Datenschutzvertrag zur Datenverarbeitung im Auftrag gemäß Art. 28 EU-Datenschutz-Grundverordnung (DSGVO)

Im Auftrag von

nachfolgend **“Verantwortlicher”** genannt

verarbeitet durch

fynk GmbH
Heinrichsgasse 2/8
A-1010 Wien

nachfolgend **“Auftragsverarbeiter”** genannt

§1 Allgemeines

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Datenschutzvertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Der vorliegende Datenschutzvertrag konkretisiert die Pflichten des Auftragsverarbeiters und des Verantwortlichen (nachfolgend auch die „Parteien“ genannt) hinsichtlich des Datenschutzes, die sich aus der Leistungsvereinbarung/ dem SLA/ dem Hauptvertrag/ dem Auftrag (im Folgenden „Leistungsvereinbarung“) ergeben.

(3) Die in diesem Vertrag verwendeten Begriffe sind gemäß ihrer Definition in der DSGVO zu verstehen.

§2 Vertragsinhalt

Gegenstand, Art und Zweck der Auftragsverarbeitung sowie die Art der verarbeiteten Daten und der Kreis der von der Datenverarbeitung betroffenen Personen ergeben sich aus der Leistungsvereinbarung, sowie aus der Anlage 1 zu diesem Vertrag.

§3 Dauer der Datenverarbeitung

Die Dauer dieses Vertrags entspricht der Laufzeit der Leistungsvereinbarung, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben. Der Vertrag gilt jedoch so lange, wie der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen verarbeitet.

§4 Weisungsrecht

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen des Verantwortlichen werden durch die Leistungsvereinbarung, diesen Vertrag sowie dessen Anlagen festgelegt und können vom Verantwortlichen auch in schriftlicher Form oder in einem dokumentierten elektronischen Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Verantwortliche ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Bezug auf Art, Umfang und Verfahren der Datenverarbeitung sowie im Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

(3) Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Verantwortlichen an den Auftragsverarbeiter entstehen, bleiben unberührt.

(4) Die zum Empfang von Weisungen berechtigten Personen des Auftragsverarbeiters sind in Anlage 1 aufgeführt. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(5) Alle erteilten Weisungen sind sowohl vom Verantwortlichen als auch vom Auftragsverarbeiter zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Verantwortlichen an den Auftragsverarbeiter entstehen, bleiben unberührt.

(6) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§5 Verarbeitungspflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter bestätigt, dass er gemäß Art. 37 DSGVO und einen Datenschutzbeauftragten bestellt hat und die Einhaltung der Vorschriften zum Datenschutz und zur Datensicherheit unter Einbeziehung des Datenschutzbeauftragten überwacht. Dessen Kontaktdaten werden dem Verantwortlichen in Anlage 1 mitgeteilt. Ein Wechsel des Datenschutzbeauftragten ist dem Verantwortlichen unverzüglich mitzuteilen.

(2) Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Verantwortlichen die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort. Der Auftragsverarbeiter sichert insbesondere 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. Des Weiteren werden die entsprechenden Mitarbeiter für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet. Die Mitarbeiter sind über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung zu belehren.

(3) Der Auftragsverarbeiter verpflichtet sich zur Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Art. 32 DSGVO. Einzelheiten dazu sind in § 10 dieser Vereinbarung geregelt.

(4) Der Verantwortliche erteilt seine ausdrückliche Zustimmung, dass Beschäftigte des Auftragsverarbeiters die mit dieser Auftragsverarbeitung im Zusammenhang stehende Datenverarbeitung auch außerhalb der Betriebsräume des Auftragsverarbeiters erbringen können, z.B. durch Telearbeit, Home Office, mobiles Arbeiten. Voraussetzung hierfür ist, dass

a) die in diesem Vertrag vereinbarten für die Verarbeitungssituation angemessenen technischen und organisatorischen Maßnahmen (siehe Anlage 2) gewährleistet sind;

b) und dass, soweit Daten des Verantwortlichen in einer Privatwohnung verarbeitet werden, der Auftragsverarbeiter durch angemessene Maßnahmen gewährleistet, dass dabei die Vorgaben der DSGVO beachtet werden.

(5) Die durch den Auftragsverarbeiter getroffenen technischen und organisatorischen Schutzmaßnahmen nach Art. 32 DSGVO für den Einsatz von Beschäftigten des Auftragsverarbeiters im Rahmen von Telearbeit, Home Office und mobilem Arbeiten werden als Anlage 2 beigefügt. Änderungen der getroffenen Maßnahmen durch den Auftragsverarbeiter sind unter bestimmten in § 10 genannten Bedingungen, zulässig.

(6) Der Auftragsverarbeiter verpflichtet sich, die internen Prozesse regelmäßig zu kontrollieren, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

§6 Mitwirkungs- und Unterstützungspflichten des Auftragsverarbeiters

(1) Macht eine betroffene Person Rechte gem. Kapitel III DSGVO, (Auskunftserteilung, Berichtigung oder Löschung ihrer Daten), unmittelbar gegenüber dem Auftragsverarbeiter geltend, so reagiert dieser nicht selbstständig. Der Auftragsverarbeiter verweist die betroffene Person unverzüglich an den Verantwortlichen und wartet dessen Weisungen ab.

(2) Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 DSGVO. Dazu überlässt der Auftragsverarbeiter dem Verantwortlichen alle dafür notwendigen Informationen, soweit dies nicht gegen Verschwiegenheitsverpflichtungen des Verantwortlichen gegenüber Dritten verstößt.

(3) Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger Zustimmung durch den Verantwortlichen erteilen.

(4) Der Auftragsverarbeiter hat die Pflicht, dem Verantwortlichen bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten im notwendigen Umfang zu unterstützen.

(5) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO und stellt auf Anfrage die jeweils erforderlichen Angaben zur Verfügung.

(6) Der Auftragsverarbeiter verpflichtet sich, die Nachweisbarkeit der Erfüllung der Pflichten aufgrund dieses Datenschutzvertrages sowie aufgrund der geltenden Datenschutzvorschriften zu gewährleisten und die entsprechenden Nachweise dem Verantwortlichen auf Verlangen verfügbar zu machen.

(7) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen bei der Durchführung seiner Kontrollverpflichtungen im Rahmen der Auftragskontrolle, wie in § 11 dieser Vereinbarung beschrieben, in geeigneter Weise zu unterstützen und die erforderlichen Mittel zur Verfügung zu stellen.

§7 Informationspflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter teilt dem Verantwortlichen unverzüglich Verstöße durch ihn selbst oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen mit. Die Mitteilungspflicht gilt auch für Verstöße gegen die im Auftrag getroffenen Festlegungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten (z.B. Abhandenkommen oder unrechtmäßige Übermittlung oder Kenntniserlangung von personenbezogenen Daten, schwerwiegende Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Verantwortlichen). Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO.

(2) Die Meldung über die Verletzung des Schutzes personenbezogener Daten enthält soweit möglich folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und

c) eine Beschreibung der vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(3) Der Auftragsverarbeiter trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informiert hierüber den Verantwortlichen und ersucht diesen um weitere Weisungen.

(4) Der Auftragsverarbeiter sichert zu, dem Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung durchführen.

§8 Unterauftragsverhältnisse

(1) Der Auftragsverarbeiter ist grundsätzlich berechtigt, Unterauftragnehmer (weitere Auftragsverarbeiter) unter Beachtung der nachfolgenden Regelungen zu

beauftragen.

(2) Die Beauftragung von weiteren Auftragsverarbeitern ist nur statthaft, wenn der Auftragsverarbeiter dem Verantwortlichen Namen und Anschrift sowie die vorgesehene Tätigkeit des Unterauftragnehmers mitteilt. Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 unterliegt. Die vertragliche Vereinbarung wird dem Verantwortlichen auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

(3) Die Hinzuziehung neuer oder die Ersetzung bisheriger Unterauftragnehmer durch den Auftragsverarbeiter ist zulässig, sofern der Auftragsverarbeiter dem Verantwortlichen die geplanten Veränderungen vorab schriftlich oder in Textform anzeigt, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Die Genehmigung gilt als erteilt, wenn der Verantwortliche nicht innerhalb von zwei Wochen nach Mitteilung Einspruch gegen eine beabsichtigte Änderung erhebt.

(4) Im Fall des Einspruchs kann der Auftragsverarbeiter nach eigener Wahl die Leistung entweder

a) ohne die beabsichtigte Änderung erbringen oder,

b) sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragsverarbeiter nicht zumutbar ist, die von der Änderung betroffene Leistung innerhalb einer angemessenen Frist und vorheriger Information des Verantwortlichen einstellen.
Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich über die beabsichtigte Einstellung und Frist informieren (Textform genügt). Beiden Parteien wird in diesem Fall das gesonderte Recht auf Kündigung innerhalb von 2 Wochen nach Bekanntgabe der Einstellung eingeräumt.

(5) Zum Zeitpunkt des Vertragsabschlusses sind für den Auftragsverarbeiter die in Anlage 3 mit Namen, Anschrift, Auftragsinhalt und Verarbeitungsstandort bezeichneten Unterauftragnehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden. Sofern die angeführten Unterauftragnehmer Verarbeitungsstandorte in Drittländern aufweisen, erklärt sich der Verantwortliche mit der Übermittlung der Daten in diese Drittländer einverstanden, sofern die Bestimmungen des § 9 dieses Vertrages

eingehalten werden.

(6) Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Leistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Verantwortlichen erbringt und Bewachungsdienste.

(7) Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen genutzt werden. Der Auftragsverarbeiter ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen werden, um den Schutz personenbezogener Daten zu gewährleisten.

§9 Internationale Datenübermittlung

(1) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 im Einklang stehen.

(2) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß § 8 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie sich auf das Bestehen und die Anwendbarkeit eines Angemessenheitsbeschlusses berufen, Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind oder sich die Unterauftragsverarbeiter nachweislich genehmigter Verhaltensregeln unterworfen haben.

§10 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen gem. Art. 32 DSGVO getroffen hat.

(2) In der Anlage 2 werden die technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragsverarbeiter dargestellt.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem Fortschritt und der Weiterentwicklung. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Getroffene Änderungen sind in jedem Fall zu dokumentieren. Die aktuelle Version der technischen und organisatorischen Maßnahmen ist dem Verantwortlichen auf Anfrage bereitzustellen.

(4) Wesentliche Änderungen muss der Auftragsverarbeiter mit dem Verantwortlichen in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

§11 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche hat das Recht, beim Auftragsverarbeiter Auftragskontrollen im Benehmen mit dem Auftragsverarbeiter durchzuführen. Er hat das Recht, sich durch Kontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung und der geltenden Datenschutzvorschriften durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen. Der Auftragsverarbeiter verpflichtet sich, bei diesen Kontrollen, soweit erforderlich, unterstützend mitzuwirken und auf Anforderung die erforderlichen Auskünfte zu erteilen und die entsprechenden Nachweise zur Verfügung zu stellen.

(2) Der Verantwortliche ist berechtigt, die Kontrollen durch einen von ihm beauftragten externen Prüfer auf eigene Kosten durchführen zu lassen, sofern diese nicht in einem Wettbewerbsverhältnis mit dem Auftragsverarbeiter stehen oder andere berechtigte Gründe seitens des Auftragsverarbeiters dem entgegenstehen. Der Auftragsverarbeiter ist berechtigt, sich vorab den Namen des externen Prüfers sowie Nachweise zu dessen Verschwiegenheitspflichten vorlegen zu lassen.

(3) Im Hinblick auf die Kontrollverpflichtungen des Verantwortlichen nach Art. 28 Abs. 1 DSGVO vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragsverarbeiter sicher, dass sich der Verantwortliche von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen jederzeit vor Ort durch Kontrollen überzeugen kann. Es wird vereinbart, dass die Anzahl anlassloser Vor-Ort-Kontrollen auf einmal pro Jahr begrenzt wird. Anlasslose Kontrollen sind rechtzeitig anzumelden und so durchzuführen, dass die Betriebsabläufe des Auftragsverarbeiters dabei nicht unverhältnismäßig gestört werden. Ggf. entstehende Kosten tragen die jeweiligen Vertragsparteien selbst. Für darüberhinausgehende anlasslose Kontrollen wird eine Vergütung durch den Verantwortlichen entsprechend des beim Auftragsverarbeiter tatsächlich entstehenden Aufwandes vereinbart.

(4) Der Auftragsverarbeiter kann den Nachweis der Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO auch durch Vorlage eines aktuellen Testats oder Berichts (z.B. Wirtschaftsprüfer, Revision) erbringen. Weitere Möglichkeiten des Nachweises sind eine aktuelle Zertifizierung (z.B. nach ISO/IEC 27001) oder ein Datenschutzsiegel oder -prüfzeichen gemäß Art. 42 DSGVO oder die Vorlage eines den Anforderungen der DSGVO entsprechenden Datenschutz- oder IT-Sicherheitskonzepts. Der Verantwortliche behält sich weitergehende Kontrollrechte nach Prüfung der vorgelegten Nachweise vor.

(5) Wird der Nachweis der Einhaltung der Vorschriften der DSGVO mit Hilfe einer Zertifizierung gem. Art. 42 DSGVO durch den Auftragsverarbeiter erbracht, so verpflichtet er sich, den Verantwortlichen über den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

§12 Löschung und Rückgabe von personenbezogenen Daten

(1) Nach Abschluss der Verarbeitung oder früher nach Aufforderung durch den Verantwortlichen, spätestens aber nach Beendigung dieses Vertrages, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- oder Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen. Alternativ können nach vorheriger Zustimmung die besagten Daten datenschutzgerecht gelöscht bzw. vernichtet werden. Gleiches gilt für Test- und Ausschussmaterial. Diese Verpflichtung gilt in gleichem Maße auch für beauftragte Unterauftragnehmer. Unberührt bleiben Daten sowie Kopien, die zur Erfüllung von Haftungs- und Gewährleistungsansprüchen erforderlich sind. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, oder aus Rechtsgründen, z.B. wegen gesetzlicher Aufbewahrungspflichten, nicht gelöscht werden dürfen, sind durch den Auftragsverarbeiter entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Nach Ablauf der Aufbewahrungsfrist sind sie unverzüglich sicher zu löschen. Der Verantwortliche ist über Art und Umfang der beim Auftragsverarbeiter verbleibenden Daten zu unterrichten. Der Auftragsverarbeiter kann diese Daten zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

§13 Haftung

(1) Auftragsverarbeiter und Verantwortlicher haften im Außenverhältnis nach Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines Verstoßes gegen die DSGVO oder DSG erleidet. Im Innenverhältnis haften Auftragsverarbeiter und Verantwortlicher entsprechend ihres jeweiligen Verursachungs- und Verschuldensanteils. Nimmt eine Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadensersatz in Anspruch, so kann diese Partei von der jeweils anderen Partei Freistellung

oder Schadloshaltung verlangen, soweit dies ihrem Verursachungs- und Verschuldensanteil entspricht.

(2) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen für schuldhafte Verletzungen dieser Vereinbarung nach den gesetzlichen Bestimmungen.

(3) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen für das Verschulden eines von ihm beauftragten Unterauftragnehmers wie für eigenes Verschulden. Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Unterauftragnehmers.

§14 Vertragsdauer und Kündigung

(1) Das Vertragsverhältnis tritt mit Unterzeichnung durch beide Vertragspartner in Kraft und läuft so lange wie der Hauptvertrag. Das ordentliche Kündigungsrecht entspricht dem des Hauptvertrages.

(2) Wenn die Grundlagen der Vertragserfüllung wesentlich verändert werden oder ganz entfallen aufgrund einer Änderung der Rechts- oder Gesetzeslage oder eines Eingreifens oder einer sonstigen Maßnahme der aufsichtführenden Behörden, haben beide Parteien einen Anspruch auf Anpassung des Vertrages an die neuen Verhältnisse, soweit dies möglich und für beide Parteien zumutbar ist. Ist eine Vertragsanpassung nicht möglich oder für eine Partei unzumutbar, ist dies für beide Parteien ein wichtiger Grund für eine außerordentliche Kündigung.

§15 Geheimhaltung

Die Parteien verpflichten sich, alle im Rahmen der Auftragsverarbeitung erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen sowie von Maßnahmen zur Datensicherheit der jeweils anderen Partei vertraulich zu behandeln. Betriebs- und Geschäftsgeheimnisse sind alle auf das Unternehmen einer der Parteien bezogenen Tatsachen, Umstände und Vorgänge, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung die betreffende Partei ein berechtigtes Interesse hat. Maßnahmen zur Datensicherheit sind alle technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO, die eine Partei getroffen hat. Diese Geheimhaltungspflicht besteht nach Beendigung dieses Vertrags fort.

§16 Schlussbestimmungen

(1) Wenn eine Bestimmung dieses Vertrages unwirksam sein oder werden sollte, wird dadurch die Geltung des Vertrages im Übrigen nicht berührt. Es gilt dann eine der unwirksamen

Bestimmung dem Sinn und der wirtschaftlichen Bedeutung nach möglichst nahekommender anderer Bestimmung zwischen den Parteien als vereinbart.

(2) Änderungen und Ergänzungen dieser Vereinbarung, des jeweiligen Einzelvertrages und aller ihrer Bestandteile bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag gilt – soweit zulässig – die Gerichtsstandvereinbarung des Hauptvertrages.

(4) Die dem Vertrag beigefügte Anlagen sind wesentlicher Bestandteil desselben.

Anlagen zum Vertrag

Anlage 1: Konkretisierung des Auftragsgegenstands

Anlage 2: Technische und organisatorische Maßnahmen zum Datenschutz

Anlage 3: Liste der Subauftragsverarbeiter

fynk GmbH
[Kein(e) Unterzeichner zugewiesen]
Signatur(en) ausständig. Details werden nach Abschluss hinzugefügt.

Kunde
[Kein(e) Unterzeichner zugewiesen]
Signatur(en) ausständig. Details werden nach Abschluss hinzugefügt.

Konkretisierung des Auftragsgegenstands

der

fynk GmbH
Heinrichsgasse 2/8
A-1010 Wien

1. Gegenstand, Art und Zweck der Auftragsverarbeitung

Gegenstand der Verarbeitung: Verarbeitung von Daten im Zusammenhang mit Verträgen und Dokumenten aller Art, ausschließlich Dokumente, welche besondere Kategorien von Daten gem Art 9 Abs 1 DSGVO beinhalten; Name und Vorname von Mitarbeitern des Auftraggebers und Mitarbeitern von Vertragspartnern des Auftraggebers; berufliche E-Mail-Adressen von Mitarbeitern des Auftraggebers und Mitarbeitern von Vertragspartnern des Auftraggebers

Art und Zweck der Verarbeitung: Erfassung, Speicherung und Verarbeitung von Daten zum Zwecke der Vertragserstellung und Vertragsverwaltung

Kategorien betroffener Personen: Mitarbeitende des Kunden, Kunden und Vertragspartner des Kunden

2. Weisungsempfangende Personen des Auftragsverarbeiters

Folgende Personen des Auftragsverarbeiters sind berechtigt, Weisungen des Verantwortlichen zu empfangen:

Es sind sämtliche Beschäftigten des Auftragsverarbeiters befugt, Weisungen des Verantwortlichen entgegenzunehmen.

3. Datenschutzbeauftragter des Auftragsverarbeiters

Der Datenschutzbeauftragte des **Auftragsverarbeiters** ist:

Marco Tessendorf
procado Consulting, IT- & Medienservice GmbH
Warschauer Str. 58a
10243 Berlin

Tel.: +49 (30) 293 98 320
E-Mail: ds-fynk@procado.de

4. Standort der Datenverarbeitung

Die von dem Auftragsverarbeiter ausgeführte Datenverarbeitung findet an folgenden Standorten statt:

Geschäftsräume des Auftragsverarbeiters:

fynk GmbH
Heinrichsgasse 2/8
A-1010 Wien

Die Datenverarbeitung findet darüberhinaus an den Verarbeitungsstandorten der Subauftragsverarbeiter statt.

Technische und organisatorische Maßnahmen zum Datenschutz

der

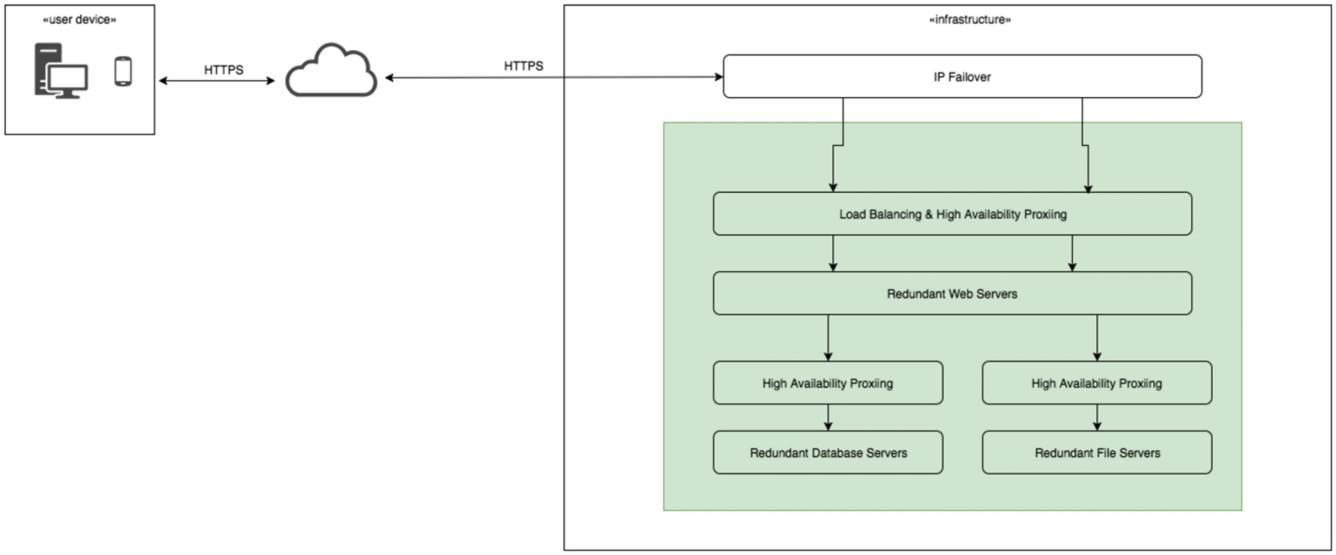
fynk GmbH
Heinrichsgasse 2/8
A-1010 Wien

1. Einleitung

Dieses Dokument soll eine Übersicht über die technischen und organisatorischen Maßnahmen bieten, die fynk im Rahmen seiner Rolle als Auftragsdatenverarbeiter vornimmt, um die Daten des Vertragspartners zu schützen. Dabei hält sich die Struktur des Dokuments an die Vorgaben die sich aus der DSGVO ergeben. Vorab werden allgemeine Informationen bereitgestellt, die das Verständnis der weiteren Angaben erleichtern sollen.

1.1 Systemarchitektur

fynk greift zum Betrieb der Applikation auf die Infrastruktur und Dienstleistungen von Amazon Web Services EMEA Sarl, 38 avenue John F. Kennedy, L-1855, Luxemburg (im folgenden „AWS“) und Microsoft Deutschland GmbH, Walter-Gropius-Straße 5, 80807 München (im folgenden „Azure“) zurück. AWS und Azure sind nach ISO27001 zertifiziert. Zur Wahrung der Datensicherheit setzt fynk unter anderem auf eine softwarebasierte Verschlüsselung aller Datenträger welche Kundendaten beinhalten. Die Architektur ist auf Sicherheit, Skalierbarkeit und hohe Verfügbarkeit ausgelegt, jede für den Betrieb zwingend erforderliche Komponente ist zumindest einfach redundant. Die Systemarchitektur ist in der folgenden Grafik dargestellt.



1.2 Rollen bei fynk mit Datenzugriff

Aus organisatorischer Sicht gibt es mehrere Anwendungsfälle die einen Datenzugriff seitens fynk auf Kundendaten erfordern. Dabei gilt es zu unterscheiden, in welcher Form der Datenzugriff erfolgt:

1.2.1 Zugriff in der Applikation

Um Kunden bei der Einrichtung des Accounts zu helfen und um Fehlerfälle nachvollziehen zu können, können Kundenbetreuer und ggf. Entwickler sich in den Firmen-Account des Kunden einloggen. Hierbei wird jede Aktion (z.B. Datenzugriff und Datenveränderung) die der individuelle User durchführt geloggt.

1.2.2 Zugriff via Datenbank

Um Kunden bei der Einrichtung des Accounts zu helfen und um Fehlerfälle nachvollziehen zu können, können Kundenbetreuer und ggf. Entwickler sich mit der Datenbank verbinden. Hierfür werden individuelle User verwendet, die Datenbankabfragen werden protokolliert.

1.2.3 Zugriff via Server

Für Wartungsarbeiten und Infrastrukturmaßnahmen können Systemadminstratoren von fynk auf die Server auf denen die Kundendaten liegen zugreifen. Dabei werden persönliche User verwendet (kein Sammeluser) und Login und Logout Zeitpunkte auf den Servern geloggt.

2. Vertraulichkeit

2.1 Zutrittskontrolle

fynk greift zum Betrieb der Applikation auf die Infrastruktur und Dienstleistungen von AWS und Azure zurück. Für die Rechenzentren von AWS und Azure werden derzeit folgende Sicherheitsmaßnahmen zur Zutrittskontrolle eingesetzt:

- elektronisches Zutrittskontrollsystem mit Protokollierung
- dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen

2.2 Zugangskontrolle

2.2.1 Nutzer

fynk bietet mehrere Arten der Authentifizierung für Nutzer. Prinzipiell kann der Kunde selbst das Schutzniveau konfigurieren. Es gibt sowohl die Möglichkeit einer einfachen Authentifizierung vie E-Mail und Passwort. Als auch die Möglichkeit der Aktivierung von Zwei-Faktor-Authentifizierung mittels Authenticator App.

Das Passwort kann mit Zugriff auf die bei der Registrierung angegeben Email-Adresse zurückgesetzt werden. Dafür wird je nach Einstellung bei der Registrierung automatisch ein Passwort generiert oder es kann ein eigenes Passwort gewählt werden. Das Passwort kann mit Zugriff auf die bei der Registrierung angegeben Email-Adresse zurückgesetzt werden.

Die Passwortrichtlinie für Nutzer ist: Mindestens 8 Zeichen

2.2.3 Kundenbetreuer

Der Login der Kundenbetreuer ist mit Email, Passwort und zwei Faktor-Authentifizierung gesichert. Die vorgegebene Passwortrichtline von fynk lautet:

- Mindestens 11 Zeichen länge
- Zumindest drei Arten von Zeichen (Großbuchstabe, Kleinbuchstabe, Zahl, Sonderzeichen)
- Passwortrotation alle 6 Monate

- Die letzten 10 Passwörter dürfen nicht verwendet werden

2.2.4 Serveradministratoren

fynk verhindert den unbefugten Zugang zur fynk Infrastruktur einerseits durch den Einsatz von RSA-Schlüsseln. Autorisierte fynk-Administratoren haben einen persönlichen Schlüssel mit dem sie sich zu den Servern verbinden können, die sie für Ihre Arbeit brauchen. Bei der Schlüsselvergabe folgen wir dem Least-Privilege Prinzip, Mitarbeiter bekommen nur Zugang zu Systemen die sie unbedingt brauchen. Andererseits wird der Zugang zur fynk Infrastruktur mittels durchgehender Zwei-Faktor-Authentifizierung mittels FIDO-Schlüsseln sichergestellt.

2.3 Zugriffskontrolle

2.3.1 Nutzer

Die Zugriffskontrolle wird vom System entsprechend der Konfiguration durch den Kunden umgesetzt. fynk bietet ein Rollen- und Berechtigungssystem welches Kunden in der Applikation selber Konfigurieren können. Die Vergabe und periodische Überprüfung der vergebenen Berechtigungen obliegen dem Kunden. Zugriffe von Nutzern in der Applikation werden protokolliert.

2.3.2 Kundenbetreuer

Für Kundenbetreuer obliegt die Zugriffskontrolle fynk. Durch organisatorisches Onboarding und Offboarding Prozesse wird sichergestellt, dass vergebene Berechtigungen aktuell sind.

Zusätzlich werden regelmäßig alle vergebenen Berechtigungen überprüft. Zugriffe von Kundenbetreuern werden protokolliert.

2.3.3 Systemadministratoren

Für Systemadministratoren obliegt die Zugriffskontrolle fynk. Durch organisatorisches Onboarding und Offboarding Prozesse bei neuen Mitarbeitern bzw. bei Abgängen wird sichergestellt, dass vergebene Berechtigungen aktuell sind. Zusätzlich werden monatlich alle vergebenen Berechtigungen überprüft. Login-Zeitpunkte von Systemadministratoren werden auf allen Servern protokolliert.

Alle Mitarbeiter von fynk sind auf das Datengeheimnis verpflichtet, diese Verpflichtung behält ihre Wirkung auch nach einer Kündigung.

3. Integrität

3.1 Weitergabekontrolle

fynk folgt bei der Weitergabekontrolle dem Least-Privilege Prinzip: Daten werden nach Möglichkeit nicht weitergegeben. Die Produktivdaten liegen ausschließlich in Produktion- und Backupsystem. In Ausnahmefällen werden Produktivdaten in ein Testsystem eingespielt, hier gibt es einen definierten Prozess nach dem vorgegangen wird und der sicherstellt, dass die Daten sobald die notwendigen Tests erfolgt sind, wieder gelöscht werden. Daten werden immer über verschlüsselte Kanäle übertragen, welche unbefugtes Lesen, Kopieren, Verändern oder Entfernen technisch verhindern. Backups werden vor der Übertragung verschlüsselt.

3.2 Eingabekontrolle

In der Applikation wird jede Anfrage von eingeloggten Nutzern protokolliert. Dadurch können Veränderungen oder Löschungen von Daten nachvollzogen werden. Das gilt auch für Mitarbeiter von fynk. Auf den Servern werden Login-Zeitpunkte von Systemadministratoren protokolliert.

4. Verfügbarkeit und Belastbarkeit

4.1 Verfügbarkeit

Hohe Verfügbarkeit ist kritisch für den Erfolg von fynk. AWS und Azure bieten sowohl auf Hardware-Ebene als auch auf Software-Ebene höchste Standards bezüglich Verfügbarkeit.

Die Architektur der Applikation ist auf „High Availability“ ausgelegt. „Single Points of Failure“, also Soft- und Hardware-Komponenten die bei einem Ausfall die Verfügbarkeit von fynk einschränken werden durch redundante Infrastruktur vermieden.

Durch eine erprobte Backupstrategie vermeiden wir Datenverluste weitestgehend. Datenbankbackups werden alle 2 Stunden abgelegt, Dateien alle 24 Stunden. Dabei kombinieren wir Vollspeicherungen mit inkrementellen Backups. Backups werden auf 3 verschiedenen Maschinen repliziert und zumindest halbjährlich testweise auf einem Testsystem eingespielt.

Durch die Dienstleistungen von AWS erfüllt fynk die höhsten Anforderungen bezüglich Netzwerksicherheit und DDoS Prävention.

4.2 Belastbarkeit

Die Belastbarkeit von fynk wird durch regelmäßige Kapazitäts- und Ressourcenplanung in der Infrastruktur sichergestellt.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Datenschutz-Management

fynk nutzt Software für das Datenschutz-Management. Hier werden relevante Dokumente abgespeichert und etwaige Änderungen im Datenschutz dokumentiert.

Mitarbeiter werden zumindest jährlich oder bei relevanten Neuerungen geschult.

5.2 Incident-Response-Management

Datenschutzrechtlich relevante Vorfälle werden nach einem definierten Prozess behandelt. Sollten Kundendaten betroffen sein werden die Kunden entsprechend der vertraglichen Regelungen benachrichtigt. Wenn durch den Vorfall behördliche Meldepflichten entstehen wird fynk diesen entsprechen.

5.3 Datenschutzfreundliche Voreinstellungen

Die Applikation unterstützt Datenschutzprozesse an vielen Stellen. Die Voreinstellungen sehen minimale Datenerfassung und automatisierte Datenlöschung nach entsprechenden Fristen vor. Fynk unterstützt Kunden bei der Konfiguration des Systems entsprechend den spezifischen Anforderungen bzgl. Datenschutz.

6. Auftragskontrolle

Zur Sicherstellung der Auftragskontrolle, also dass fynk die Daten der Kunden ausschließlich im Sinne der Kunden verwendet, wird ein Vertrag zur Auftragsdatenverarbeitung geschlossen, in dem Rechte und Pflichten beider Parteien definiert sind.

fynk Subauftragsverarbeiter

fynk setzt mit 27.02.2026 folgende Subauftragsverarbeiter ein, um seine Leistung für den Verantwortlichen zu erbringen:

Name	Adresse	Eingesetzt für	Verarbeitungsstandorte
Amazon AWS	Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855, Luxembourg	Hosting der fynk Anwendung	Europäischer Wirtschaftsraum
Bird	Bird B.V. Keizersgracht 268 1016 EV, Amsterdam Niederlande	SMS und WhatsApp Versand	Europäischer Wirtschaftsraum, bei Nutzung von WhatsApp: USA
Google Cloud	Google Cloud EMEA Limited 70 Sir John Rogerson’s Quay, Dublin 2, Irland	Bereitstellung von (nicht-qualifizierten) SES und AES E-Signaturen	Europäischer Wirtschaftsraum
Hetzner	Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland	Hosting des fynk AI Services	Deutschland
Intercom	Intercom R&D Unlimited Company 124 St Stephen's Green Dublin 2, DC02 C628 Irland	Customer Support	Europäischer Wirtschaftsraum, (in Ausnahmefällen USA)
Microsoft	Microsoft Ireland Operations, Ltd. One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland	Anbindung an die Azure AI Services	Europäischer Wirtschaftsraum, USA

Pusher	Pusher Ltd. 3 More London Riverside 4th Floor London, SE1 2AQ United Kingdom	Bereitstellung von Echtzeit-Komponenten für die Webanwendung	Europäischer Wirtschaftsraum
Sentry	Functional Software, Inc. d/b/a Sentry 45 Fremont Street 8th Floor San Francisco, CA 94105 United States	Automatisierte Fehler- und Fehlermeldungserstellung	Europäischer Wirtschaftsraum, (in Ausnahmefällen USA)
eIDEasy	EID Easy OÜ Telliskivi tn 60/1, Tallinn, 10412, Estonia	Bereitstellung von qualifizierten E-Signatur-Diensten (eIDAS)	Europäischer Wirtschaftsraum
pyne.ai	Pyne GmbH Große Hamburger Str. 17 10115 Berlin Germany	Onboarding von Nutzern und Bereitstellung digitaler Demos innerhalb der App	Deutschland