AUFTRAGSVERARBEITUNGSVERTRAG NACH ART. 28 DSGVO

zwischen dem Verantwortlichen

– nachfolgend „Auftraggeber“ genannt

und dem Auftragsverarbeiter

bchic UG (haftungsbeschränkt), Ilsensteinweg 37A, 14129 Berlin – nachfolgend „Auftragnehmer“ genannt

nachfolgend zusammen die „Parteien“ genannt

PRÄAMBEL

Für diesen Auftragsverarbeitungsvertrag gelten die Begriffe und Definitionen der Verordnung (EU) 2016/679 (nachfolgend „DSGVO“), insbesondere des Art. 4 DSGVO.

1. GEGENSTAND

1.1 Gegenstand dieses Auftragsverarbeitungsvertrages ist die Festlegung des datenschutzrechtlichen Rahmens für die vertraglichen Beziehungen zwischen den Parteien.

1.2 Die Beschreibung des jeweiligen Auftrags mit den Angaben über Gegenstand des Auftrags, Umfang, Art und Zweck der Datenverarbeitung, Art der personenbezogenen Daten sowie Kategorien der betroffenen Personen befindet sich in der Anlage unter der Ziffer 1.

2. ORT DER DATENVERARBEITUNG Die vertraglich vereinbarte Verarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den

DATA PROCESSING AGREEMENT PURSUANT TO ART. 28 GDPR

between the Controller

– hereinafter referred to as "Controller"

and the Processor

bchic UG (haftungsbeschränkt), Ilsensteinweg 37A, 14129 Berlin – hereinafter referred to as "Processor"

hereinafter collectively referred to as the "Parties"

PREAMBLE

For this Data Processing Agreement, the terms and definitions of Regulation (EU) 2016/679 (hereinafter "GDPR") apply, in particular those of Art. 4 GDPR.

1. SUBJECT MATTER

1.1 The subject matter of this Data Processing Agreement is the establishment of the data protection framework for the contractual relationships between the Parties.

1.2 The description of the respective order, including details on the subject matter, scope, nature and purpose of data processing, type of personal data, and categories of data subjects, can be found in the Annex under Section 1.

2. LOCATION OF DATA PROCESSING The contractually agreed processing shall take place exclusively in a Member State of the European Union or in another Contracting State to the Agreement on the European

Europäischen Wirtschaftsraum statt, sofern sich aus der Anlage nichts Anderes ergibt. Jede Verlagerung der Verarbeitung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers in schriftlicher Form und darf nur erfolgen, wenn die besonderen Voraussetzungen für die Übermittlung in ein Drittland nach Art. 44 ff. DSGVO erfüllt sind.

Economic Area, unless otherwise specified in the Annex. Any transfer of processing to a third country requires the prior written consent of the Controller and may only take place if the special requirements for transfer to a third country pursuant to Art. 44 et seq. GDPR are met.

3. LAUFZEIT

3.1 Die Laufzeit dieses Vertrages richtet sich nach der Dauer des in der Anlage beschriebenen Auftrags (Hauptvertrag).

3.2 Der Auftraggeber kann diesen Vertrag ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

3. DURATION

3.1 The term of this Agreement depends on the duration of the order described in the Annex (Main Agreement).

3.2 The Controller may terminate this Agreement without notice if the Processor commits a serious breach of data protection regulations or the provisions of this Agreement. In particular, non-compliance with the obligations agreed in this Agreement and derived from Art. 28 GDPR constitutes a serious breach.

4. WEISUNG

4.1 Der Auftragnehmer verarbeitet die personenbezogenen Daten nur im Rahmen der vom Auftraggeber erteilten Weisungen. Dies gilt nicht, soweit der Auftragnehmer durch das Recht der EU oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung verpflichtet ist. In diesem Fall teilt der Auftragnehmer diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, die Mitteilung ist durch das betreffende Recht wegen eines wichtigen öffentlichen Interesses verboten.

4. INSTRUCTIONS

4.1 The Processor shall process personal data only within the framework of the instructions issued by the Controller. This does not apply if the Processor is obliged to process the data by EU law or the law of the Member States to which the Processor is subject. In such a case, the Processor shall communicate these legal requirements prior to processing, unless such communication is prohibited by the relevant law on important grounds of public interest.

4.2 Falls Weisungen die unter Ziffer 1 der Anlage dieses Vertrages getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Vereinbarung in schriftlicher Form erfolgt.

4.2 If instructions change, cancel, or supplement the stipulations made in Section 1 of the Annex to this Agreement, they are only permissible if a corresponding new agreement is made in writing.

4.3 Unabhängig von der Form der Erteilung dokumentieren sowohl der Auftragnehmer als auch der Auftraggeber jede Weisung des Auftraggebers in Textform. Die Weisungen sind für ihre Geltungsdauer dieses Vertrages und anschließend noch für drei Jahre aufzubewahren.

4.3 Regardless of the form of issuance, both the Processor and the Controller shall document every instruction of the Controller in text form. Instructions must be kept for the duration of this Agreement and subsequently for three years.

4.4 Der Auftragnehmer weist den Auftraggeber unverzüglich darauf hin, wenn eine vom Auftraggeber erteilte Weisung seiner Auffassung nach gegen gesetzliche Vorschriften verstößt.

4.4 The Processor shall immediately inform the Controller if, in its opinion, an instruction issued by the Controller violates statutory provisions.

4.5 Der Auftraggeber legt den oder die Weisungsberechtigten fest. Der Auftragnehmer legt Weisungsempfänger fest.

4.5 The Controller determines the person(s) authorized to issue instructions. The Processor determines the recipient(s) of instructions.

5. UNTERSTÜTZUNGSPFLICHTEN DES AUFTRAGNEHMERS

5. SUPPORT OBLIGATIONS OF THE PROCESSOR

5.1 Der Auftragnehmer ergreift angesichts der Art der Verarbeitung geeignete technische und organisatorische Maßnahmen, um den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen der betroffenen Personen nach Art. 12 bis 22 DSGVO zu unterstützen.

5.1 Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organizational measures for the fulfillment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

5.2 Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Verantwortlichen bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DSGVO.

5.2 Taking into account the nature of processing and the information available to him, the Processor shall assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR.

5.3 Sofern sich eine betroffene Person oder eine Datenschutzaufsichtsbehörde im Zusammenhang mit den unter dieser Vereinbarung verarbeiteten personenbezogenen Daten direkt an den Auftragnehmer wendet, informiert der Auftragnehmer den Auftraggeber hierüber unverzüglich.

5.3 If a data subject or a data protection supervisory authority contacts the Processor directly in connection with the personal data processed under this Agreement, the Processor shall inform the Controller immediately.

6. PRÜFUNGSRECHTE DES AUFTRAGGEBERS

6. AUDIT RIGHTS OF THE CONTROLLER

6.1 Der Auftragnehmer stellt dem Auftraggeber auf dessen Anfrage alle erforderlichen Informationen zum Nachweis der in diesem Vertrag und Art. 28 DSGVO geregelten Pflichten zur Verfügung.

6.1 The Processor shall make available to the Controller on request all information necessary to demonstrate compliance with the obligations laid down in this Agreement and Article 28 GDPR.

6.2 Der Auftraggeber ist berechtigt, die Einhaltung der Pflichten aus diesem Vertrag und aus Art. 28 DSGVO zu überprüfen und beim Auftragnehmer Inspektionen vor Ort durchzuführen (grundsätzlich nach Terminvereinbarung).

6.2 The Controller is entitled to verify compliance with the obligations under this Agreement and Art. 28 GDPR and to conduct on-site inspections at the Processor's premises (generally by appointment).

6.3 Soweit dem Auftragnehmer durch die Unterstützung bei Inspektionen oder die Beantwortung umfangreicher Fragenkataloge Kosten entstehen, die über das übliche Maß hinausgehen, ist der Auftraggeber verpflichtet, dem Auftragnehmer diesen Mehraufwand zu vergüten, sofern der Auftragnehmer nicht selbst Anlass zur Prüfung gegeben hat (z.B. durch einen Datenverstoß).

6.4 Insofar as the Processor incurs costs through assistance with inspections or answering extensive questionnaires that exceed the usual scope, the Controller is obliged to reimburse the Processor for this additional effort, unless the Processor itself gave cause for the audit (e.g., through a data breach).

7. DATENSCHUTZBEAUFTRAGTER Der Datenschutzbeauftragte des Auftragnehmers ist in der Anlage dieses Vertrages unter Ziffer 3 angeführt, soweit ein solcher bestellt ist.

7. DATA PROTECTION OFFICER The Data Protection Officer of the Processor is listed in Section 3 of the Annex to this Agreement, insofar as one is appointed.

8. VERTRAULICHKEIT

8. CONFIDENTIALITY

8.1 Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er wahrt das Datengeheimnis sowie die Vertraulichkeit.

8.1 The Processor confirms that it is familiar with the relevant data protection regulations. It maintains data secrecy and confidentiality.

8.2 Der Auftragnehmer verpflichtet seine Mitarbeiter vertraglich zur Vertraulichkeit, sofern sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

8.2 The Processor commits its employees to confidentiality by contract, unless they are subject to an appropriate statutory duty of confidentiality.

9. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (TOMs) Der Auftragnehmer führt geeignete technische und organisatorische Maßnahmen durch, um ein angemessenes Schutzniveau zu gewährleisten (Art. 32 DSGVO). Die Maßnahmen sind in der Anlage beschrieben.

9. TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs) The Processor implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk (Art. 32 GDPR). The measures are described in the Annex.

10. INFORMATIONSPFLICHTEN Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über jegliche Verstöße oder vermutete Verstöße gegen diesen Vertrag oder Vorschriften, die den Schutz personengezogener Daten betreffen.

10. INFORMATION OBLIGATIONS The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach or any violation of this Agreement or data protection regulations.

11. UNTERAUFTRAGNEHMER

11. SUB-PROCESSORS

11.1 Die Beauftragung von Unterauftragnehmern erfolgt nur nach Zustimmung des Auftraggebers (Textform). Der Auftraggeber stimmt hiermit den in der Anlage aufgeführten Unterauftragnehmern zu.

11.1 The engagement of sub-processors shall only take place with the consent of the Controller (text form). The Controller hereby consents to the sub-processors listed in the Annex.

11.1 Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Unterauftragnehmer hinzuzuziehen. Der Auftragnehmer informiert den Auftraggeber vorab (z.B. per E-Mail oder im Admin-Dashboard) über jede beabsichtigte Änderung in Bezug auf die

11.1 The Controller grants the Processor general permission to engage further sub-processors. The Processor shall inform the Controller in advance (e.g., via email or within the admin dashboard) of any intended change regarding the addition or replacement of sub-processors. The

Hinzuziehung oder die Ersetzung von Unterauftragnehmern. Der Auftraggeber kann gegen die Änderung innerhalb von 14 Tagen nach Zugang der Information schriftlich oder in Textform Einspruch erheben, sofern ein wichtiger datenschutzrechtlicher Grund vorliegt. Erfolgt kein Einspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als erteilt.

Controller may object to the change in writing or in text form within 14 days of receipt of the information, provided there is a significant data protection reason. If no objection is made within the deadline, consent to the change shall be deemed granted.

12. LÖSCHUNG UND RÜCKGABE Nach Abschluss der Leistungen ist der Auftragnehmer verpflichtet, alle personenbezogenen Daten nach Wahl des Auftraggebers zurückzugeben oder zu löschen, sofern keine gesetzlichen Aufbewahrungspflichten bestehen.

12. DELETION AND RETURN Upon completion of the services, the Processor is obliged to return or delete all personal data at the choice of the Controller, unless statutory storage obligations exist.

13. HAFTUNG Der Auftragnehmer haftet im Rahmen der gesetzlichen Bestimmungen.

13. LIABILITY The Processor is liable within the framework of the statutory provisions.

14. SCHLUSSBESTIMMUNGEN Änderungen bedürfen der Schriftform. Sollte eine Bestimmung unwirksam sein, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht.

14. FINAL PROVISIONS Amendments require the written form. Should a provision be invalid, this shall not affect the validity of the remaining provisions.

Für den Auftraggeber:

For the Controller:

Ort, Datum Unterschrift & Name

Place, Date, Signature & Name

Für den Auftragnehmer:

For the Processor:

Ort, Datum, Leander Jo Bärwaldt, Gründer & CEO

Place, Date, Leander Jo Bärwaldt, Founder & CEO

ANLAGE ZUM AUFTRAGSVERARBEITUNGSVERTRAG

1. GEGENSTAND DES AUFTRAGES Erbringung von Cookieless-Web-Tracking-Dienstleistungen durch den Auftragnehmer für den Auftraggeber (SaaS). Bereitstellung der Software, Hosting und Support.

2. UMFANG, ART UND ZWECK Art: Erhebung, Speicherung, Organisation, Analyse und Bereitstellung von Nutzungsdaten.
Zweck: Analyse des Nutzerverhaltens auf der Webseite des Auftraggebers, Bereitstellung von Statistiken.

3. ART DER DATEN
- IP-Adresse (anonymisiert)
- Online-Kennungen, Nutzungsdaten (z.B. besuchte Seiten, Scroll-Tiefe)
- Technische Daten (z.B. Browser-Typ, Gerätetyp)

4. KREIS DER BETROFFENEN
- Website-Besucher
- Mitarbeiter des Auftraggebers (für Login/Support)

5. UNTERAUFTRAGNEHMER (Genehmigt)

Hetzner Online GmbH (Deutschland/Finnland) Tätigkeit: Hosting / Server-Infrastruktur

Stripe Payments Europe, Ltd. (Irland) Tätigkeit: Zahlungsabwicklung & Rechnungsstellung

Loops Inc. (USA) Tätigkeit: System-E-Mails & Onboarding

ANNEX TO THE DATA PROCESSING AGREEMENT

1. SUBJECT MATTER OF THE ORDER Provision of cookieless web tracking services by the Processor for the Controller (SaaS). Provision of software, hosting, and support.

2. SCOPE, NATURE AND PURPOSE Nature: Collection, storage, organization, analysis, and provision of usage data.
Purpose: Analysis of user behavior on the Controller's website, provision of statistics.

3. TYPES OF DATA
- IP address (anonymized)
- Online identifiers, usage data (e.g., visited pages, scroll depth)
- Technical data (e.g., browser type, device type)

4. CATEGORIES OF DATA SUBJECTS
- Website visitors
- Employees of the Controller (for login/support)

5. SUB-PROCESSORS (Approved)

Hetzner Online GmbH (Germany/Finland) Activity: Hosting / Server Infrastructure

Stripe Payments Europe, Ltd. (Ireland) Activity: Payment Processing & Invoicing

Loops Inc. (USA) Activity: System Emails & Onboarding

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (TOMs)

1. Zutrittskontrolle Die Verarbeitung erfolgt ausschließlich in Rechenzentren der Hetzner Online GmbH (ISO/IEC 27001 zertifiziert). Maßnahmen: 24/7 Videoüberwachung, Sicherheitspersonal, Zutrittskontrollsysteme, Protokollierung.

2. Zugangs- und Zugriffskontrolle

- Authentifizierung: Zugriff auf Server nur über personalisierte Konten und verschlüsselte Verbindungen (SSH-Keys).

- 2-Faktor-Authentifizierung (2FA) für administrative Zugänge.

- Rollenbasiertes Zugriffskonzept (Need-to-know-Prinzip).

- Firewalls und Protokollierung aller administrativen Zugriffe.

3. Eingabekontrolle Systemseitige Protokollierung (Logging) aller administrativen Tätigkeiten, um Änderungen nachvollziehen zu können.

4. Trennungskontrolle Logische Trennung der Daten verschiedener Kunden (Mandantenfähigkeit) auf Datenbank- und Anwendungsebene.

5. Weitergabekontrolle Verschlüsselte Übertragung (TLS 1.2 oder höher) zwischen Client und Server sowie intern. Unverschlüsselte Übertragungen sind deaktiviert.

6. Verfügbarkeit und Belastbarkeit

TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)

1. Physical Access Control Processing takes place exclusively in data centers of Hetzner Online GmbH (ISO/IEC 27001 certified). Measures: 24/7 video surveillance, security personnel, access control systems, logging.

2. System and Data Access Control

- Authentication: Server access only via personalized accounts and encrypted connections (SSH keys).

- 2-Factor Authentication (2FA) for administrative access.

- Role-Based Access Control (RBAC) / Need-to-know principle.

- Firewalls and logging of all administrative access.

3. Input Control System-side logging of all administrative activities to ensure traceability of changes.

4. Separation Control Logical separation of data from different customers (multi-tenancy) at database and application levels.

5. Transfer Control Encrypted transmission (TLS 1.2 or higher) between client and server as well as internally. Unencrypted transmissions are deactivated.

6. Availability and Resilience

- Redundante Infrastruktur (Failover-Konfiguration).

- Tägliche verschlüsselte Backups an einem geographisch getrennten Standort.

- DDoS-Schutz auf Netzwerkebene.

7. Privacy by Design / Default IP-Adressen werden standardmäßig und frühestmöglich anonymisiert (z.B. Kürzung des letzten Oktetts), bevor sie gespeichert werden.

8. Auftragskontrolle Auswahl ISO-zertifizierter Subunternehmer (Hetzner).

- Redundant infrastructure (failover configuration).

- Daily encrypted backups at a geographically separate location.

- DDoS protection at network level.

7. Privacy by Design / Default IP addresses are anonymized by default and as early as possible (e.g., masking the last octet) before storage.

8. Order Control Selection of ISO-certified sub-processors (Hetzner).