

Bedingungen für die Nutzung des Maklerportals der Grundeigentümer-Versicherung VVaG (Nutzungsbedingungen)

1. Gegenstand der Nutzung

Die Grundeigentümer-Versicherung VVaG (nachstehend: GEV) stellt dem Vertriebspartner auf Antrag einen Zugang zu ihrem Maklerportal (nachstehend: MaklerNet) zur Verfügung. Über diesen Zugang kann der Vertriebspartner bestimmte Geschäftsprozesse online erledigen und auf Dienstleistungsprogramme, Informationen sowie – im Rahmen seiner Betreuungszuständigkeit – auf Kunden- bzw. Vertragsdaten zugreifen. Bei der Einräumung des Zugangs handelt es sich um eine freiwillige und unentgeltliche Serviceleistung der GEV; demgemäß ist die GEV jederzeit berechtigt, Inhalte und Schnittstellen des MaklerNet sowie die Domain ganz oder teilweise zu ändern, umzugestalten oder deren Bereitstellung einzustellen.

2. Nutzungsvereinbarung, Nutzungsrecht

Mit der Eröffnung des Zugangs zum MaklerNet kommt zwischen der GEV und dem Vertriebspartner eine Nutzungsvereinbarung nach Maßgabe dieser Nutzungsbedingungen zu Stande. Im Rahmen dieser Nutzungsvereinbarung wird dem Vertriebspartner das nicht ausschließliche und nicht übertragbare Recht eingeräumt, das MaklerNet selbst oder durch weitere berechtigte Nutzer (nachstehend Ziff. 3) im Rahmen der Erfüllung des zwischen ihm und der GEV bestehenden Vertragsverhältnisses (z. B. Maklervertrag) zu nutzen; eine Nutzung für andere Zwecke ist nicht gestattet. Das Nutzungsrecht beinhaltet das Recht zur Speicherung erhaltener Daten zur unmittelbaren vertragsgemäßen Verarbeitung und zur Datensicherung.

3. Berechtigte Nutzer, Administrator

Berechtigte Nutzer sind der Vertriebspartner bzw. dessen gesetzliche Vertreter, ein von dem Vertriebspartner benannter Administrator und solche natürlichen Personen, die

- mit dem Vertriebspartner in einem Vertragsverhältnis (z. B. Arbeits- oder sonstiger

Dienstvertrag, Untermaklervertrag) stehen, dessen Inhalt den Zugriff auf die im MaklerNet bereitgestellten Dienstleistungsprogramme, Informationen und Daten erforderlich macht,

- schriftlich oder in Textform eine Verpflichtung auf das Datengeheimnis und das Privatgeheimnis gemäß § 203 Strafgesetzbuch (StGB) bzw. des Geschäftsgeheimnisses gem. GeschGehG abgegeben haben, wobei diese Verpflichtung über die Dauer des Vertragsverhältnisses unbefristet hinausgehen muss,
- diesen Nutzungsbedingungen schriftlich oder in Textform zugestimmt haben und
- durch die GEV oder durch den von dem Vertriebspartner benannten Administrator als berechtigte Nutzer namentlich registriert wurden.

Die Nutzung eines Zugangs durch Dritte ist nicht gestattet. Der Vertriebspartner kann der GEV einen oder mehrere berechtigte Nutzer benennen, die mit ihm in einem Vertragsverhältnis im Sinne des vorstehenden Absatzes stehen und schriftlich oder in Textform ihre Verpflichtung auf das Daten- und das Privatgeheimnis sowie die Zustimmung zu diesen Nutzungsbedingungen erklärt haben müssen. Diese berechtigten Nutzer werden durch die GEV registriert. Endet das zur Nutzung berechtigte Vertragsverhältnis oder wird dem Vertriebspartner ein Verstoß des Nutzers gegen die Verpflichtung auf das Daten- und das Privatgeheimnis oder eine sonstige missbräuchliche Nutzung bekannt, so hat der Vertriebspartner dies unverzüglich anzuzeigen, damit die GEV den Zugang sperren kann.

Alternativ kann der Vertriebspartner der GEV über das Administrationsrecht selbstständig tätig werden und weitere berechtigte Nutzer in der Benutzerverwaltung registrieren. Für auf diesem Wege angelegte weitere berechtigte Nutzer überprüft der Vertriebspartner eigenverantwortlich die Berechtigung zur Nutzung gemäß dem vorstehenden Absatz 1, nämlich das Bestehen eines Vertragsverhältnisses, die Verpflichtung auf das Daten- und das Privatgeheimnis sowie die Zustimmung zu diesen Nutzungsbedingungen; die

Verpflichtung auf das Daten- und das Privatgeheimnis sowie die Zustimmungserklärung verwahrt der Administrator für die GEV; der er deren Vorliegen auf jederzeitiges Verlangen nachzuweisen hat. Nach Prüfung der Berechtigung zur Nutzung registriert der Administrator den berechtigten Nutzer online und vergibt online eine Nutzerkennung. Der Administrator kann die Registrierung jederzeit aufheben; endet das zur Nutzung berechtigende Vertragsverhältnis oder wird dem Administrator ein Verstoß des Nutzers gegen die Verpflichtung auf das Daten- und das Privatgeheimnis oder eine sonstige missbräuchliche Nutzung bekannt, so ist er zur unverzüglichen Aufhebung verpflichtet.

Ein Wechsel des im Antrag benannten berechtigten Nutzers ist der GEV unverzüglich mitzuteilen, damit die GEV den bisherigen Benutzeraccount sperren und einen neuen Zugang inklusive Administrationsrechten einrichten kann.

4. Passwort, missbräuchliche Nutzung

Wird der Antrag auf Zugang zum Maklerportal seitens der GEV positiv entschieden, erfolgt eine Aufforderung zur Vergabe eines Passworts an die im Antrag durch den Vertriebspartner angegebene E-Mail-Adresse. Der Link zur Passwortvergabe hat eine begrenzte Gültigkeit von 45 Tagen und ist nur einmalig pro erstelltem berechtigtem Nutzer anwendbar.

Mindestanforderungen an die Passwortsicherheit werden im Zuge der Registrierung mitgeteilt und folgen aktuellen Empfehlungen des Datenschutzbeauftragten der GEV.

Das Passwort darf nur durch den berechtigten Nutzer verwendet und anderen Personen nicht mitgeteilt werden; es darf nicht notiert oder elektronisch gespeichert werden. Der Administrator und jeder andere berechtigte Nutzer sind verpflichtet, die GEV unverzüglich zu unterrichten, wenn ihnen eine missbräuchliche Nutzung des MaklerNet bekannt wird.

5. Urheberrecht, sonstige Schutzrechte

Inhalt und Struktur des MaklerNet sind urheberrechtlich geschützt. Eine Nutzung von Informationen oder Daten (Text, Bild, Grafik, Ton, Video oder Animationsdateien) ist nur im Rahmen dieser Nutzungsbedingungen zulässig. Geschützt sind alle auf dem MaklerNet verwendeten Marken und Logos, deren Nutzung der vorherigen schriftlichen Zustimmung der GEV bedarf.

6. Hyperlinks

Die GEV ist nicht für den Inhalt von Webseiten verantwortlich, auf die mittels Hyperlink verwiesen wird, und lehnt ausdrücklich jede Haftung für deren Inhalt ab: Ein Hyperlink auf eine andere Webseite ist lediglich als Hilfe zu verstehen und impliziert nicht, dass die GEV diese Webseite oder Produkte und Dienstleistungen, die dort beschrieben werden, ihrerseits geprüft hat, billigt oder für richtig befindet.

7. Gewährleistung der GEV

Die GEV leistet keine Gewähr für die ununterbrochene Verfügbarkeit des MaklerNet, für Lauffähigkeit von Programmen und für Virenfreiheit; Sicherheitsvorkehrungen trifft die GEV allein im Eigeninteresse und in dem von der GEV für zweckmäßig erachteten Umfang. Die GEV ist um aktuelle und zutreffende Informationen bemüht, ohne für deren Aktualität, Richtigkeit und Vollständigkeit einzustehen.

8. Haftung der GEV

Die GEV haftet bei einfacher Fahrlässigkeit nicht auf Aufwendungs- oder Schadensersatz – gleich aus welchem Rechtsgrund –, es sei denn, der Schaden beruht auf einer Verletzung wesentlicher Vertragspflichten. Die Haftung für einfache Fahrlässigkeit ist generell auf den Ersatz des typischerweise bei Eröffnung des Zugangs zum MaklerNet voraussehbaren Schadens beschränkt. Die vorstehenden Sätze gelten nicht bei Schäden aus der Verletzung des Lebens, des Körpers und der Gesundheit und nicht für die Haftung nach dem Produkthaftungsgesetz.

9. Datenschutz und Datensicherheit

Der Schutz der Daten des Nutzers ist der GEV sehr wichtig. Informationen zum Umgang und zur Verarbeitung personenbezogener Daten im Rahmen der Nutzung der Plattform finden sich in den Datenschutzhinweisen der GEV – siehe auch [gev-versicherung.de/informationen/datenschutz/](https://www.gev-versicherung.de/informationen/datenschutz/)

10. Löschung personenbezogener Daten

Wir löschen Ihre personenbezogenen Daten, sobald sie für die oben genannten Zwecke nicht mehr erforderlich sind. Dabei kann es vorkommen, dass personenbezogene Daten für die Zeit aufbewahrt werden, in der Ansprüche gegen unser Unternehmen geltend gemacht

werden können (gesetzliche Verjährungsfrist von drei oder bis zu dreißig Jahren). Zudem speichern wir Ihre personenbezogenen Daten, soweit wir dazu gesetzlich verpflichtet sind. Entsprechende Nachweis- und Aufbewahrungspflichten ergeben sich unter anderem aus dem Handelsgesetzbuch, der Abgabenordnung und dem Geldwäschegesetz. Die Speicherfristen betragen danach bis zu zehn Jahre.

11. Willenserklärungen und Mitteilungen

Willenserklärungen und Mitteilungen im Rahmen der Nutzung des MaklerNet sind abgegeben, wenn sie der berechnigte Nutzer im Anschluss an die vollständige Eingabe gemäß der Benutzerführung (z. B. durch Betätigen des OK-Feldes) übermittelt. Hinsichtlich solcher Willenserklärungen und Mitteilungen wird sich die GEV nicht auf eine vertraglich etwa vereinbarte Schriftform berufen; die GEV und der Vertriebspartner verzichten insoweit auf ein vertragliches Schriftformerfordernis. Für Willenserklärungen und Mitteilungen der GEV genügt, soweit diese Nutzungsbedingungen für einzelne Willenserklärungen keine strengere Form vorsehen, die Übermittlung per E-Mail.

12. Webcontrolling

Zur Optimierung der nutzerbezogenen Abläufe und für interne statistische Zwecke wird die Nutzung des MaklerNet überwacht und aufgezeichnet (Webcontrolling). Wird Webcontrolling durch individuelle Browsereinstellungen (z. B. „Cookies annehmen“ deaktiviert) ausgeschlossen, ist ein Zugang zum MaklerNet nicht möglich.

13. Betroffenenrechte

Sie können über die unter Punkt 17 benannte Adresse des GEV Datenschutzbeauftragten Auskunft über die zu Ihrer Person gespeicherten Daten verlangen. Darüber hinaus können Sie unter bestimmten Voraussetzungen die Berichtigung oder die Löschung Ihrer Daten verlangen. Ihnen kann weiterhin ein Recht auf Einschränkung der Verarbeitung Ihrer Daten sowie ein Recht auf Herausgabe der von Ihnen bereitgestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zustehen.

14. Änderung der Nutzungsbedingungen

Die GEV ist berechtigt, diese Nutzungsbedingungen mit angemessener Ankündigungsfrist zu ändern oder zu ergänzen. Es genügen die Ankündigung auf der Startseite des MaklerNet und Einstellung der neuen Nutzungsbedingungen in das MaklerNet. Durch die weitere Nutzung des MaklerNet erklären sich der Vertriebspartner und jeder berechnigte Nutzer mit der Änderung der Nutzungsbedingungen einverstanden.

15. Widerruf von Nutzungsrechten, Zugangssperre

Das Nutzungsrecht und/oder der Zugang jedes berechtigten Nutzers können durch die GEV jederzeit widerrufen bzw. gesperrt werden. Die GEV wird den Widerruf erklären bzw. einen Nutzerzugang sperren, wenn Tatsachen den Verdacht einer missbräuchlichen Nutzung oder eines sonstigen schweren Verstoßes gegen die Nutzungsbedingungen begründen. Die GEV wird auch dann einen Widerruf erklären bzw. den Nutzerzugang sperren, wenn der Vertriebspartner

bzw. der berechnigte Nutzer einer Änderung der Nutzungsbedingungen widerspricht.

Sie haben das Recht, einer Verarbeitung Ihrer personenbezogenen Daten zu widersprechen. Verarbeiten wir Ihre Daten zur Wahrung berechtigter Interessen, können Sie dieser Verarbeitung widersprechen, wenn sich aus Ihrer besonderen Situation Gründe ergeben, die gegen die Datenverarbeitung sprechen.

16. Beendigung der Nutzungsvereinbarung

Die Nutzungsvereinbarung kann von jeder Partei mit einer Frist von einem Monat zum Monatsende schriftlich oder in Textform gekündigt werden; sie endet ferner, ohne dass es einer besonderen Kündigung bedarf, wenn die Geschäftsverbindung zwischen der GEV und dem Vertriebspartner endet. Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

17. Beschwerderecht

Sie haben die Möglichkeit, sich mit einer Beschwerde an den Datenschutzbeauftragten der GEV oder an eine Datenschutzaufsichtsbehörde zu wenden.

Datenschutzbeauftragter der GEV:

Grundeigentümer-Versicherung, Versicherungsverein auf Gegenseitigkeit (VVaG)

Große Bäckerstraße 7

20095 Hamburg

Tel.: 040 / 376 63 - 159

E-Mail: datenschutz@grundvers.de

Die für uns **zuständige Datenschutzaufsichtsbehörde** ist:

DER HAMBURGISCHE BEAUFTRAGTE FÜR
DATENSCHUTZ UND INFORMATIONSFREIHEIT

Ludwig-Erhard-Str 22, 7. OG

20459 Hamburg

Tel.: 040 / 428 54 - 4040

Fax: 040 / 428 54 - 4000

E-Mail: mailbox@datenschutz.hamburg.de

18. Schlussbestimmungen

Die Nutzungsvereinbarung und jede Nutzung des MaklerNet unterliegen deutschem Recht. Gerichtsstand für alle Streitigkeiten aus der Nutzung des MaklerNet zwischen der GEV und dem Vertriebspartner ist Hamburg.

Auftragsverarbeitung gemäß Art. 28 der EU-Datenschutzgrundverordnung (DS-GVO)

zwischen der

**Grundeigentümer-Versicherung VVaG
(im Folgenden kurz „GEV“ genannt)**

Große Bäckerstraße 7
20095 Hamburg

- Auftragsverarbeiter - nachstehend Auftragnehmer oder GEV genannt

und dem

**im Antrag auf Zugang zum Maklerportal der
Grundeigentümer-Versicherung VVaG genannten Vertragspartner**

- Verantwortlicher - nachstehend Auftraggeber genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Gegenstand und Zweck des Auftrags bestehen darin, dem Makler die Möglichkeit zu geben, in Maklerportal der GEV (nachstehend: MaklerNet) Interessendaten zu speichern.

Die vertraglich vereinbarte Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

(2) Dauer

Der Vertrag beginnt zum im **Antrag auf Zugang zum Maklerportal der Grundeigentümer-Versicherung VVaG** benannten Datum und endet mit Ablauf der vereinbarten Laufzeit bzw. mit seiner Kündigung oder Aufhebung spätestens aber mit dem Ende der Laufzeit der entsprechenden Nutzungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

- Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

Der Makler hat Zugang zu dem von der GEV zur Verfügung gestellten Maklerportal. Es bietet dem Makler die Möglichkeit, über den Zugriff auf die für die GEV dort gespeicherten Antrags- und Vertragsdaten hinaus auch in seiner eigenen Verantwortung stehende personenbezogene Daten (Interessentendaten) zu speichern und zu verarbeiten. Diese Interessentendaten sind logisch getrennt von den sonstigen im System gespeicherten Daten. Sofern es die Speicherung und Verarbeitung von Interessentendaten betrifft, ist die GEV Auftragnehmer des Maklers gemäß Art. 28 DSGVO. Der Makler ist Auftraggeber.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(2) Art der Daten

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

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Schadendaten
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftangaben (von Dritten, z.B. Auskunftsteilen, oder aus öffentlichen Verzeichnissen)
- ...

(3) Kategorien betroffener Personen

- Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter:

oder

- Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
 - Kunden

- Anspruchsteller
- Interessenten
- Beschäftigte
- Lieferanten
- Vermittler
- ...

3. Technische und organisatorische Maßnahmen (TOM)

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage].

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

4. Berichtigung, Einschränkung und Löschung von Daten

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

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

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben: Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer

Herr Christian Brockhausen
Compliance ; Datenschutz

Tel.: 040 – 376 63 – 159
E-Mail: Datenschutz@grundvers.de

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

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

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

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

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

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

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

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

6. Unterauftragsverhältnisse

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

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Der Wechsel eines bestehenden Unterauftragnehmers ist zulässig, soweit:

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

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

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

7. Kontrollrechte des Auftraggebers

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

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

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

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

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

8. Mitteilung bei Verstößen des Auftragnehmers

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

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

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

9. Weisungsbefugnis des Auftraggebers

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

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

10. Löschung und Rückgabe von personenbezogenen Daten

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

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

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

Anlage – Technische und organisatorische Maßnahmen der GEV

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

- **Zutrittskontrolle**
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pfortner, Alarmanlagen, Videoanlagen;
- **Zugangskontrolle**
Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- **Zugriffskontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- **Trennungskontrolle**
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- **Pseudonymisierung** (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

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

- **Weitergabekontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- **Eingabekontrolle**
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

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

- **Verfügbarkeitskontrolle**
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/off-line; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- **Rasche Wiederherstellbarkeit** (Art. 32 Abs. 1 lit. c DS-GVO)

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

- **Datenschutz-Management**
- **Incident-Response-Management**
- **Datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DS-GVO)
- **Auftragskontrolle**
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.