Auftragsverarbeitungsvertrag nach Art 28 DSGVO

(Verantwortlicher)

nachstehend „Verantwortlicher" genannt

einerseits

und

andererseits

wie folgt:

Behires Services GmbH
Leopold-Ungar-Platz 2/2
Wien (Vienna), 1190, Austria

(Auftragsverarbeiter)

nachstehend „Auftragsverarbeiter" genannt

1. Gegenstand der Vereinbarung

1.1 Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben: Ermöglichung der Nutzung von Produkten und Dienstleistungen des AV, dies betrifft insbesondere die Nutzung der klassischen Visitenkarte in digitaler Form, der digitalen Visitenkarte, samt dazugehörigen Verwaltungsportalen und die Herstellung und Produktion von personalisierten Hardwarekomponenten.

1.2 Diese Vereinbarung ist als Ergänzung zu unserer Datenschutzerklärung und unseren allgemeinen Geschäftsbedingungen zu verstehen.

1.3 Folgende Arten von personenbezogenen Daten werden verarbeitet:

Für die Nutzung unserer Dienstleistungen und für das Portal für die Verwaltung der digitalen Visitenkarten, werden folgende Daten verarbeitet: Profilbild, Kontaktdaten, Bestelldaten, Vertragsdaten, Verrechnungsdaten, Login-Zugriff, Browserdaten, Gerätedaten (Fingerprint & Betriebssystem), Land und Bundesland

Für die Nutzung der digitalen Visitenkarten werden folgende Daten verarbeitet, die jedoch dem Benutzer selbst überlassen sind, welche Daten er zur Verfügung stellen möchte: Profilbild, Kontaktdaten, Social-Media Daten

Um Statistiken und Auswertungen zu ermöglichen, werden zusätzlich folgende Daten bei jedem Aufruf der digitalen Visitenkarte erfasst: Zeitstempel, Browserdaten, Gerätedaten (Fingerprint & Betriebssystem), Land und Bundesland – IP-Adresse wird durch den Download des Kontaktes erfasst.

1.1 Folgende Kategorien betroffener Personen unterliegen der Verarbeitung: Kunden

1.2 Die Verarbeitung ist folgender Art: Erheben, Erfassen Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten

2. Dauer der Vereinbarung

2.1 Die Vereinbarung ist auf unbestimmte Zeit abgeschlossen und kann von beiden Parteien jederzeit, jedoch frühestens zum Monatsende, gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Pflichten und Rechte des Auftragsverarbeiters

3.1 Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen – zu verarbeiten, sofern er nicht hierzu rechtlich verpflichtet ist. In solch einem Fall teilt der Verarbeitung mit, sofern eine solche Mitteilung nicht rechtlich verboten ist.

3.2 Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht.

3.3 Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat.

3.4 Der Auftragsverarbeiter unterstützt angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen, damit der Verantwortliche seine Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person (zB Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Verantwortlichen alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragsverarbeiter gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Verantwortlichen der von ihm betriebenen Datenanwendung hält, hat der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiterzuleiten und dies dem Antragsteller mitzuteilen.

3.5 Der Auftragsverarbeiter unterstützt unter Berücksichtigung der Art der Vereinbarung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (zB Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

3.6 Der Auftragsverarbeiter hat für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten.

3.7 Dem Verantwortlichen wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen – die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen.

3.8 Der Auftragsverarbeiter ist nach Beendigung dieser Vereinbarung verpflichtet – sofern nicht eine rechtliche Verpflichtung zur Speicherung besteht – alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Verantwortlichen in dessen Auftrag zu vernichten.

3.9 Der Auftragsverarbeiter teilt dem Verantwortlichen unverzüglich Störungen, Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung des Verantwortlichen durchführen.

4. Ort der Durchführung der Datenverarbeitung

Sofern der Verantwortliche keine abweichende Angabe trifft, werden sämtliche Datenverarbeitungstätigkeiten standardmäßig innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums (EWR) durchgeführt.

5. Sub-Auftragsverarbeiter

5.1 Der Auftragsverarbeiter ist nicht berechtigt, einen Sub-Auftragsverarbeiter hinzuzuziehen - ausgenommen sind jedoch Punkt 5.2 und Produktionen von Hardwarekomponenten, wie Produktion von NFC oder Personalisierten physischen Visitenkarten nötig sind. Es werden nur die zwingend erforderlichen Kundenstammdaten and den Sub-Auftragsverarbeiter übermittelt. Der Sub-Auftragsverarbeiter richtet sich je nach Produkt und Komponente unterschiedlich und kann auf Nachfrage vom Verantwortlichen erläutert werden. Die Kundenstammdaten werden für maximal 1 Jahr bei Sub-Auftragsverarbeiter gespeichert.

5.2 Der Verantwortliche stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Name und Anschrift	**Auftragsinhalt**
Akamai Technologies GmbH Att.: Global Data Protection Officer 22 Parkring DE-85748 Garching	Bereitstellung der dedizierten Server nach ISO27001 Norm für die Datenverarbeitung und speicherung
Akamai Technologies GmbH Att.: Global Data Protection Officer 22 Parkring DE-85748 Garching	Bereitstellung der Bilder, von Dateien und Dokumenten, welche vom Verantwortlichen hochgeladen werden, nach ISO27001 Norm.
Laravel Holdings Inc. 60 Broad Street, 24th Floor #1559, New York, New York 10004, United States	Reporting und Verarbeitung von Fehlermeldungen welche bei der Nutzung entstehen.
Stripe, Inc. now known as Stripe, LLC 354 Oyster Point Boulevard South San Francisco, California, 94080, United States	Verarbeitung von Bezahlvorgängen und Speicherung von Zahlungsmethoden inkl. Speichern von Bankverbindungen für bestimmte Zahlungsmethoden (zB SEPA oder Überweisung)

5.3 *Absatz Gültig für verarbeitete Daten welche über die Domain business.becard.me erfolgen:* Der Verantwortliche Beauftragte nachfolgenden Unterauftragnehmer bis zum voraussichtlichen Stichtag 01. Mai 2026 unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Name und Anschrift	**Auftragsinhalt**
Hetzner Online GmbH Industriestraße 25 DE-91710 Gunzenhausen	Bereitstellung der dedizierten Server nach ISO27001 Norm für die Datenverarbeitung und speicherung

5.4 *Absatz Gültig für verarbeitete Daten bis zum genanten Stichtag:* Der Verantwortliche Beauftragte nachfolgenden Unterauftragnehmer bis zum Stichtag 30. März 2026 unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Name und Anschrift	**Auftragsinhalt**
Google Irland Ltd. Google Building Gordon House, 4 Barrow St, Grand Canal Dock, Dublin 4, D04 V4X7, Irland	Bereitstellung der Bilder, von Dateien und Dokumenten, welche vom Verantwortlichen hochgeladen werden, nach ISO27001 Norm.

6. Grundsätzliche Aufbewahrung der Daten

6.1 Alle personenbezogenen Daten welche bei der Registrierung und Verwendung auf/von becard.me und dazugehörigen Services und Produkten verarbeitet werden, werden höchstens zehn Jahre, nach der letzten Aktivität des Verantwortlichen, auf den Servern des Auftragsverarbeiter gespeichert – Voraussetzung es wurde kein Löschantrag durch den Verantwortlichen gestellt (siehe Punkt 4).

6.2 Folgende Daten werden in den jeweiligen Rechenzentren nach ISO27001 / ISO27017 / ISO27018 / SOC 1/2/3 / PCI DSS gespeichert:

Datentyp	**Serverstandort**	**Servertyp**
Personenbezogene Daten (Name, Adresse, Statistiken, etc.), STRING/TEXT Daten zur Verarbeitung (Log-Files, etc.)	Frankfurt o. Falkenstein, Deutschland	Cloud
PDF-, EXCEL Dokumente (Rechnungen, Bestellbestätigungen, Lieferscheine, etc.) und Bilder (Profilbilder, Firmenlogos, etc.)	Je nach Serverauswahl des Verantwortlichen werden Daten an den nächstgelegenen Standorten gespeichert in: -Paris, Frankreich -Washington, DC, USA -Osaka, Japan	Cloud
Sicherungen / Backups	Frankfurt, Deutschland	Cloud
API-Nutzungs-Reportings & Fehlermeldungen welche bei der Nutzung entstehen	Frankfurt, Deutschland	Cloud
Abonnements, Abrechnungseinstellungen, Zahlungsmethoden und Bankverbindungen	San Francisco, United States	Cloud

7. Sicherungsvorgänge / Backups

7.1 Alle Daten werden zweimal täglich gesichert und verschlüsselt aufbewahrt, davon erfolgt jeden Morgen zwischen 02.00 und 05.00 eine vollständige Sicherung aller Daten. Es werden immer die letzten sieben Tage gespeichert. Backups die älter als sieben Tage sind, werden automatisch vollständig gelöscht.

8. Löschvorgang

8.1 Der Löschvorgang tritt in Kraft durch die schriftliche Aufforderung des Verantwortlichen. Wenn keine steuerlich relevanten Daten verarbeitet wurden, werden alle Daten innerhalb von 48 Stunden an Werktagen (Österreich) gelöscht, ausgenommen Punkt 8.3.

8.2 Im Falle einer getätigten Bestellung innerhalb von becard.me und den damit verbundenen Services und Produkten, werden alle Daten lt. Punkt 8.1 gelöscht, ausgenommen Daten die für Rechnungswesen, Steuer- und Zollrecht nach § 132 Abs 1 BAO und § 11 Abs 2 3. Unterabsatz UstG, aufzubewahren sind. Diese Daten verjähren nach 7 Jahren und werden in diesem Zuge nachträglich gelöscht.

8.3 Der Löschvorgang kann aus technischen Möglichkeiten und aufgrund des außergewöhnlich hohen Aufwandes nicht in Backup-Sicherungen erfolgen. Siehe Löschvorgang von Backup-Sicherungen unter Punkt 3.1 – Im falle einer Wiederherstellung eines Backups siehe Punkt 8.4

8.4 Beim Löschantrag wird automatisch eine anonymisierte Identifikationsnummer mit der internen Identifikationsnummer des Verantwortlichen im separierten Backup-Server gespeichert. Diese dient für den Löschvorgang in Backup-Restaurierungen (Wiederherstellungen). Der genaue Ablauf wird unter Punkt 5.1 deklariert. Dieser Datensatz wird 8-Tage gespeichert.

9. Löschvorgang in Backup-Restaurierungen

9.1 Im Falle einer Backup-Restaurierung werden die Identifikationsnummern aus der Datenbank „Antrag für Löschung" (lt. Punkt 8.4) überprüft und automatisiert erneut aus dem aktuellen Backup-Restore entfernt. Somit kann sichergestellt werden, dass keine Daten im Umlauf sind, wo der Löschantrag bereits eingegangen ist.

10. Technische und organisatorische Maßnahmen

10.1 Der Auftragsverarbeiter hat die Sicherheit gem Art 28 Abs 3 lit c, 32 DSGVO insbesondere in Verbindung mit Art 5 Abs 1, Abs 2 DSGVO 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 Risi-kos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art 32 DSGVO zu berücksichtigen.

10.2 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und zuvor dem Verantwortlichen mitzuteilen.

10.3 Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art 32 Abs 1 lit d DS-GVO). Das Ergebnis ist dem Verantwortlichen mitzuteilen.

11. Berichtigung, Einschränkung und Löschung von Daten

11.1 Der Auftragsverarbeiter darf die Daten, die aufgrund dieses Vertrages verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

11.2 Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen.

12. Haftung und Schadenersatz

12.1 Verantwortlicher und Auftragsverarbeiter haften gegenüber betroffenen Personen entsprechend der in Art 82 DSGVO getroffenen Regelungen.

13. Sonstiges

13.1 Änderungen und Ergänzungen dieses Vertrages – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt.

13.2 Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit des Vertrages im Übrigen unberührt.

13.3 Es gilt österreichisches Recht.

14. DSG 2000, DSGVO, Datenschutz-Anpassungsgesetz 2018

14.1 Zum Zeitpunkt der Unterfertigung dieses Vertrages gelten nach wie vor die Bestimmungen des DSG 2000. Die Vertragsparteien vereinbaren allerdings bereits jetzt, dass der Auftragsverarbeiter mit Inkrafttreten der Datenschutz-Grundverordnung sowie des Datenschutz-Anpassungsgesetz 2018 die Verpflichtungen gemäß deren Bestimmungen vollumfänglich einzuhalten hat.

, am
Für den Verantwortlichen:

.....

Wien, am
Für den Auftragsverarbeiter:

.....

Anlage ./1 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit

1.1 Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:

☒ Schlüssel

☒ Magnet- oder Chipkarten

☐ Elektrische Türöffner

☒ Portier

☐ Sicherheitspersonal

☒ Alarmanlagen

☒ Videoanlage

☒ Einbruchshemmende Fenster und/oder Sicherheitstüren

☒ Anmeldung beim Empfang mit Personenkontrolle

☒ Begleitung von Besuchern im Unternehmensgebäude

☒ Tragen von Firmen-/Besucherausweisen

☐ Sonstiges:

1.2 Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch:

☒ Kennwörter (einschließlich entsprechender Policy)

☐ Verschlüsselung von Datenträgern

☒ Automatische Sperrmechanismen

☒ Sonstiges: Teilverschlüsselung von Datenträgern

☒ Zwei-Faktor-Authentifizierung

1.3 Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

☒ Standard-Berechtigungsprofile auf „need to know-Basis“

☐ Standardprozess für Berechtigungsvergabe

☒ Protokollierung von Zugriffen

☒ Sichere Aufbewahrung von Speichermedien

☒ Periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten

☒ Datenschutzgerechte Wiederverwendung von Datenträgern

☒ Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger

☐ Clear-Desk/Clear-Screen Policy

☐ Sonstiges:

1.4 Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.

☒ Ja ☐ Nein

1.5 Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

☒ Ja ☐ Nein

2. Datenintegrität

2.1 Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

☐ Verschlüsselung von Datenträgern

☒ Verschlüsselung von Dateien

☒ Virtual Private Networks (VPN)

☐ Elektronische Signatur

☐ Sonstiges:

2.2 Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:

☒ Protokollierung

☐ Dokumentenmanagement

☐ Sonstiges:

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

☒ Backup-Strategie (online/offline; on-site/off-site)

☒ Unterbrechungsfreie Stromversorgung (USV, Dieselaggregat)

☒ Virenschutz

☒ Firewall

☒ Meldewege und Notfallpläne

☒ Security Checks auf Infrastruktur- und Applikationsebene

☒ Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum

☐ Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern

☐ Sonstiges:

3.2 Rasche Wiederherstellbarkeit:

☒ Ja ☐ Nein

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen:

☒ Ja ☐ Nein

4.2 Incident-Response-Management:

☒ Ja ☐ Nein

4.3 Datenschutzfreundliche Voreinstellungen:

☒ Ja ☐ Nein

4.4 Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers durch:

☒ Eindeutige Vertragsgestaltung

☐ Formalisiertes Auftragsmanagement

☒ Strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS)

☐ Vorabüberzeugungspflicht

☒ Nachkontrollen

5. Sonstiges & Bemerkungen

Die Zertifizierungsprozesse ISO-27001, ISO27002 und ISO31000/ ISO27005 wurden angestoßen.