ApptiveGrid

Vertrag über die Auftragsverarbeitung gemäß EU-Standardvertragsklauseln

Datum 05.02.2026

ApptiveGrid GmbH

Brüsseler Platz 26

50674 Köln

verpflichtet sich als Auftragnehmer (nachfolgend **“Auftragnehmer”** oder **“Auftragsverarbeiter”** gegenüber dem Kunden (nachfolgend entweder als „**Kunde**“ oder „**Auftraggeber**“ bezeichnet)

nach Maßgabe der folgenden Bestimmungen:

1. Vertragsgegenstand

Dieser Vertrag zur Auftragsverarbeitung gemäß Art. 28 der EU Datenschutz-Grundverordnung (DSGVO) (nachfolgend „Vertrag“) konkretisiert die Verpflichtungen der Parteien zum Datenschutz, welche sich aus den zwischen den Parteien bereits bestehenden oder künftig abzuschließenden Verträgen (nachfolgend „Hauptvertrag“ (AGB)) ergeben, unter denen es zu einer Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Auftraggeber kommt. Er findet Anwendung auf alle Tätigkeiten, die mit dem Gegenstand des Auftrags (Ziffer 4) in Zusammenhang stehen und bei denen Beschäftigte des Auftragsverarbeiters oder durch den Auftragsverarbeiter Beauftragte, personenbezogene Daten des Verantwortlichen verarbeiten.

2. Anwendung der EU-Standardvertragsklauseln

2.1. Die Parteien legen diesem Vertrag in Anlage 1 die „Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter in der EU / im EWR“ gemäß dem Durchführungsbeschluss der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Abs. (7) DSGVO und Artikel 29 Abs. (7) der Verordnung (EU) 2018/1725 (nachfolgend „EU Standardvertragsklauseln“) zugrunde.

2.2. Dabei vereinbaren die Parteien folgende in den EU-Standardvertragsklauseln aufgeführten Optionen:

- Klausel 1: Option 1
- Klausel 7.7. a): Option 2, Zeitraum: 30 Tage (siehe Anlage 5 Ziffer 2)
- Klausel 8.c) 4: Option 1
- Klausel 9.1.b): Option 1
- Klausel 9.1.c): Option 1
- Klausel 9.2.c): Option 1

Die Klauseln 2 und 4 der EU Standardvertragsklauseln finden keine Anwendung.

3. Abweichungen von den EU-Standardvertragsklauseln

Die Parteien vereinbaren in Anlage 5 zusätzliche Regelungen zu den EU-Standardvertragsklauseln.

4. Gegenstand des Auftrags

Gegenstand der Verarbeitung ist die Bereitstellung der im Hauptvertrag/AGB bezeichneten Leistungen durch den Auftragsverarbeiter für den Auftraggeber.

Der Auftragsverarbeiter stellt eine No-Code Digitalisierungsplattform zur Verfügung, die branchenübergreifend die Abbildung und Digitalisierung von Geschäftsprozessen ermöglicht.

Der Auftragsverarbeiter stellt hierfür eine cloudbasierte Plattform in Form eines Spreadsheets zur Verfügung, das über verschiedene Ansichten (z.B. Kalender, Kanban, Map) organisiert und bearbeitet werden kann. Über digitale Formulare können Daten in das Spreadsheet eingegeben, verarbeitet und verwaltet werden. Darüber hinaus bietet Auftragsverarbeiter die Möglichkeit, Prozesse zu automatisieren und Schnittstellen zu Anwendungen Dritter zu erstellen.

5. Dauer des Auftrags

Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags/AGB. Eine Kündigung des Hauptvertrags/AGB bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

6. Anlagenverzeichnis

- Anlage 1: EU-Standardvertragsklauseln (Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter in der EU / im EWR – Stand: 4. Juni 2021, Sprache: deutsch)
- Anlage 2: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen
- Anlage 3: Unterauftragsverarbeiter
- Anlage 4: Technische und organisatorische Maßnahmen gem. Art 32 DSGVO
- Anlage 5: Zusatzregelungen zu von den EU-Standardvertragsklauseln

Anlage 1: EU-Standardvertragsklauseln

(Stand 4. Juni 2021)

Siehe:

https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0915&from=DE

Anlage 2: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

1. Zweck und Art der Verarbeitung

ApptiveGrid ist eine No-Code Digitalisierungsplattform des Auftragsverarbeiters, die branchenübergreifend die Abbildung und Digitalisierung von Geschäftsprozessen ermöglicht.

Der Auftragsverarbeiter stellt hierfür eine cloudbasierte Plattform in Form eines Spreadsheets zur Verfügung, das über verschiedene Ansichten (z.B. Kalender, Kanban, Map) organisiert und bearbeitet werden kann. Über digitale Formulare können Daten in das Spreadsheet eingegeben, verarbeitet und verwaltet werden. Darüber hinaus bietet der Auftragsverarbeiter die Möglichkeit, Prozesse zu automatisieren sowie Schnittstellen zu Anwendungen Dritter zu erstellen.

2. Kategorien von Daten

Die von der Verarbeitung betroffenen Kategorien von Daten hängen von der Nutzung der ApptiveGrid Dienstleisung durch den Auftraggeber ab. Als Gegenstand der Verarbeitung in Betracht kommende Kategorien von Daten sind:

Nutzer (mit ApptiveGrid Account)

- Email-Adresse
- Browser
- Betriebssystem
- Endgerät
- Anzahl der Seitenaufrufe
- Anzahl der Seitenbesuche
- Referrer
- Vorname
- Nachname
- Sprache
- Zeitzone

- Mediale Dateien, die der Nutzer in der Datenbank speichert
- Optionale Datenfelder und deren Werte, die der Nutzer in der Datenbank erstellt und eingibt
- IP-Adresse

Externer-Nutzer (Ohne ApptiveGrid Account)

- Sprache
- Zeitzone
- Werte die der Externe-Nutzer in ein Formular eingibt
- Mediale Dateien, die der Externe-Nutzer in ein Formular eingibt
- IP-Adresse

3. Kategorien betroffener Personen

Die von der Verarbeitung betroffenen Kategorien betroffener Personen hängen von der individuellen Nutzung der ApptiveGrid Dienstleistung durch den Auftraggeber ab. Als Kategorien betroffener Personen kommen dabei in Betracht:

- Nutzer (Kunden mit ApptiveGrid Account)
- Website-Besucher
- Interessenten
- Externe-Nutzer (Nutzung ohne ApptiveGrid Account)

Anlage 3: Unterauftragsverarbeiter

Der Kunde hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

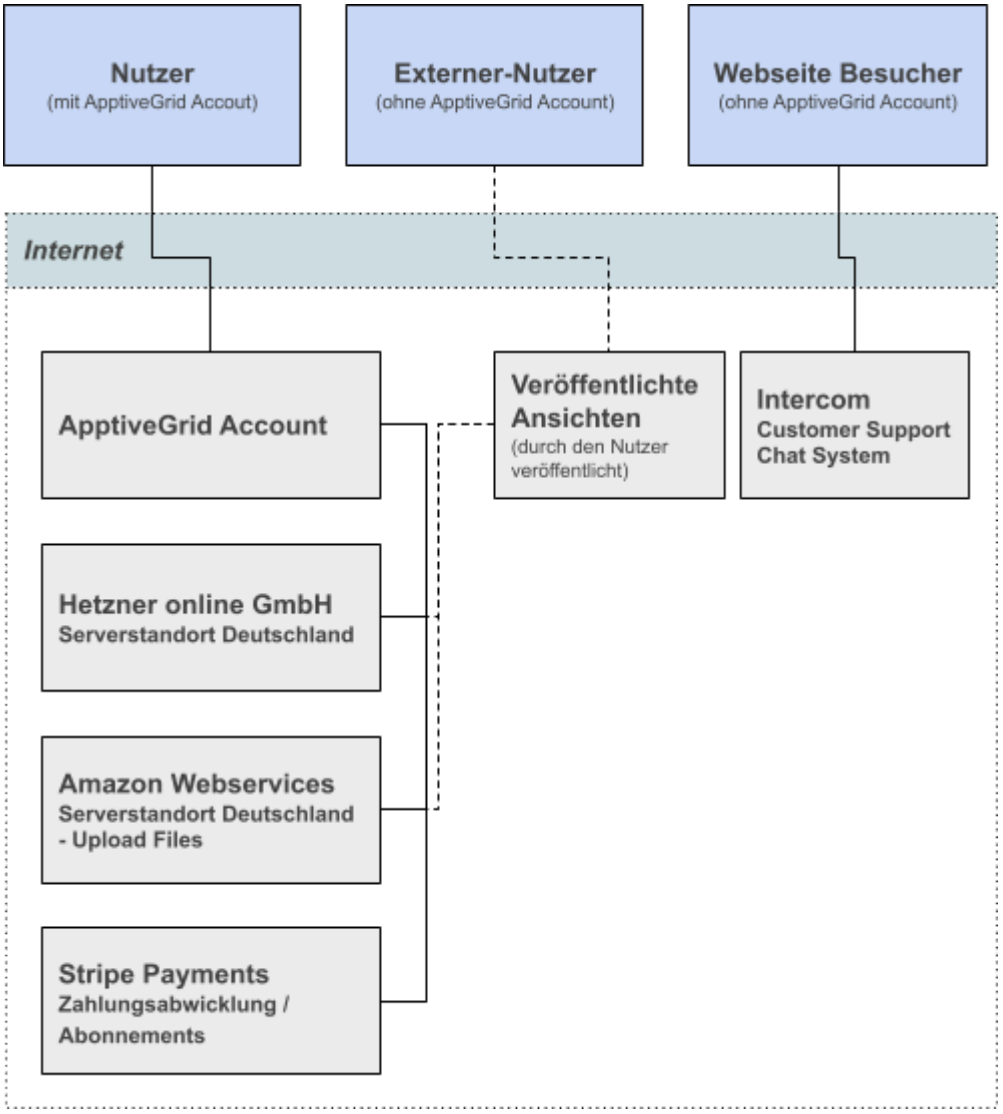
Dienstleister	**Erläuterung und Zweck**	**Funktion, in deren Rahmen der Einsatz stattfindet**	**Serverstandort**	**Rechtsgrundlage für etwaige Drittstaatentransfers**
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland	Hosting der Server Speicherung der Daten Verarbeitete Daten: Siehe Anlage 1, Ziffer 2	Systemimmanent	Deutschland	-
Stripe Payments Europe, Ltd. 1 Grand Canal Street Lower Grand Canal Dock Dublin 2, Irland	Zahlungsabwicklung, Abonnementverwaltung, Rechnungsstellung, Betrugsprävention	Systemimmanent	EU (Irland)	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c DSGVO)
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxemburg	**S3:** Angebot des File Uploads. Erweiterung und Verbesserung de Kerndienstleistung. - IP-Adresse - Browser - Betriebssystem - Zeitstempel - Referrer - User Profil-Bilder - File Upload Attachment Type	Optional	Deutschland	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO)
Intercom, Inc., a Delaware corporation with offices at 55 2nd Street, 4th Fl., San Francisco, CA 94105, USA	Chat- Kommunikation, Software-Anleitung und Dokumentation Nutzerverwaltung	Optional nur im Webauftritt von Apptivegrid.de nicht in der Software	USA	Art. 45 DSGVO (EU-US Data Privacy Framework)
Mailchimp The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA	E-Mail-Benachrichtigungen	Optional	USA	Art. 45 DSGVO (EU-US Data Privacy Framework)

Anlage 4: Technische und organisatorische Maßnahmen 2025 gemäß Art. 32 DSGVO

Zum Zeitpunkt des Vertragsschlusses hat ApptiveGrid die nachfolgend dargestellten technisch-organisatorischen Maßnahmen implementiert:

1. Datenflussdiagramm

Auf dem nachfolgenden Chart ist der grobe Datenfluss dargestellt:



2. Organisationskontrolle

Sollvorgabe: Das Personal des Auftragnehmers ist auf das Datengeheimnis und die Einhaltung der Verschwiegenheitsvorschriften zu verpflichten. Die Tatsache der Verpflichtung sollte zum Zweck eines jederzeitigen Nachweises in der Personalakte dokumentiert werden.

Entsprechende Unterlagen sind in der Personalakte hinterlegt.

- Textbaustein ist im Standardvertrag für alle Mitarbeiter hinterlegt.
- Mitarbeiter werden nochmals in internen Schulungen darauf hingewiesen.

3. Zutrittskontrolle

Sollvorgabe: Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (wobei der Begriff räumlich zu verstehen ist). Der Auftragnehmer hat zu diesem Zweck ein Zutrittskontrollsystem zu installieren.

Beschreibung der Zutrittskontrollsysteme im Büro (inklusive der physischen Schutzvorkehrungen):

- mechanische Schließanlage Haupteingang sowie Büroeingänge

4. Zugangskontrolle

Sollvorgabe: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Zu diesem Zweck muss der Zugang zu den DV-Anlagen kontrolliert und protokolliert werden (z. B. Anmelden in System,unerlaubtes Hochfahren und Eindringen in DV- System verhindern). Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Beschreibung der implementierten Authentifizierungsmechanismen (z.B. Passwortkomplexität, Wechselzyklen, SSH Keys):

- SSH: personalisierte Public Private Keys
- Wartungsarbeiten: OpenVPN (Zertifikate) S2S Kommunikation: IPSec
- C2S (Client to Server) Kommunikation: TLS 1.3 und TLS 1.2

Beschreibung der Maßnahmen bei temporärer Inaktivität der Nutzer (z.B. Mitarbeiter verlässt den Arbeitsplatz):

- Beim MacOS X System sind Hot Corners konfiguriert, sodass die Maus in eine Ecke geschoben wird, um den Bildschirm schnell zu sperren. Andernfalls sperrt sich der Monitor nach 5 Minuten.
- Alle MA werden aufgerufen, Bildschirme immer zu sperren.

Beschreibung der technischen Schutzmaßnahmen für Ihre Netzwerkumgebung:

- iptables-Regeln auf externen Schnittstelle
- Dienste lauschen nur auf internen Netzen
- wöchentliche nmap-Scans
- tägliches Monitoring mit Grafana
- tägliches Audit neuer kritischer Fehler
- Anti-DDoS im Datencenter Hetzner online GmbH
- OpenVPN-Tunnel zu internen Diensten

5. Zugriffskontrolle

Sollvorgabe: Es ist zu gewährleisten, dass die zur Nutzung 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.

Personenbezogene Daten müssen bei persistenter Speicherung verschlüsselt werden.

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

Beschreibung der Verhinderung unerlaubter Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen (Rollen und Berechtigungen nach dem Need-to-Know Prinzip):

- Rechte- und Rollenmanagement
- Technisches Onboarding und Offboarding von Mitarbeitern
- Zugänge und Rechtevergabe nur nach Erforderlichkeit

Beschreibung der Maßnahmen gegen unzulässige Zugriffe (z. B. Brute Force, SQL Injection, Login Validierung):

- SSH: fail2ban
- Alle kritischen Endpunkte werden mit Rate Limits gegen Brute Force Angriffe geschützt
- Zugänge für AptiveGrid Mitarbeiter sind durch eine 2-Faktor Authentifizierung zusätzlich geschützt.

Beschreibung der Sicherstellung, dass ausschließlich personifizierte Benutzerkonten für den Zugriff auf die Systeme genutzt werden (ein Konto je Benutzer):

- personalisierter Produkt/Backend-Account je Nutzer.
- personalisierter Benutzer-Account auf einem Computer

Beschreibung der implementierten Verlüsselungsmaßnahmen der personenbezogenen Daten:

- Transportverschlüsselung mit TLS 1.3 und 1.2
- IPSec
- OpenVPN
- SSH-Sicherungen: GPG

5.1. Weitergabekontrolle

Sollvorgabe: Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft

und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Personenbezogene Daten sind nur verschlüsselt (Transportverschlüsselung).

Beschreibung der Transportverschlüsselung:

- Transportverschlüsselung mit TLS 1.3 und 1.2 IPSec zu übertragen
- OpenVPN
- SSH

Beschreibung der Protokollierung der Weitergabe von personenbezogenen Daten:

- Nicht anwendbar. Personenbezogene Daten werden nicht von Servern heruntergeladen oder weitergegeben. Ausnahme Sicherungen. Sicherungen werden protokolliert und verschlüsselt. Täglich manuell geprüft.

Beschreibung der Transportsicherung bei einem physikalischen Transport:

- Nicht anwendbar. Personenbezogene Daten werden nicht von Servern physikalisch transportiert.

5.2. Eingabekontrolle

Sollvorgabe: Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Ein detailliertes Logging System über die Eingabe, Veränderung oder Löschung von personenbezogenen Daten (z. B. Logdateien) ist zu implementieren und regelmäßig auszuwerten.

Beschreibung der Logging / Monitoringsystem zur Überwachung der Zugriffe:

- Auf der Ebene von Servern werden diverse Protokolle mitgeschrieben, die durch das Anmelden von Mitarbeitern bei Wartungsarbeiten erstellt werden. Diese Protokolle werden stichprobenartig kontrolliert.
- Weiterhin werden diverse Protokolle generiert, die den technischen Zustand des Systems darstellen.

5.3. Verfügbarkeitskontrolle

Sollvorgabe: Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beschreibung des Datensicherungskonzepts (z. B. Back-Up Verfahren, Redundanzen, USV, Notfallpläne):

- USVs und Dieselgeneratoren an allen Datencenter-Standorten gespiegelte Festplatten
- Enterprise-Festplatten
- Replizierte Services: Alle Services und Daten sind 3-fach vorhanden
- Autofailover für Webnodes
- Automatisiertes Monitoring
- tägliche Backups aller Daten
- Backups an 2 verschiedenen Orten
- mehrere Mitarbeiter, die Prozess beherrschen

5.4. Trennungsgebot

Sollvorgaben: Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. Der Auftragnehmer sorgt für eine nachweislich logische Trennung der Daten des Mandanten, d.h. Daten verschiedener Auftraggeber sind getrennt zu verarbeiten. Gegenseitiger Zugriff ist auszuschließen. Ebenso werden die Daten nur zweckgebunden verarbeitet.

Beschreibung der Umsetzung zur Mandantenfähigkeit:

- Daten werden zweckgebunden verarbeitet. Jeder Nutzer besitzt eine individualisierte Datenbank-Instanz, die getrennt von anderen ist

Beschreibung der Sicherstellung der Trennung von Entwicklung-, Test- und Produktivsystemen:

Physikalische Trennung (verschiedene Server) in 3 Umgebungen:

- Development
- Staging
- Produktion

5.5. Informationssicherheit

Beschreibung des Informationssicherheitsmanagementsystems (ISMS):

Diverse Prozesse:

- IT-Sicherheitsprozess
  - Input: Scans, Meldungen, Protokolle
  - Verarbeitung: Bewertung
  - Output: Maßnahmen
  - Tools: nmap, rkhunter, maldet
- ● Verantwortung:
  - IT-Security: security@apptivegrid.de
  - Datenschutz: privacy@apptivegrid.de
- ● Regelmäßige Schulungen
  - IT Security
  - Datenschutz
  - Feste Prozesse
  - Onboarding
  - Offboarding
- Rechte und Rollenmanagement

5.6. Sonstiges

Beschreibung der Sicherstellung der vertraulichen Aufbewahrung sowie der Löschung oder Vernichtung von Test- und Ausschussmaterialen mit personenbezogenen Daten (z. B. Papier):

- Nicht anwendbar. Da keine Nutzung von Papier. Ausnahme Buchhaltung, sowie Verträge. Dokumente werden geschreddert.
- Festplatten werden grundsätzlich immer verschlüsselt und vor Abgabe mehrfach überschrieben.

6. Einsatz von Unterauftragnehmern

Die von uns eingesetzten weiteren Auftragsverarbeiter jeweils zum Zeitpunkt des Abschlusses dieser Vereinbarung implementierten technischen und organisatorischen Maßnahmen sind auf Anfrage zu erhalten. Wir versichern uns in regelmäßigen Abständen von der Angemessenheit und Wirksamkeit der von unseren Unterauftragnehmern getroffenen Maßnahmen.

7. Versicherung des Auftragnehmers

Der Auftragnehmer garantiert, dass alle in diesem Dokument genannten Angaben der Wahrheit entsprechen.

Anlage 5: Zusatzregelungen zu den EU-Standardvertragsklauseln

Die Parteien vereinbaren folgende Zusatzregelungen zu den EU-Standardvertragsklauseln (Anlage 1):

1. Dokumentation und Einhaltung der Klauseln (Klausel 7.6)

Zusätzlich zu Klausel 7.6 der EU-Standardvertragsklauseln gelten die folgenden Regelungen:

Der Verantwortliche ist berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 10 bis 18 Uhr) nach rechtzeitiger Vorankündigung die Geschäftsräume des Auftragsverarbeiters zu betreten. Der Zutritt hat ohne Störung des Betriebsablaufs und unter strikter Wahrung der Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters zu erfolgen.

2. Einsatz von Unterauftragsverarbeitern (Klausel 7.7)

Zusätzlich zu Klausel 7.7. a) der EU-Standardvertragsklauseln gelten die folgenden Regelungen:

ApptiveGrid wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter in elektronischem Format mit einer Frist von 30 Tagen informieren. In Ausnahmefällen, beispielsweise wenn die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter aus Gründen akuter Vorkommnisse im Bereich der IT-Sicherheit geboten erscheint, ist es ApptiveGrid gestattet, den Auftraggeber über beabsichtigte Änderungen mit einer Frist von 5 Werktagen zu informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus berechtigtem Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Werktagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist ApptiveGrid berechtigt, den Hauptvertrag (AGB) und diesen

Vertrag zum nach dem Hauptvertrag (AGB) nächstmöglichen Zeitpunkt zu kündigen.