichen obliegen: Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis.



## Vereinbarung zur Auftragsdatenverarbeitung gemäß Artikel 28 DSGVO

Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Verarbeitung von Daten des Auftragsverarbeiters in Privatwohnungen, Tele- bzw. Heimarbeit von Beschäftigten des Auftragsverarbeiters, oder mit mobilen Geräten von unterwegs ist möglich, wenn der Auftraggeber einwilligt. Zum Beispiel, wenn ein Dienst im großen Umfang gestört ist. In diesem Fall hält der Auftragnehmer den höchstmöglichen Schutz ein.

d) Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage und Kosten des Auftraggebers mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Verantwortlichen 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 Auftragsverarbeiter ermittelt.

f) Soweit der Verantwortliche 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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

g) Der Auftragsverarbeiter 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.

### § 6 Weitere Auftragnehmer (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 Auftragsverarbeiter 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 Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Verantwortliche stimmt der Beauftragung der nachfolgenden, weiteren Auftragnehmer (Unterauftragnehmer) zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe der Art. 28 Abs. 2-4 DSGVO. (siehe Anlage II Auftragnehmer)

(3) Die Auslagerung auf Unter-Auftragsverarbeiter oder der Wechsel bestehender Unter-Auftragsverarbeiter sind zulässig, soweit:

- der Auftragsverarbeiter eine solche Auslagerung auf Unter-Auftragsverarbeiter dem Verantwortlichen eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Verantwortliche nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(4) Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

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

(6) Eine weitere Auslagerung durch den Unterauftragsverarbeiter bedarf der ausdrücklichen Zustimmung des Auftragsverarbeiters (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unter-Auftragsverarbeiter aufzuerlegen.



## Vereinbarung zur Auftragsdatenverarbeitung gemäß Artikel 28 DSGVO

### § 7 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche hat das Recht, im Benehmen mit dem Auftragsverarbeiter 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 Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen kann erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditor, Qualitätsauditor);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI- Grundschrift, DIN-ISO 27001).

### § 8 Mitteilung bei Verstößen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO 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 Verantwortlichen zu melden

c) die Verpflichtung, dem Verantwortlichen 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 Verantwortlichen für dessen Datenschutz-Folgenabschätzung e) die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

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

### § 9 Weisungsbefugnis des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten des Verantwortlichen ausschließlich entsprechend der Weisung des Verantwortlichen. Mündliche Weisungen bestätigt der Verantwortliche unverzüglich (mind. Textform).

(2) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird. Die Parteien benennen wechselseitig Ansprechpartner, die eine Weisungsberechtigung haben, bzw. beim Auftragsverarbeiter eine Weisungsbefugnis bezüglich des konkreten Auftrages haben. Sie werden diesbezügliche Änderungen dem jeweils anderen Vertragspartner unverzüglich schriftlich mitteilen. Grundsätzlich gilt der gesetzliche Vertreter als weisungsbefugt.

### § 10 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen 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.



## Vereinbarung zur Auftragsdatenverarbeitung gemäß Artikel 28 DSGVO

### § 10 Löschung und Rückgabe von personenbezogenen Daten

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher, nach Aufforderung durch den Verantwortlichen, spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder, nach vorheriger Zustimmung, datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Die Löschung bzw. Vernichtung ist dem Auftraggeber auf Anforderung zu bestätigen.

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

Bad Kreuznach

Halime Koppius  
degenia Versicherung AG | DMU Deutsche Makler Union GmbH

Ort | Datum

Unterschrift Makler/in

MUSTER

#### degenia Versicherungsdienst AG

Vorstand: Halime Koppius  
Aufsichtsrat: Karl Spies (Vorsitzender)  
Amtsgericht: Bad Kreuznach HRB 4221  
DIHK Nr.: D-MASO-DO7VY-12 IHK Koblenz  
Erl. n. § 34d Abs 1 GewO

#### DMU Deutsche Makler Union GmbH

Geschäftsführung: Halime Koppius | Ortwin Spies  
Amtsgericht: Bad Kreuznach HRB 20327  
DIHK Nr.: D-311W-LT-JOM-65 IHK Koblenz  
Erl. n. § 34d Abs 1 GewO

#### Kontakt

Brückes 63-63a | 55545 Bad Kreuznach  
Fon 0671 84003-0  
Fax 0671 84003-29  
www.degenia.de | info@degenia.de  
www.makler-union.de | post@makler-union.de



## Anlage 1

### Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Artikel 32 Absatz 1 DSGVO)

#### a) Pseudonymisierung personenbezogener Daten

Daten werden in unterschiedlichen Tabellen gespeichert. Referenzen werden nur über Nummern/IDs hergestellt.

#### b) Verschlüsselung personenbezogener Daten

Verschlüsselung der Daten auf SQL-Server

**c) Gewährleistung der Vertraulichkeit der Systeme und Dienste**, die einen unautorisierten Zugang oder Zugriff auf personenbezogene Daten verhindern sollen.

Zutrittskontrolle

Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen:

- Gebäude nur mit Schlüssel betretbar
- Empfang in der Arbeitszeit besetzt sonst Tür verschlossen
- Serverräume werden durch elektronische Schlösser vor unbefugtem Zutritt geschützt.
- Gebäude sind außerhalb der Arbeitszeiten Alarm gesichert und der Hof Videoüberwacht.

Zugangskontrolle

Schutz vor unbefugter Systembenutzung

- Sicheres Passwort
- Passwortsperrung nach Fehlversuchen
- Autom. Bildschirmspernung
- Firewall

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.

- AD Gruppen und Rollen
- Festlegung der Zugriffsrechte nach Bedarf
- Papierdokumente werden mit Partikelschredder oder durch zertifizierten Dienstleistern vernichtet

Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

- Verschlüsselung
- VPN
- Verschlüsselter Versand per Cryptshare

Trennungskontrolle

Maßnahmen, damit zu unterschiedlichen Zwecken – insbesondere für unterschiedliche Kunden – erhobene bzw. zu verarbeitende Daten getrennt voneinander verarbeitet werden

- Trennung von Produktions- und Testumgebungen

#### d) Gewährleistung der Integrität der Systeme und Dienste

- Protokollierung der Eingabe mit Benutzer und Zeitpunkt

#### e) Gewährleistung der Verfügbarkeit der Systeme und Dienste

- Datensicherungen als Komplettsicherungen und Differenzsicherungen
- USV
- Temperatursensoren
- Redundante Klimatisierung



## Anlage 1

---

**f) Gewährleistung der Belastbarkeit der Systeme und Dienstag**

- Durch Kapazitätsprognosen und ständige Aktualisierung der Systeme ist die Auslastung bei 30-40%

**g) Verfahren zur raschen Wiederherstellung der Verfügbarkeit nach einem Zwischenfall**

- Backupkonzept (3 Varianten)
- 2 Serverräume räumlich getrennt

**h) Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen**

- Externe Prüfungen (Revision durch Versicherungsgesellschaften)
- Wirtschaftsprüfer

MUSTER





## Anlage 2

---

### Name und Anschrift der weiteren Beschreibung der Leistung Auftragnehmer

#### Softwareentwicklung

ids-software Ltd. & Co KG | Am Willenbach 3 | 74229 Oedheim

#### Telefonanlage

Sascha Knob | more than IT | Trierer Straße 90 | 54411 Hermeskeil

#### Kopiergeräte/ Drucker

BLUM GmbH | Rhenser Str. 12 | 56323 Waldesch

#### Webserveranbieter

- 1&1 Internet SE | Elgendorfer Str. 57 | 56410 Montabaur
- STRATO AG | Pascalstraße 10 | 10587 Berlin

#### Vergleichsrechner

- Mr-Money Software | Dirk Natschke | Schillerstraße 3 | 09366 Stollberg
- Verivox GmbH | Am Taubenfeld 10 | 69123 Heidelberg
- NAFI® GmbH | Lütmarser Straße 60 | 37671 Hötter
- Gewerbeversicherung24 Vergleichsportal GmbH | Rotfeder-Ring 5 | 60327 Frankfurt am Main

#### Bonitätsauskunft

- Bertelsmann SE & Co. KGaA | Carl-Bertelsmann-Straße 270 | 33311 Gütersloh
- Verein Creditreform Bad Kreuznach | Planiger Straße 34 a | 55543 Bad Kreuznach

#### Inkassobüro

Dr. KÄMPF & Associates GmbH | INKASSOdienstleistungen | Stromberger Str. 2 | D-55545 Bad Kreuznach

#### Steuerberater & Wirtschaftsprüfer

Dipl.-Kfm. Hans-Joachim Haßlinger | Wirtschaftsprüfer, Steuerberater | Rebgarten 24 | 55543 Bad Kreuznach