Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO zwischen der

HYPOFY GmbH

Schwindstr. 5

76135 Karlsruhe

- im Folgenden „**Auftragnehmer**“ -

und gewerblichen Lizenznehmern der Anwendung „HYPOFY“

- im Folgenden „**Auftraggeber**“ -

Stand: 01.09.2025

1. Vertragsgegenstand

Im Rahmen der Leistungserbringung nach den Allgemeinen Geschäftsbedingungen zur Anwendung „HYPOFY“ (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „Auftraggeber-Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

2. Umfang der Beauftragung

2.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn.

2.2 Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie in Anlage 1 zu diesem Vertrag spezifiziert; die Verarbeitung betrifft die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

2.3 Der Auftragnehmer ist berechtigt, Anwendernutzungsdaten des Auftraggebers für Zwecke des Monitorings, Stabilitäts- und Performance-

verbesserungen sowie Weiterentwicklungen anonymisiert zu verarbeiten, sodass ein Personenbezug irreversibel ausgeschlossen ist. Anonymisierte Daten gelten nicht mehr als personenbezogene Daten.

2.4 Soweit der Auftragnehmer personenbezogene Daten zu eigenen Zwecken verarbeitet, erfolgt dies ausschließlich in eigener datenschutzrechtlicher Verantwortlichkeit. Diese Verarbeitungen sind nicht Gegenstand dieses AVV.

2.5 Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44 - 48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

2.6 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet ist.

3. Weisungsbefugnisse des Auftraggebers

3.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2 Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses Vertrags festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des im Hauptvertrag festgelegten Änderungsverfahrens, in dem die Weisung zu dokumentieren und die Übernahme etwa dadurch bedingter Mehrkosten des Auftragnehmers durch den Auftraggeber zu regeln ist.

3.3 Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Auftraggeber-Daten beim Auftraggeber

liegt.

4. Verantwortlichkeit des Auftraggebers

4.1 Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

4.2 Dem Auftraggeber obliegt es, dem Auftragnehmer die Auftraggeber-Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für die Qualität der Auftraggeber-Daten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4.3 Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung zu stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.

4.4 Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

5. Anforderungen an Personal

Der Auftragnehmer stellt sicher, dass alle zur Verarbeitung der Auftraggeber-Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

6. Sicherheit der Verarbeitung

6.1 Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen

erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.

6.2 Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen.

6.3 Der Auftragnehmer implementiert einen Eskalationsprozess für Sicherheitsvorfälle, der die Analyse, Eindämmung und Behebung von Vorfällen regelt. Der Auftraggeber wird über relevante Vorfälle unverzüglich informiert und unterstützt die Abstimmung mit Aufsichtsbehörden nach Maßgabe von Art. 33 DSGVO.

6.4 Der Auftragnehmer erstellt regelmäßig gesicherte Backups der Auftraggeber-Daten und implementiert Verfahren zur Wiederherstellung im Fall von Datenverlust oder Systemausfällen. Backup-Zyklen, Speicherorte und Wiederherstellungszeiten werden dokumentiert und auf Anforderung dem Auftraggeber mitgeteilt.

7. Inanspruchnahme weiterer Auftragsverarbeiter

7.1 Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus Anlage 2. Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten trifft.

7.2 Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter 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 wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.

7.3 Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass

diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.

7.4 Unter Einhaltung der Anforderungen der Ziffer 2.5 dieses Vertrags gelten die Regelungen in dieser Ziffer 7 auch, wenn ein weiterer Auftragsverarbeiter in einem Drittstaat eingeschaltet wird. Der Auftraggeber bevollmächtigt den Auftragnehmer hiermit, in Vertretung des Auftraggebers mit einem weiteren Auftragsverarbeiter einen Vertrag unter Einbeziehung der Standardvertragsklauseln der Europäischen Kommission gemäß Durchführungsbeschluss (EU) 2021/914 („SCC 2021“) zu schließen. Der Auftraggeber erklärt sich bereit, an der Erfüllung der Voraussetzungen nach Art. 49 DSGVO im erforderlichen Maße mitzuwirken. Soweit erforderlich, werden zusätzliche Schutzmaßnahmen gemäß Art. 44 ff. DSGVO implementiert.

7.5 Der Auftragnehmer informiert den Auftraggeber mindestens 14 Tage vor der Beauftragung eines neuen Subprozessors. Der Auftraggeber kann der Beauftragung aus nachweislich wichtigen Gründen widersprechen. Änderungen der Subprozessoren-Liste werden regelmäßig, mindestens einmal jährlich, aktualisiert.

8. Rechte der betroffenen Personen

8.1 Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

8.2 Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

8.3 Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Auftraggeber-Daten, die Empfänger von Auftraggeber-Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt, und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.

8.4 Der Auftragnehmer wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten, Auftraggeber-Daten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

8.5 Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeber-Daten nach Art. 20 DSGVO besitzt, wird der Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei der Bereitstellung der Auftraggeber-Daten in einem gängigen und maschinenlesbaren Format unterstützen, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

8.6 Der Auftragnehmer unterstützt den Auftraggeber bei der Datenübertragbarkeit nach Art. 20 DSGVO, indem er die Auftraggeber-Daten in einem gängigen, maschinenlesbaren Format bereitstellt. Bei Massenanfragen stellt der Auftragnehmer technische Unterstützung zur Verfügung.

9. Mitteilungs- und Unterstützungspflichten des Auftragnehmers

9.1 Soweit den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeber-Daten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber zeitnah über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten unterstützen.

9.2 Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

9.3 Soweit die Verarbeitung Auftraggeber-Daten eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich macht, wird der Auftragnehmer den Auftraggeber unverzüglich unterstützen. Der Auftragnehmer stellt hierzu alle für die DSFA notwendigen Informationen zu den technischen und organisatorischen Maßnahmen sowie zur Art der Verarbeitung zur Verfügung.

10. Datenlöschung

10.1 Der Auftragnehmer wird die Auftraggeber-Daten nach Beendigung dieses Vertrages löschen, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht.

10.2 Der Auftragnehmer darf Dokumentationen und Nachweise, die der Einhaltung dieses Vertrages dienen, bis maximal zwei Jahre nach Beendigung des Vertrages aufbewahren, sofern keine gesetzliche Verpflichtung zu längerer Speicherung besteht.

11. Nachweise und Überprüfungen

11.1 Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.

11.2 Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen.

11.3 Zur Durchführung der Überprüfung nach Ziffer 11.2 ist der Auftraggeber im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 10 bis 18 Uhr) nach rechtzeitiger Vorankündigung gemäß Ziffer 11.5 auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers berechtigt.

11.4 Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

11.5 Der Auftraggeber ist berechtigt, einmal jährlich oder nach vorheriger Vereinbarung Audits zur Einhaltung der technischen und organisatorischen Maßnahmen durchzuführen. Audits erfolgen unter Berücksichtigung der Betriebsabläufe des Auftragnehmers und unter Wahrung von Betriebs- und Geschäftsgeheimnissen Dritter.

12. Protokollierung der Verarbeitung

Der Auftragnehmer führt ein Verzeichnis aller Verarbeitungstätigkeiten im Rahmen dieses Vertrages, einschließlich Art, Umfang, Zweck und Empfänger der Auftraggeber-Daten sowie der Dauer der Verarbeitung. Das Verzeichnis wird dem Auftraggeber auf Anforderung zugänglich gemacht, um die Einhaltung der Weisungen nach

Art. 28 DSGVO nachzuweisen.

13. Vertragsdauer und Kündigung

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

14. Haftung

14.1 Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

14.2 Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

15. Schlussbestimmungen

15.1 Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.

15.2 Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Zweck, Art und Umfang der Datenverarbeitung	Der Gegenstand der Auftragsverarbeitung durch den Auftragnehmer für den Auftraggeber als Verantwortlichen ergibt sich konkret aus den bestehenden Verträgen zwischen den Parteien, insbes.: • Bereitstellung der HYPOFY-App & CRM • Nutzerverwaltung & Authentifizierung • Hosting & Datenspeicherung • Zahlungsabwicklung • Support & Ticketbearbeitung • Analyse / Performance-Monitoring
Kategorien der personenbezogenen Daten	Es werden Daten der folgenden Personenkategorien verarbeitet: ☒Namensdaten ☒Geburtsdaten ☒Bank- und Zahlungsdaten ☒Kontakt- und Adressdaten ☒Kundenvertragsdaten ☒Login-Daten ☒Foto- und Videodaten (z.B. Dokumente für Darlehensantrag)
Kategorien betroffener Personen	Es werden Daten der folgenden Personenkategorien verarbeitet: ☒Kunden

Anlage 2: Weitere Auftragsverarbeiter

1. Identity / Authentifizierung

Okta, Inc.

100 First Street, San Francisco, CA 94105, USA

- Tätigkeit: Nutzerverwaltung / Identity Provider / MFA
- Zweck: Authentifizierung & Zugriffssicherheit
- Daten: Login-Daten, Nutzerkennungen
- Betroffene: Anwendungsnutzer
- Transfer: SCC 2021/914

2. Hosting / Infrastruktur

netcup GmbH

Daimlerstraße 25, 76185 Karlsruhe, Deutschland

- Tätigkeit: Hosting / Serverbetrieb
- Zweck: Bereitstellung App & CRM
- Daten: Alle Auftraggeber-Daten
- Betroffene: Nutzer, Kunden
- Transfer: keiner (EU)

Hetzner Online GmbH

Industriestraße 25, 91710 Gunzenhausen, Deutschland

- Tätigkeit: Hosting / Rechenzentrum
- Zweck: Infrastruktur / Backup / Storage
- Daten: Alle Auftraggeber-Daten
- Betroffene: Nutzer, Kunden
- Transfer: keiner (EU)

3. Zahlungsabwicklung

Stripe Payments Europe Ltd.

1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Irland

- Tätigkeit: Zahlungsabwicklung
- Zweck: Abonnement- & Kaufzahlungen
- Daten: Zahlungsdaten, Vertragsdaten
- Betroffene: Kunden
- Transfer: ggf. SCC 2021/914

4. CDN / Security / Performance

Cloudflare, Inc.

101 Townsend Street, San Francisco, CA 94107, USA

- Tätigkeit: CDN / DDoS-Schutz / Security
- Zweck: Performance & Absicherung Webservices
- Daten: IP-Adressen, Logdaten
- Betroffene: Nutzer
- Transfer: SCC 2021/914

5. Monitoring / Analyse / Attribution

Google LLC (Firebase / FCM)

1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

- Tätigkeit: Monitoring / Crashlytics / Push
- Zweck: Performance-Analyse / Push-Versand
- Daten: Device-IDs, Events, Logdaten
- Betroffene: Nutzer
- Transfer: SCC 2021/914

PostHog, Inc.

2261 Market Street #4008, San Francisco, CA 94114, USA

- Tätigkeit: Produkt- & Nutzungsanalyse
- Zweck: Optimierung App & CRM
- Daten: Nutzungsdaten, Events, IDs
- Betroffene: Nutzer
- Transfer: SCC 2021/914

Branch Metrics, Inc.

1400 Seaport Blvd, Redwood City, CA 94063, USA

- Tätigkeit: Marketing-Attribution / Deep Linking
- Zweck: Kampagnenmessung
- Daten: Device-IDs, Events
- Betroffene: Nutzer
- Transfer: SCC 2021/914

6. E-Mail-Kommunikation

Brevo (Sendinblue GmbH / Brevo SAS)

Köpenicker Straße 126, 0179 Berlin, Deutschland (Hauptsitz: Paris, Frankreich)

- Tätigkeit: E-Mail-Versand

- Zweck: Transaktions- & Systemmails
- Daten: E-Mail-Adressen, Namen
- Betroffene: Nutzer, Kunden
- Transfer: keiner (EU)

7. Push-Benachrichtigungen

Apple Inc. (APNS)

One Apple Park Way, Cupertino, CA 95014, USA

- Tätigkeit: Push Notification Service
- Zweck: Versand Push-Nachrichten
- Daten: Push-Token / Device-IDs
- Betroffene: iOS-Nutzer
- Transfer: SCC 2021/914

8. Support / Ticketsystem

Atlassian Pty Ltd. (Jira Service Management)

Level 6, 341 George Street, Sydney NSW 2000, Australien

- Tätigkeit: Ticketsystem / Support
- Zweck: Bearbeitung Supportanfragen
- Daten: Kontaktdaten, Ticket-Inhalte
- Betroffene: Nutzer, Kunden
- Transfer: SCC 2021/914

9. Kommunikation / Alerting

Slack Technologies, LLC

500 Howard Street, San Francisco, CA 94105, USA

- Tätigkeit: Interne Kommunikation / Alerts
- Zweck: Incident- & Fehlerkommunikation
- Daten: Fehlerlogs (minimiert)
- Betroffene: Nutzer (indirekt möglich)
- Transfer: SCC 2021/914

10. Dokumentenmanagement / Cloud

Microsoft Corporation

- One Microsoft Way, Redmond, WA 98052, USA
- Tätigkeit: SharePoint / OneDrive / M365

- Zweck: Dokumentenspeicherung / Zusammenarbeit
- Daten: Dokumenteninhalte
  Betroffene: Nutzer, Kunden
  Transfer: SCC 2021/914

Anlage 3: Technische und organisatorische Maßnahmen (TOM)

gemäß Art. 32 DSGVO

Der Auftragnehmer trifft unter Berücksichtigung des Stands der Technik, der Art, des Umfangs und der Zwecke der Verarbeitung geeignete technische und organisatorische Maßnahmen, um ein angemessenes Schutzniveau für personenbezogene Daten sicherzustellen.

Die Maßnahmen betreffen die Verarbeitung personenbezogener Daten im Rahmen der Bereitstellung der HYPOFY-Plattform (CRM, Web-Anwendung, mobile App, Backend-Systeme).

1. Vertraulichkeit

1.1 Zutrittskontrolle

- Hosting über professionelle Rechenzentrumsbetreiber innerhalb der EU (insbesondere Netcup GmbH und Hetzner Online GmbH)
- Rechenzentren mit physischer Zugangssicherung
- Keine lokale Serverhaltung in Büroräumen des Auftragnehmers

1.2 Zugangskontrolle

- Zugriff auf Systeme nur über personalisierte Benutzerkonten
- Passwortgeschützte Authentifizierung
- Starke Passwortanforderungen
- Multi-Faktor-Authentifizierung (MFA) für Administratoren
- Automatische Session-Beendigung bei Inaktivität
- Verwaltung von Benutzerberechtigungen

1.3 Zugriffskontrolle

- Rollen- und Berechtigungskonzept
- Zugriff nach dem „Need-to-know“-Prinzip
- Mandantentrennung innerhalb der Plattform
- Beschränkung administrativer Zugriffe
- Regelmäßige Überprüfung von Berechtigungen

1.4 Trennungskontrolle

- Trennung von Test- und Produktivsystemen
- Logische Mandantentrennung
- Separate Umgebungen (z.B. Entwicklung / Staging / Produktion)

2. Integrität

2.1 Weitergabekontrolle

- Verschlüsselte Datenübertragung (TLS / HTTPS)

- Gesicherte API-Kommunikation
- Zugriffsschutz für Administrationszugänge
- Protokollierung sicherheitsrelevanter Zugriffe

2.2 Eingabekontrolle

- Nachvollziehbarkeit von Benutzeraktionen (Audit-Logs)
- Protokollierung von Änderungen (wo technisch vorgesehen)
- Zuordnung von Aktionen zu Benutzerkonten
- Dokumentierte Zuständigkeiten für Datenlöschungen

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

- Betrieb auf redundanter Hosting-Infrastruktur
- Verteilung der Systeme auf mehrere Anbieter / Standorte
- Systemmonitoring

3.2 Datensicherung

- Regelmäßige Backups produktiver Daten
- Getrennte Speicherung von Backups
- Dokumentierte Wiederherstellungsverfahren

3.3 Wiederherstellbarkeit

- Verfahren zur Wiederherstellung von Daten nach Störungen
- Dokumentierte Restore-Prozesse

4. Belastbarkeit / Systemsicherheit

- Monitoring der Systemstabilität
- Patch- & Update-Management
- Schutzmaßnahmen gegen Schadsoftware
- Maßnahmen zur Fehler- und Störungserkennung

5. Verfahren zur regelmäßigen Überprüfung

5.1 Sicherheits- und Datenschutzmanagement

- Regelmäßige Überprüfung der Wirksamkeit der TOM
- Schwachstellenanalysen nach Bedarf
- Dokumentierte Datenschutzprozesse
- Führung eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO)

5.2 Incident-Response-Management

- Verfahren zur Behandlung von Sicherheitsvorfällen

- Dokumentierte Melde- und Eskalationsprozesse
- Unterstützung bei Meldungen nach Art. 33 / 34 DSGVO

6. Verschlüsselung & Schutzmaßnahmen

- TLS-Verschlüsselung für Datenübertragungen
- Passwort-Hashing
- Verschlüsselung sensibler Daten, sofern technisch vorgesehen

7. Organisationsmaßnahmen

7.1 Vertraulichkeit & Sensibilisierung

- Verpflichtung von Mitarbeitenden auf Vertraulichkeit
- Datenschutz- und IT-Sicherheitsschulungen
- Interne Richtlinien zur sicheren Systemnutzung

7.2 Weisungsmanagement

- Verarbeitung nur auf dokumentierte Weisung des Auftraggebers
- Verfahren zur Weisungsannahme und -umsetzung

7.3 Auftragskontrolle

- Sorgfältige Auswahl von Subprozessoren
- Vertragliche Datenschutzvereinbarungen
- Löschung / Rückgabe personenbezogener Daten nach Vertragsende

8. Datenschutz durch Technikgestaltung (Art. 25 DSGVO)

- Datenminimierung
- Zweckbindung
- Rollen- und Berechtigungskonzepte
- Berücksichtigung von Privacy-by-Design bei Weiterentwicklungen

9. Löschung & Datenminimierung

- Dokumentiertes Löschkonzept
- Löschung nach Weisung / Vertragsende
- Einschränkung unnötiger Datenspeicherung

Hinweis zur Hosting-Infrastruktur

Die Verarbeitung erfolgt auf Cloud-Infrastruktur innerhalb der Europäischen Union.

Zur Sicherstellung von Verfügbarkeit und Ausfallsicherheit nutzt der Auftragnehmer insbesondere:

- Netcup GmbH
- Hetzner Online GmbH