

## **Auftrag gemäß § 11 BDSG**

### **Vereinbarung**

zwischen dem / der

.....

.....

- nachstehend Auftraggeber genannt -

und dem / der

Mr-Money Unternehmensgruppe (Mr-Money Software GmbH, Mr-Money Service GmbH und Mr-Money Makler-Bund GmbH)

Mr-Money Software GmbH, Schillerstraße 3, 09366 Stollberg

Mr-Money Makler-Bund GmbH, Schillerstraße 3, 09366 Stollberg

Mr-Money Service GmbH, Aggensteinstr. 23, 81545 München

- nachstehend Auftragnehmer genannt -

### **1. Gegenstand und Dauer des Auftrags**

#### **Gegenstand des Auftrags**

Der Gegenstand des Auftrags ergibt sich aus den Lizenzvereinbarungen der Softwareprodukt zwischen den Auftraggeber und Auftragnehmer.

#### **Dauer des Auftrags**

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Lizenzvereinbarung

## **2. Konkretisierung des Auftragsinhalts**

### **Umfang, Art und Zweck**

#### **der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten**

Umfang, Art und Zweck der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Lizenzvereinbarung in § 1 der Allgemeinen Geschäftsbedingungen

Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, 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 §§ 4b, 4c BDSG erfüllt sind.

### **Art der Daten**

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

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Allgemeine Vertragsdaten
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

### **Kreis der Betroffenen**

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst (Aufzählung / Beschreibung der betroffenen Personenkategorien):

- Kunden
- Interessenten
- Lizenznehmer
- Beschäftigte i. S. d. § 3 Abs. 11 BDSG
- Lieferanten des Auftragnehmers
- Handelsvertreter
- Tippgeber
- Werbepartner
- Ansprechpartner in der Unternehmensgruppen
- Techniker
- Programmierer
- Support

### **3. Technisch-organisatorische Maßnahmen**

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten 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.

Insgesamt handelt es sich bei den zu treffenden Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie des Trennungsgebots, sowie andererseits um auftragsspezifische Maßnahmen, insbesondere im Hinblick auf die Art des Datenaustauschs / Bereitstellung von Daten, Art / Umstände der Verarbeitung / der Datenhaltung sowie Art / Umstände beim Output / Datenversand, die – soweit sie sich nicht aus der zugrundeliegenden Leistungsvereinbarung ergeben.

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.

#### **4. Berichtigung, Sperrung und Löschung von Daten:**

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

#### **5. Kontrollen und sonstige Pflichten des Auftragnehmers:**

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach § 11 Abs. 4 BDSG folgende Pflichten:

- Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß §§ 4f, 4g BDSG ausüben kann.
- Die Wahrung des Datengeheimnisses entsprechend § 5 BDSG. 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 Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG und Anlage.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG. Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG beim Auftragnehmer ermittelt.
- 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.

#### **6. Unterauftragsverhältnisse:**

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 nur mit schriftlicher Zustimmung des Auftraggebers gestattet. Ohne schriftliche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner unter Punkt 5 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen sowie im Einzelfall andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn der Verarbeitung oder Nutzung mitteilt.
- Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem / den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.
- Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des § 11 BDSG i.V.m. Nr. 6 der Anlage zu § 9 BDSG beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

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, Wartung und Benutzerservice, 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. Kontrollrechte des Auftraggebers:**

Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu § 9 BDSG vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer 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. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben.

## **8. Mitteilung bei Verstößen des Auftragnehmers:**

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

Es ist bekannt, dass nach § 42a BDSG 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 § 42a BDSG treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

## **9. Weisungsbefugnis des Auftraggebers:**

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl. § 11 Abs. 3 Satz 1 BDSG). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. 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.

Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen

datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

#### **10. Löschung von Daten und Rückgabe von Datenträgern:**

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte 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.

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

\_\_\_\_\_, den \_\_\_\_\_

\_\_\_\_\_, den \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Auftraggeber

Auftragnehmer - Mr-Money

## **Allgemeine technische und organisatorische**

### **Maßnahmen nach § 9 BDSG und Anlage für :**

**Mr-Money Software GmbH, Schillerstraße 3, 09366 Stollberg**

**Mr-Money Makler-Bund GmbH, Schillerstraße 3, 09366 Stollberg**

#### **1. Zutrittskontrolle**

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- *Alarmanlage*
- *Biometrische Zugangssperren*
- *Schlüsselregelung (Schlüsselausgabe etc.)*
- *Videoüberwachung der Zugänge*
- *Sicherheitsschlösser*

#### **2. Zugangskontrolle**

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Zuordnung von Benutzerrechten
- Passwortvergabe
- Authentifikation mit Benutzernamen / Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Sicherheitsschlösser
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall



### **3. Zugriffskontrolle**

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- Erstellen eines Berechtigungskonzepts
- Anzahl der Administratoren auf das "Notwendigste" reduziert
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Verschlüsselung von Datenträgern
- Verwaltung der Rechte durch Systemadministrator
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- 

### **4. Weitergabekontrolle**

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- Einrichtungen von Standleitungen bzw. VPN-Tunnel
- E-Mail-Verschlüsselung
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen

### **5. Eingabekontrolle**

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Lösung von Daten auf Basis eines Berechtigungskonzeptes

## **6. Auftragskontrolle**

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

- Wirksam Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

## **7. Verfügbarkeitskontrolle**

Maßnahmen zur Datensicherung (physikalisch / logisch):

- Unterbrechungsfreie Stromversorgung (USV)
- Feuer- und Rauchmeldeanlagen
- Aufbewahrung von Datensicherung an einem sicheren , ausgelagerten Ort
- Schutzsteckdosenleisten in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Serverräume nicht unter sanitären Anlagen

## **8. Trennungskontrolle**

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- physikalische getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem