

Vertraulichkeitsvereinbarung mit externen Partnern

Zwischen der

**Volksbank Mittelhessen Immobilien-service GmbH,
Schiffenberger Weg 110, 35394 Gießen**

(nachstehend Auftraggeber genannt)

und

externen Partnern

(nachstehend Auftragnehmer genannt)

Es sind die Vorschriften der Datenschutzgrundverordnung, des Telekommunikationsgesetzes, und die für den Auftraggeber maßgebenden gesetzlichen und betrieblichen Bestimmungen für alle Auftragsverhältnisse, die zwischen dem Auftragnehmer und dem Auftraggeber bestehen oder künftig zustande kommen und alle sonstigen Betriebsangelegenheiten des Auftraggebers zur Vertraulichkeit und zum Datenschutz zu beachten.

Die Parteien verpflichten sich, die ihnen übergebenen oder sonst zur Kenntnis gelangten Betriebsgeheimnisse, vertraulichen Unterlagen, Betriebsinterna und individuelle Projektinformationen (vertraulichen Informationen) ausschließlich für die Zwecke der Auftragsbearbeitung zu nutzen. Die Pflicht zur absoluten Vertraulichkeit dauert auch nach Beendigung der Zusammenarbeit zeitlich unbefristet an.

Darüber hinaus dürfen die jeweils übergebenen oder sonst zur Kenntnis gelangten Betriebsgeheimnisse, vertraulichen Unterlagen, Betriebsinterna und die individuellen Projektinformationen (vertraulichen Informationen) weder aufgezeichnet noch weitergegeben oder für eigene Zwecke verwertet werden. Der Auftragnehmer wird durch geeignete vertragliche Abreden mit den für ihn tätigen Arbeitnehmern und Beauftragten sicherstellen, dass auch diese unbefristet jede eigene Verwertung, Weitergabe oder unbefugte Aufzeichnung vertraulicher Informationen unterlassen.

Die Verschwiegenheitspflicht gilt für jede Art der Kenntniserlangung sei es mündlich, in Papierform oder in elektronischer Form (durch Datenübermittlung oder auf Datenträgern), durch die Gestattung von Besichtigungen oder auf andere Weise durch direkte oder indirekte Übermittlung.

Jede der Parteien darf vertrauliche Informationen der anderen Partei nur dann weitergeben, wenn gesetzliche oder rechtliche Bestimmungen oder Anordnungen dies gebieten oder wenn die andere Partei hierzu eingewilligt hat. Sofern es hierzu der Einwilligung der Betroffenen bedarf, wird die andere Partei diese einholen. Der Auftragnehmer wird die Informationen nur mit Zustimmung des Auftraggebers an Mitarbeiter oder Dritte übergeben. Der Auftragnehmer wird alle Mitarbeiter, denen er vertrauliche Informationen überlässt bzw. die er zur Leistungserbringung einsetzt, dazu verpflichten, dass diese die ihnen zugänglich gemachten vertraulichen Informationen gleichfalls vertraulich behandeln und ausschließlich für den Vertragszweck benutzen. Der Auftragnehmer haftet für die Einhaltung der von ihm mit dieser Vereinbarung übernommenen Verpflichtungen durch seine Mitarbeiter.

Die Parteien treffen alle angemessenen Vorkehrungen, um einen Zugriff Dritter auf vertrauliche Informationen der anderen Partei zu vermeiden (z.B. Zugangskontrolle, Verschlüsselung). Diese Vorkehrungen haben sich am aktuellen Stand der Technik zu orientieren.

Die Parteien sind berechtigt, im Zusammenhang mit einzelnen Geschäftsvorfällen, während der laufenden Geschäftsbeziehung, Handakten in physischer oder elektronischer Form anzulegen.

Die Auftraggeber kann die Herausgabe vertraulicher Unterlagen jederzeit verlangen. Verlangt der Auftraggeber die Herausgabe vertraulicher Unterlagen, wird der Auftragnehmer sämtliche vom Auftraggeber erhaltenen vertraulichen Unterlagen diesem unverzüglich übergeben. Der Auftragnehmer hat kein Zurückbehaltungsrecht an Unterlagen. Bei elektronisch auf wiederbeschreibbaren Speichermedien gespeicherten Informationen genügt die Löschung der Informationen bzw. Dateien, sofern dies so geschieht, dass ein Wiederherstellen der Daten nicht möglich ist und ein Protokoll über die Löschung erstellt und auf Anforderung zur Verfügung gestellt wird.

Die Parteien sind verpflichtet, die Bestimmungen der Datenschutzgrundverordnung (DSGVO) sowie etwaiger bereichsspezifischer datenschutzrechtlicher Bestimmungen bei der Erbringung der Leistungen nach dem Vertrag zu beachten. Im Rahmen des Zumutbaren wird die datenspeichernde Partei dem jeweiligen Datenschutzbeauftragten der anderen Partei nach vorheriger Anmeldung ermöglichen, die Einhaltung der datenschutzrechtlichen Vorschriften durch die speichernde Partei zu überprüfen. Die speichernde Partei wird Weisungen des Auftraggebers, die sich auf die Einhaltung der datenschutzrechtlichen Vorschriften beziehen, beachten.

Die Vertraulichkeit wird auch bei der E-Mail-Kommunikation beachtet, indem die Parteien vertrauliche Informationen, die per E-Mail übermittelt werden sollen, gegen Kenntnisnahme und Manipulationen durch unberechtigte Dritte schützen. Die Parteien können hierzu entsprechende technische Maßnahmen, z.B. Verschlüsselungs- und Signaturverfahren, abstimmen.

Den Parteien ist bekannt, dass

- der Verrat von Geschäfts- und Betriebsgeheimnissen sowie die Verwertung von Vorlagen nach den §§ 17,18 UWG strafbar ist und mit Freiheitsstrafe bis zu 5 Jahren geahndet werden kann,
- derjenige, der Geschäfts- und Betriebsgeheimnisse verletzt, zum Ersatz des daraus entstehenden Schadens nach § 9 UWG verpflichtet ist und die Verletzung datenschutzrechtlicher Bestimmungen nach Art. 83 DSGVO strafbar ist. Der Auftragnehmer haftet für alle Schäden in vollem Umfang, die dem Auftraggeber durch Verletzung dieser vertraglichen Pflichten entstehen.

Die Vertraulichkeitsverpflichtung gilt auch für die Rechtsnachfolger der Parteien. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

Bitte beachten Sie die Anlage zur Vertraulichkeitserklärung

Anlage zur Vertraulichkeitsvereinbarung

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim betrieblichen Datenschutzbeauftragten.

Begrifflichkeiten

Art. 4 Nr. 1 DS-GVO: „Personenbezogene Daten“ [sind] 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.

Art. 4 Nr. 2 DS-GVO: „Verarbeitung“ [meint] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten 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, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Grundsätze der Verarbeitung

Art. 5 Abs. 1 lit. a DS-GVO: Personenbezogene Daten müssen [...] auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“).

Art. 5 Abs. 1 lit. f DS-GVO: Personenbezogene Daten müssen [...] in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Art. 29 DS-GVO: Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Art. 32 Abs. 2 DS-GVO: Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Art. 33 Abs. 1 Satz 1 DS-GVO: Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der [...] zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Haftung

Art. 82 Abs. 1 DS-GVO: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Art. 83 Abs. 1 DS-GVO: Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung [...] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

§ 42 BDSG

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
 2. auf andere Art und Weise zugänglich macht
- und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

§ 202a Abs. 1 StGB: Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

§ 303a Abs. 1 StGB: Wer rechtswidrig Daten [...] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Fernmeldegeheimnis

§ 88 TKG

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. 2Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. 2Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. 2Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang. [...]