Vertrag über die Verarbeitung

personenbezogener Daten und zur Wahrung der Verschwiegenheit

(„Auftragsdatenverarbeitungsvertrag“)

zwischen

_____

Name & Adresse des gekartel -Partners

(Auftraggeber)

und

gekartel AG

Berliner Strasse 11

01067 Dresden

(Auftragsverarbeiter oder Auftragnehmer)

- gemeinsam nachfolgend einzeln oder gemeinsam auch „Parteien“ genannt -

1. **Grundlage der Verarbeitung**
   Der Auftragsverarbeiter kommt im Rahmen seiner vertraglichen Tätigkeit für den Auftraggeber möglicherweise mit personenbezogenen Daten in Kontakt. Der Auftragsverarbeiter verpflichtet sich hiermit zur Beachtung des Datenschutzes, insbesondere zur Wahrung der Vertraulichkeit.

2. **Gegenstand und Dauer der Verarbeitung**
   Gegenstand der Verarbeitung sind Dienstleistungen zur Informationsübermittlung und zu interaktiven Diensten über die Digitale Haustafel. Die Dauer der Verarbeitung beschränkt sich auf die Dauer der vertraglichen Beauftragung des Auftragnehmers durch den Auftraggeber.

3. Art und Zweck der Verarbeitung

Der Zweck der Verarbeitung gründet sich auf den Dienstleistungsvertrag zwischen den Parteien und kann je nach Vertragsumfang folgende Punkte umfassen:

- Darstellung und Verwaltung von Informationen (auch personenbezogenen Daten) auf den vom Auftraggeber erworbenen, gemieteten, geleasten oder im Rahmen eines Testbetriebes zur Verfügung gestellten Digitalen Haustafeln
- Management von Dienstleistern (z.B. Reinigungsfirma) über Eingabemöglichkeiten an der Digitalen Haustafel

Der Auftragnehmer stellt hierfür geeignete Hard- und Softwareplattformen zur Verfügung und stellt deren Betrieb sicher.

4. Art der personenbezogenen Daten und Kategorien betroffener Personen

- Name, Telefonnummer, Fotos von Mitarbeitern des Auftraggebers
- Login-Daten, Ort und Zeit des Logins, Texteingabe durch Dienstleister, die im Auftrag des Auftraggebers die Digitale Haustafel nutzen

5. Benennung einer/s Datenschutzbeauftragten

Der Auftragnehmer ist nach § 38 Abs. 1 BDSG nicht zur Bestellung einer/s Datenschutzbeauftragten verpflichtet. Ein/e Datenschutzbeauftragte/r muss benannt werden, wenn in der Regel mindestens 20 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind. Sollte die Benennung einer Datenschutzbeauftragten beim Auftragnehmer erforderlich werden, wird der Auftragnehmer dies umgehend tun und dem Auftraggeber Name und Kontaktdaten mitteilen.

6. Rechte und Pflichten des Auftraggebers

a) Der Auftraggeber ist dafür verantwortlich, dass die Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten nach Art. 6 DSGVO gewährleistet ist, insbesondere dass eine Einwilligung der betroffenen Personen schriftlich vorliegt und sie über ihre Rechte informiert wurden.

b) Bei der Erfassung von vor Ort erbrachten Serviceleistungen am Gerät ist es nicht gestattet, Namen natürlicher Personen, auch nicht Namensteile wie Vorname und/oder Nachname zu verwenden. Für diese Anwendungsfälle sind ausschließlich Firmenbezeichnungen oder Pseudonyme zu verwenden. Die Zuordnung der Pseudonyme zu den entsprechenden natürlichen Personen darf nicht im gekartel CMS erfasst werden.

c) Die Übermittlung personenbezogener Daten an den Auftragsverarbeiter durch den Auftraggeber erfolgt verschlüsselt per E-Mail oder auf einem anderen sicheren Weg z.B. als passwortgesichertes ZIP-Archiv.

d) Der Auftraggeber ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen (siehe Anhang) zu überzeugen.

e) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

7. Pflichten des Auftragnehmers

a) Die Verpflichtung des Auftragnehmers zur Einhaltung des Datenschutzes nach DSGVO, insbesondere zur Wahrung der Vertraulichkeit besteht umfassend. Es ist dem Auftragsverarbeiter untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zu unbefugter Offenlegung oder unbefugtem Zugang

führt. Es ist dem Auftragsverarbeiter nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der ihm durch den Auftraggeber übertragenen Aufgaben erforderlich ist.

b) Soweit die Mitarbeiter des Auftragsverarbeiters und/oder etwaige Erfüllungsgehilfen, insbesondere auch Subunternehmen, im Rahmen der Geschäftsbeziehungen mit der Verarbeitung von personenbezogenen Daten betraut werden müssen, sind ihnen die gleichen Verpflichtungen aufzuerlegen. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und sie auf das Datengeheimnis schriftlich verpflichtet.
c) Eine Übermittlung oder Verarbeitung personenbezogener Daten außerhalb der EU bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Dies gilt auch für den Einsatz von IT in entsprechenden Drittländern.
d) Der Auftragsverarbeiter verpflichtet sich, diejenigen technischen und organisatorischen Maßnahmen zu treffen und aufrecht zu erhalten, die erforderlich sind, um die Anforderungen gemäß Art. 32 DSGVO zu gewährleisten (siehe Anlage 2).
e) Datenschutzverletzungen, auch begründete Verdachtsfälle, sind beim Auftraggeber anzuzeigen. Dabei sind mindestens die Angaben gemäß Art. 33 DSGVO bekannt zu geben.
f) Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber bei der Durchführung der Datenschutzbestimmungen zu unterstützen, dies beinhaltet auch die stichprobenartige Kontrolle der technischen und organisatorischen Maßnahmen.
g) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer nach Wahl des Auftraggebers sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

8. Subunternehmen

Die Auftragsverarbeitung erfolgt grundsätzlich und ausschließlich innerhalb der EU, bevorzugt in Deutschland. Der Auftragnehmer versichert, dass er etwaige Subunternehmen unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen und unter Verpflichtung auf die Vorschriften der DSGVO sorgfältig auswählt. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. Insbesondere muss der Auftraggeber berechtigt sein, Kontrollen vor Ort beim Subunternehmer durchzuführen oder durch Dritte durchführen zu lassen.

Subunternehmer sind in der Anlage 1 mit Namen, Anschrift und Auftragsinhalt bezeichnet und mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

9. Widerspruchsrecht

Der Auftraggeber kann der Verarbeitung personenbezogener Daten jederzeit widersprechen oder diese einschränken. Der Auftragsverarbeiter hat personenbezogene Daten zu berichtigen, zu löschen und zu sperren, wenn der Auftraggeber es verlangt. Dies kann Auswirkungen auf die Erbringung der vertraglich festgelegten Dienstleistungen haben und unter Umständen dazu führen, dass diese ganz oder teilweise nicht erbracht werden können.

10. Datenschutzverstöße

Unter Geltung der DSGVO können Verstöße gegen Datenschutzbestimmungen nach § 42 DSAnpU_G-EU (BDSG-neu) sowie nach anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden.

Datenschutzverstöße können zugleich eine Verletzung zivilrechtlicher Pflichten bedeuten und entsprechende Konsequenzen haben.

11. Anlagen

Dieser Vertrag enthält folgende Anlagen, die verbindlicher Vertragsbestandteil sind.

- Anlage 1 zu Unterauftragnehmern (IT-Dienstleister)
- Anlage 2 zu den technischen und organisatorischen Maßnahmen laut Art. 32 DSGVO

Je nach Erfordernis können die Vertragsparteien weitere Anlagen als Bestandteil dieses Vertrages aufnehmen.

12. Schlussbestimmungen

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

_____

Ort, Datum Unterschrift Auftraggeber

_____

Ort, Datum Unterschrift Auftragnehmer

gekartel AG

Anlage 1

Beauftragte IT-Dienstleister (Subunternehmer) nach Art. 28 DSGVO

V2.0

Hetzner Online GmbH

Industriestr. 25
91710 Gunzenhausen, Deutschland
Tel.: +49 (0)9831 505-0
E-Mail: info@hetzner.com

RZ-Standort

Rechenzentrum Nürnberg, Sigmundstraße 135, DE-90431 Nürnberg

ISO 27001-Zertifikat

https://www.hetzner.com/pdf/FOX_Zertifikat.pdf

Auftragsinhalt

- Anmietung eines oder mehrerer eigener gesicherter Server, insbesondere von Rechenleistung und Speicherplatz, in einem von der Hetzner Online GmbH betriebenen, zertifizierten Rechenzentrum in der Europäischen Union
- gesicherter Remote-Zugang zum oder zu den Servern ausschließlich für die gekartel AG
- umfangreiche Sicherheitsleistungen nach dem neusten Stand der Technik siehe Auflistung technisch-organisatorischer Maßnahmen der Hetzner Online GmbH

Technische und organisatorische Maßnahmen der Hetzner Online GmbH nach Art. 32 DSGVO

https://www.hetzner.com/AV/TOM.pdf

gekartel AG

Anlage 2

Technische und organisatorische Maßnahmen nach Art. 5 DSGVO

V1.2

Es folgt eine Beschreibung der technischen und organisatorischen Maßnahmen, die getroffen werden, um die Bestimmungen der DSGVO und das BDSG (inkl. Neufassung) im Unternehmen einzuhalten.

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

1. Alarmanlage und Schließanlage

   - Alarmanlage mit verschiedenen Sicherheitsbereichen
   - Personalisierte Tokens zur Zutrittskontrolle
   - Pseudonymisierte Erfassung in der Alarmanlage

   Die Geschäftsräume sind nach den offiziellen Öffnungszeiten standardmäßig verschlossen. In der Zeit zwischen 20:00 Uhr und 07:00 Uhr sowie am Wochenende und Feiertagen ist der Zugang zu den Geschäftsräumen nur in Absprache mit einem Sicherheitsdienst möglich.

2. Transponder-Schließsystem
3. Bewegungsmelder und Fenster- /Türkontakte die bei Scharfschaltung der Alarmanlage aktiviert werden
4. Schlüsselregelung (Schlüsselausgabe etc.)
   Übergabeprotokoll Schlüsselausgabe und Ablage in der Personalakte
5. Besucherregelung:

   Besucher der gekartel AG werden persönlich am Eingang in Empfang genommen und in einen Besprechungsraum geleitet. Die Besprechungsräume verfügen über gesicherte Datendosen, zudem sind die Räume einsehbar. Der oder die Ansprechpartner sind angehalten den Besucher zeitnah zu begrüßen. Sollten der oder die Ansprechpartner nicht unmittelbar Zeit haben, sind die Mitarbeiter der gekartel AG angewiesen, den oder die Besucher regelmäßig aufzusuchen. Die Mitarbeiter sind zudem angewiesen, unternehmensfremde Personen, die sich allein in den Geschäftsräumen der gekartel AG bewegen oder aufhalten, anzusprechen. Ebenso werden Fremdfirmen, die sich in den Geschäftsräumen der gekartel AG aufhalten, regelmäßig kontrolliert.

6. Sorgfältige Auswahl von Reinigungspersonal
7. Sorgfältige Auswahl von Wachpersonal

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

1. Zuordnung von Benutzerrechten
   Einteilung von Benutzergruppen
2. Physische Trennung des Verarbeitungssystems für Personaldaten und Geschäftspläne von anderen betrieblichen Systemen.
3. Passwortvergabe
   Passwortregelung für Exchange und Sharepoint (Art des Passwortes und Änderung aller 3 Monate)
4. Einsatz von VPN-Technologie für Home-Office für ausgewählte Personen auf firmeneigenen Endgeräten
5. Keine Nutzung privater Endgeräte im Büro und im Home-Office
6. Besucherregelung für Zugang zum Internet
   Nutzung eines separaten WLAN Gastzuganges, der über einen separaten unabhängigen DSL-Anschluss realisiert wird.
7. Verschlüsselung von mobilen Datenträgern
   Notebooks für Gebrauch außerhalb der Büroräume haben folgende Sicherheitsmerkmale:
   - Verschlüsselter Container (VeraCrypt) in welchem alle Outlook- und Firmendaten gespeichert werden
   - Backupfestplatten für Lagerung außerhalb der Firmenräume sind verschlüsselt
8. Verschlüsselung von Smartphone-Inhalten für Firmenhandys aktiviert
9. Einsatz von Anti-Viren-Software
10. Einsatz einer Hardware-Firewall als Bestandteil des Internet-Routers
    Alle Ports von außen geschlossen.
11. Keine Dienste verfügbar, die von außen über das Internet erreichbar sind. Alle Dienste die von außen erreichbar sein müssen (Bsp: Webseite und CMS digitale Haustafel) liegen bei einem zertifizierten in Rechenzentrum innerhalb der EU.
12. Einsatz einer Software-Firewall als Bestandteil des Betriebssystems
13. Keine Verbindung von privaten mobilen Endgeräten mit dem Firmennetzwerk gestattet, regelmäßige Überprüfung der Login-Vorgänge.

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssysteme 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.

1. Dokumentiertes Berechtigungssystem für Zugänge zu digitalen und analogen Dokumenten
2. Rechtevergabe durch ausgewählte Personen
3. Anzahl der Administratoren auf das „Notwendigste“ reduziert
4. Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel für Sharepoint und Exchange-Server
5. physische Löschung von Datenträgern vor Wiederverwendung bei mobilen Endgeräten
6. ordnungsgemäße Vernichtung von Datenträgern von Endgeräten auf welchen personenbezogene Daten verarbeitet wurden durch IT Abteilung
7. Einsatz von Aktenvernichtern

4. Weitergabekontrolle

Maßnahmen, die 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.

1. Einrichtung von VPN-Tunneln für Home-office Anwendungen (Anzahl der Personen auf das Notwendigste begrenzt)
2. Arbeit im Home-Office ausschließlich auf firmeneigenen Endgeräten
3. Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bei Auswertungen
4. E-Mail-Verschlüsselung von pbD
5. Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
6. Verschlüsselung während des Transportes

5. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

1. Abschluss von AV-Verträgen mit allen Dienstleistern / Kunden / Partnern und weiteren natürlichen oder juristischen Personen die im Auftrag der gekartel AG Daten verarbeiten.
2. Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit z.B. zertifizierte Dienstleister)
3. Verpflichtung der Auftragnehmer auf die EU-DSGVO und das BDSG-neu
4. Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
5. Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart

6.Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträgliche überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

1. Sensible Daten, wie Personaldaten, Lohn- und Gehaltsabrechnungen, Krankmeldungen werden von externen Dienstleistern (Lohn- bzw. Steuerbüro) verarbeitet. (siehe AV-Verträge)

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten. dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

1. Schutzsteckdosenleisten in Serverräumen
2. Feuer- und Rauchmeldeanlagen
3. Feuerlöschgeräte am Serverräumen
4. Backup- & Recoverykonzept
5. Testen von Datenwiederherstellung
6. Aufbewahrung von Datensicherung an einem sicheren ausgelagerten Ort
7. Auslagerung von Serverdiensten an einen professionellen Dienstleister in Deutschland

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Typische Maßnahmen (nur Stichworte) sind z.B.:

1. Vertragliche Vereinbarung mit Kunden z.B. Wohnungsgenossenschaften zur Pseudonymisierung z.B. von Reinigungspersonal
2. physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
3. Berechtigungskonzept
4. Trennung von Produktiv- und Testsystem