Auftragsverarbeitungsvertrag (AVV)

Version: AVV FC2

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

zwischen

Flixcheck GmbH, Martin-Kremmer-Str. 12, 45327 Essen, Deutschland

– nachfolgend „Verantwortlicher“ genannt –

und

der Flixcheck GmbH, Martin-Kremmer-Straße 12, 45327 Essen

– nachfolgend „Auftragsverarbeiter“ genannt –

Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen im Zusammenhang mit der SaaS-Anwendung „Flixcheck“. Dabei erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten des Verantwortlichen. Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen der Verantwortliche und der Auftragsverarbeiter diesen Vertrag. Die Regelungen des Vertrages zur Auftragsverarbeitung gehen im Zweifel den Regelungen des Hauptvertrages vor.

Die Laufzeit dieses Vertrages richtet sich nach der Dauer der Verarbeitung.

Der Gegenstand der Verarbeitung ergibt sich aus der Produktbeschreibung, den allgemeinen Geschäftsbedingungen und der Konditionenübersicht des Verantwortlichen (nachfolgend gemeinsam als „Leistungsvereinbarung“ bezeichnet).

Die Dauer der Verarbeitung richtet sich nach der Laufzeit des Hauptvertrages.
Die Verarbeitung kann über die Laufzeit des Hauptvertrages hinaus bis zur Rückgabe und Löschung bzw. Vernichtung der personenbezogenen Daten des Verantwortlichen andauern.

Die Art und der Zweck der Verarbeitung ergeben sich aus der Leistungsvereinbarung.

Die Art der personenbezogenen Daten bestimmt der Verantwortliche durch den Umfang der konkreten Nutzung und unter Beachtung der Nutzungsbedingungen des vom Auftragsverarb angebotenen Dienstes „flixcheck“ sowie gegebenenfalls auch der von dem Verantwortlich „flixcheck“ angesprochene „Check-Empfänger“. Dabei kann der Verantwortliche durch Fix der Datenfelder die konkreten Eingaben der „Check-Empfänger“ lenken.

Die Kategorien der von der Verarbeitung betroffenen Personen ergeben sich durch den Umfang der konkreten Nutzung und unter Beachtung der Nutzungsbedingungen des vom Auftragsverarbeiter angebotenen Dienstes „flixcheck“ durch den Verantwortlichen. Insbesondere sind folgende Kategorien von Personen betroffen:

- Mitarbeiter des Verantwortlichen
- Kunden des Verantwortlichen
- Interessenten des Verantwortlichen

Der Auftragsverarbeiter darf personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragsverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Die Weisungen des Verantwortlichen werden anfänglich durch diesen Vertrag und den Hauptvertrag festgelegt und können vom Verantwortlichen danach in Schriftform oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Alle erteilten Weisungen sind sowohl vom Verantwortlichen als auch vom Auftragsverarbeiter zu dokumentieren. Dem Verantwortlichen obliegt die Beurteilung der Zulässigkeit der Verarbeitung. Ist der Auftragsverarbeiter jedoch der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

Der Auftragsverarbeiter gewährleistet, dass sich die von ihm mit der Verarbeitung von personenbezogenen Daten betrauten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Der Auftragsverarbeiter trifft alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO zum angemessenen Schutz der personenbezogenen Daten des Verantwortlichen, insbesondere mindestens die in der Anlage aufgeführten Maßnahmen. Eine Änderung der getroffenen Maßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Über wesentliche Änderungen der Maßnahmen hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu unterrichten.

Die im Hauptvertrag vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der im Folgenden genannten weiteren Auftragsverarbeiter („Subunternehmer“) durchgeführt:

- Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn
- Limbozz GmbH, Winterswijker Str. 25, 46399 Bocholt
- CM Telecom Germany GmbH, Mainfrankenpark 53, 97337 Dettelbach

Bei Buchung der kostenpflichtigen Zusatzfunktion „Rechtssichere Unterschrift“ wird zusätzlich folgender Subunternehmer eingesetzt:

- nepatec GmbH, Seelhorststr. 44, 30175 Hannover

Der Auftragsverarbeiter ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründun Unterauftragsverhältnissen mit weiteren Auftragsverarbeitern („Subunternehmern“) befug zt den Verantwortlichen hiervon unverzüglich in Kenntnis, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

Der Auftragsverarbeiter informiert den Verantwortlichen in Textform rechtzeitig vorab über die Beauftragung von weiteren Subunternehmern oder Änderungen bei Unterauftragsverhältnissen. Der Verantwortliche kann in Textform unter Darlegung eines wichtigen Grundes der Beauftragung des Subunternehmers oder der Änderung bei Unterauftragsverhältnissen innerhalb von 14 Tagen nach Kenntnisnahme widersprechen. Im Fall eines begründeten Widerspruchs räumt der Verantwortliche dem Auftragsverarbeiter eine angemessene Frist zur Ersetzung des von dem Widerspruch betroffenen Subunternehmers durch einen anderen Subunternehmer ein. Ist dies dem Auftragsverarbeiter nicht möglich oder dem Verantwortlichen nicht zumutbar, ist der jeweilige Vertragspartner berechtigt, den Hauptvertrag aus wichtigem Grunde zu kündigen.

Der Auftragsverarbeiter ist verpflichtet, weitere Auftragsverarbeiter sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragsverarbeiter hat bei der Einschaltung von weiteren Auftragsverarbeitern diese entsprechend den Regelungen dieses Vertrages zu verpflichten und dabei sicherzustellen, dass der Verantwortliche seine Rechte aus diesem Vertrag (insbesondere seine Kontrollrechte) auch direkt gegenüber den weiteren Auftragsverarbeitern wahrnehmen kann. Sofern eine Einbeziehung von weiteren Auftragsverarbeitern in einem Drittland erfolgen soll, hat der Auftragsverarbeiter sicherzustellen, dass ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standardvertragsklauseln).

Unterauftragsverhältnisse mit weiteren Auftragsverarbeitern im Sinne dieser Bestimmungen liegen nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsarbeiten, Telekommunikationsleistungen und Bewachungsdienste ohne konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Verantwortlichen erbringt.

Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Personen nachzukommen.

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DS-GVO.

Der Auftragsverarbeiter wird nach Beendigung des Hauptvertrages alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löschen bzw. vernichten oder zurückgeben und die vorhandenen Kopien löschen bzw. vernichten, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

Der Auftragsverarbeiter stellt dem Verantwortlichen auf Verlangen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten des Auftragsverarbeiters nach diesem Vertrag und nach Art. 28 DS-GVO zur Verfügung.

Der Auftragsverarbeiter ermöglicht dem Verantwortlichen hierzu auch Überprüfungen - einschließlich Inspektionen -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu diesen bei. Der Verantwortliche wird Überprüfungen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragsverarbeiters dabei nicht unverhältnismäßig stören.

Für den Ersatz von Schäden, die eine betroffene Person wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen im Rahmen des Auftragsverhältnisses erleidet, haften der Verantwortliche und der Auftragsverarbeiter als Gesamtschuldner.

Macht eine betroffene Person gegenüber dem Auftragsverarbeiter Schadensersatzansprüch[illegible]en eines Verstoßes gegen datenschutzrechtliche Bestimmungen im Rahmen des Auftragsverh[illegible]s geltend, stellt der Verantwortliche den Auftragsverarbeiter von diesen Ansprüchen auf erst[illegible] Anfordern hin frei. Dies umfasst insbesondere auch die Kosten der Rechtsverteidigung einschließlich der Gerichts- und Rechtsanwaltskosten sowie Bußgelder in der tatsächlich festgesetzten Höhe. Der spätere Haftungsausgleich im Innenverhältnis gemäß Art. 82 DS-GVO bleibt hiervon unberührt. Der

Verantwortliche bleibt ausdrücklich berechtigt, den Teil des Schadensersatzes vom Auftragsverarbeiter zurückzufordern, der unter den in Art. 82 Abs. 2 DS-GVO festgelegten Bedingungen dem Anteil des Auftragsverarbeiters an der Verantwortung für den Schaden entspricht.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragsverarbeiter wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Verantwortlichen liegt.

Die Einrede des Zurückbehaltungsrechts im Sinne von § 273 BGB wird hinsichtlich der für den Verantwortlichen verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Essen, den 2.3.2022

Bestätigt von IP 87.145.117.142

Ort, Datum

Unterschrift Auftraggeber

Der Vertrag wurde digital am 2.3.2022, 15:48 Uhr von Anne Seggewiß über die IP-Adresse 87.145.117.142 mit der E-Mail-Adresse anne.seggewiss@gmx.de bestätigt.

Essen, den 2.3.2022

Ort, Datum

Unterschrift Auftragnehmer

Der Auftragsverarbeiter trifft zum angemessenen Schutz der Daten des Verantwortlichen unmittelbar erforderliche technische und organisatorische Maßnahmen. Ergänzend zu diesen Maßnahmen werden von den Subunternehmern weitere technische und organisatorische Maßnahmen realisiert.

Insbesondere folgende Sicherheitsvorkehrungen gemäß Art. 32 DS-GVO werden vom Auftragsverarbeiter umgesetzt:

a) Zutrittskontrolle

Die Zutrittskontrolle betrifft insbesondere Maßnahmen, die Unbefugten den physischen Zugang zu Datenverarbeitungsanlagen, mit denen der Auftragsverarbeiter personenbezogene Daten verarbeitet, sowie zu Dateien und Speichermedien, die personenbezogene Daten beinhalte verwehren. Der Auftragsverarbeiter setzt insoweit insbesondere folgende Maßnahmen hierz

Geschäftsrelevante Unterlagen (Verträge, Rechnungen, etc.), Systemdaten, personenbezogene Daten mit Bezug zu Vertragsdaten werden vom Auftragsverarbeiter ausschließlich zentral in der MS

OneDrive abgelegt. Diese Daten werden vor dem Transport in die MS OneDrive und dem dortigen Speichern symmetrisch verschlüsselt. Daten, die über die Flixcheck-Anwendung durch den Auftragsverarbeiter im Auftrag verarbeitet werden, werden ausschließlich in der Open Telekom Cloud (OTC) der Telekom Deutschland GmbH verarbeitet.

Alle Daten, die über die lokalen Rechner des Auftragsverarbeiters verarbeitet werden, werden insoweit bevor sie den Rechner des Mitarbeiters verlassen durch einen geteilten Schlüssel symmetrisch verschlüsselt. Dies geschieht mit Hilfe einer Verschlüsselungs-Software. Das bedeutet, dass nur Mitarbeiter des Auftragsverarbeiters Zugriff auf diese Schlüssel haben und somit die Daten nur von den Mitarbeitern gelesen und verarbeitet werden können. Der jeweilige Schlüssel wird vor Ort an die Mitarbeiter des Auftragsverarbeiters übergeben und von diesen vertraulich behandelt und verschlossen aufbewahrt. Der Schlüssel wird nicht online abgelegt bzw. gespeichert.

Der Auftragsverarbeiter bzw. die Mitarbeiter des Auftragsverarbeiters speichern keine relevanten Daten auf lokalen Endgeräten. Insoweit trägt der Auftragsverarbeiter bereits durch die ausgelagerte Datenspeicherung ausreichend Sorge für die Zutrittskontrolle. Es findet ebenfalls eine Trennung von Produktions- und Entwicklungsumgebung statt. Externe Rechenzentren und Subunternehmer, die Daten des Auftragsverarbeiters speichern und verarbeiten, werden sorgfältig und mit Blick auf den dort realisierten Datenschutz und die Datensicherheit ausgewählt.

b) Zugangskontrolle

Die Zugangskontrolle betrifft insbesondere Maßnahmen, die Unbefugten die Nutzung der Datenverarbeitungsanlagen, mit denen der Auftragsverarbeiter personenbezogene Daten verarbeitet, sowie zu Dateien und Speichermedien, die personenbezogene Daten beinhalten, verwehren, also eine unberechtigte Systembenutzung zu verhindern. Insoweit wird auch gewährleistet, dass personenbezogene Daten während der Verarbeitung ohne Autorisierung nicht gelesen, kopiert, geändert, gespeichert oder entfernt werden können. Der Auftragsverarbeiter setzt insoweit insbesondere folgende Maßnahmen hierzu um:

- Zwei-Faktor-Authentifizierung (mit Mindestlänge nach BSI-Standard bzw. Stand der Technik, sowie mit regelmäßiger Änderung und strenger Vertraulichkeit für verwendete Passwörter)
- SSH-Netzwerkprotokoll und VPN-Verbindung für den Zugriff auf die Plattforminfrastruktur
- Automatische Sperre, Abmeldung
- Berechtigungskonzepte (Beschränkung auf autorisierte Mitarbeiter auf Rollenbasis)
- Verschlüsselte Speichermedien
- Nachverfolgung unerlaubter Aktivitäten/Zugriffe
- Verkapselung sensibler Systeme durch separate Netzwerkbereiche
- Firewall, regelmäßig aktualisierte Antiviren-Programme
- Dokumentierte Richtlinie zum sicheren und ordnungsgemäßen Umgang mit Passwörtern, Sicherung (mobiler) Endgeräte und Festplattenverschlüsselung
- Die Zugangsberechtigungen werden durch den technischen Leiter vergeben. Die Verwaltung dieser Zugangsberechtigungen erfolgt durch autorisierte Administratoren.
- Ein Fernzugriff auf Server des Auftragsverarbeiters zu administrativen Zwecken, z.B. zur Wartung der Systeme, ist nur über verschlüsselte Verbindungen und nach vorheriger Authentifizierung möglich – hier: 4-Augen-Prinzip (nur überwachte Fernzugriffe)

Alle Arbeitsplatzsysteme (auch Laptops) sind zudem vor unberechtigtem Zugang geschützt. Dies erfolgt insbesondere durch obige Grundsätze sowie dadurch, dass

- alle verwendeten Arbeitsplatzsysteme sich hinter einer Firewall befinden,
- alle verwendeten Arbeitsplatzsysteme mit einer aktuellen Antiviren-Software ausgestattet sind,
- alle verwendeten Arbeitsplatzsysteme nach Inaktivität gesperrt werden,
- alle verwendeten Arbeitsplatzsysteme über eine Zwei-Faktor Authentifizierung verfügen,
- alle Mitarbeiter des Auftragsverarbeiters ausschließlich mit personalisierten Benutzerprofilen arbeiten und

- alle mobilen Datenträger (insbesondere Laptops) verschlüsselt sind.

c) Zugriffskontrolle

Die Zugriffskontrolle betrifft insbesondere Maßnahmen, die Unbefugten den Zugriff auf die Datenverarbeitungsanlagen, mit denen der Auftragsverarbeiter personenbezogene Daten verarbeitet, sowie zu Dateien und Speichermedien, die personenbezogene Daten beinhalten, verwehren. Insoweit wird auch gewährleistet, dass personenbezogene Daten während der Verarbeitung ohne Autorisierung nicht gelesen, kopiert, geändert, gespeichert oder entfernt werden können. Der Auftragsverarbeiter setzt insoweit insbesondere folgende Maßnahmen hierzu um:

- Zwei-Faktor-Authentifizierung (mit Mindestlänge, regelmäßiger Änderung und strenger Vertraulichkeit für verwendete Passwörter)
- VPN-Verbindung für den Zugriff auf die Plattforminfrastruktur
- Automatische Sperre, Abmeldung
- Berechtigungskonzepte (Beschränkung auf autorisierte Mitarbeiter auf Rollenbasis)
- Bedarfsgerechte Zugriffsrechte
- Protokollierung von Zugriffen
- Verschlüsselte Speichermedien
- Nachverfolgung unerlaubter Aktivitäten/Zugriffe
- Verkapselung sensibler Systeme durch separate Netzwerkbereiche
- Firewall, regelmäßig aktualisierte Antiviren-Programme
- Dokumentierte Richtlinie zur Zugriffskontrolle
- Dokumentierte Richtlinie zum sicheren und ordnungsgemäßen Umgang mit Passwörtern, Sicherung (mobiler) Endgeräte und Festplattenverschlüsselung
- Trennung von Produktions- und Entwicklungsumgebung

d) Trennungskontrolle

Getrennte Verarbeitung von personenbezogenen Daten, die zu unterschiedlichen Zwecken erhoben wurden: Es werden folgende Maßnahmen umgesetzt, um zu gewährleisten, dass die aus verschiedenen Anlässen erfassten Daten getrennt verarbeitet und infolgedessen von anderen Daten und Systemen abgesondert werden, um so eine ungeplante Verarbeitung dieser Daten aus anderen Gründen unmöglich zu machen:

- Berechtigungskonzepte
- Mandantenfähigkeit
- Sandboxing
- Verschlüsselte Speicherung personenbezogener Daten
- Trennung der Clients innerhalb der Software
- Trennen von Test- und Produktionssystemen
- Geografische Verteilung: Ressourcen werden über mehrere Datenzentren mit verschiedenen Netzwerken verteilt. Grundsätzliche Einbindung der Redundanz in die Infrastruktur.
- Trennung von Produktions- und Entwicklungsumgebung

Der Auftragsverarbeiter verarbeitet die Daten auf Serversystemen, die durch ein System logischer und physischer Zugriffskontrollen im Netzwerk logisch getrennt sind.

e) Weitergabekontrolle

Die Weitergabekontrolle betrifft insbesondere Maßnahmen, die Unbefugten die Weitergabe von beim Auftragsverarbeiter verarbeitete personenbezogene Daten die Weitergabe dieser Daten verwehren. Es soll demnach gewährleistet werden, dass personenbezogene Daten ohne Erlaubnis wäh[illegible]r elektronischen Übertragung oder dem Transport nicht gelesen, kopiert, geändert oder entf[illegible] werden können und dass die Überprüfung und Feststellung möglich ist, zu welcher Stelle die Übermittlung personenbezogener Daten geplant ist. Der Auftragsverarbeiter setzt insoweit insbesondere folgende Maßnahmen hierzu um:

Der Auftragsverarbeiter setzt ein zentrales System zur Verwaltung der Zugriffsberechtigungen ein. Alle Zugriffe werden lokal und im zentralen Logserver gespeichert. Administrative Rechte sind nur über ein zentrales Verwaltungsprogramm ausführbar. (Rechte-Rollen-Konzept)

Der Zugriff auf alle Daten ist bei allen Berechtigten auf das zur konkreten Aufgabenerfüllung notwendige Maß beschränkt. (Rechte-Rollen-Konzept)

Um zu gewährleisten, dass Daten bei der elektronischen Übertragung, während des Transportes oder ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft werden kann, an welchen Stellen die Übertragung von Daten durch Systeme zur Datenübertragung vorgesehen sind, unterliegt der Zugriff auf sämtliche Systeme, die Kundendaten verarbeiten, wirksamen Zugriffskontrollen. Diese Mechanismen zur Zugriffskontrolle sind bereits oben näher beschrieben.

- Übermittlung von Daten über verschlüsselte Datennetzwerke (https)
- Umfangreiche Aufzeichnungsprozesse
- Kein Datenverkehr außerhalb der EU
- Verschlüsselung
- Nutzung von Virtual Private Networks (VPN)
- Die Datenkommunikation wird verschlüsselt (z.B. VPN, SSL)
- Der Transport von E-Mails erfolgt grundsätzlich verschlüsselt (TLS)
- Beim physischen Transport werden die Transportpersonen sorgfältig ausgewählt
- Dokumentierte Richtlinie zum sicheren und ordnungsgemäßen Umgang mit Passwörtern, Sicherung (mobiler) Endgeräte und Festplattenverschlüsselung
- Trennung von Produktions- und Entwicklungsumgebung

f) Eingabekontrolle

Um zu gewährleisten, dass der Auftragsverarbeiter nachträglich überprüfen und feststellen kann, ob und von wem Daten in den Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind, werden alle Zugriffe auf die gespeicherten, personenbezogenen Daten innerhalb bzw. über die Anwendung Flixcheck protokolliert. Entsprechende Dokumentationen zu Anforderungen werden für eine Dauer von 30 Tagen aufbewahrt.

g) Verfügbarkeitskontrolle

Maßnahmen, um zu gewährleisten, dass die personenbezogenen Daten vor unbeabsichtigter Zerstörung oder unbeabsichtigtem Verlust geschützt sind:

- Datensicherung
- Backup-Strategie
- Firewall
- Replizierung der Datenbanken in mehrere Systeme
- Geografische Verteilung: Ressourcen werden über mehrere Datenzentren mit verschiedenen Netzwerken verteilt.
- Grundsätzliche Einbindung der Redundanz in die Infrastruktur
- Trennung von Produktions- und Entwicklungsumgebung

Der Auftragsverarbeiter verwendet in allen Systemen eine Kombination aus redundanten Systemen und Backup Lösungen, um die gespeicherten Daten zu schützen und ggf. wiederherstellen zu können. Diese Systeme werden ausschließlich in nach dem aktuellen Stand der Technik gesicherten und ausgestatteten Räumlichkeiten von Subunternehmern betrieben, die über die notwendige Klimatisierung, Feuer- und Rauchmeldeanlagen verfügen und für die i. d. R. detaillierte Notf[illegible]ne seitens der Subauftragsverarbeiter bestehen.

h) Permanente Zugriffsmöglichkeit und schnelle Widerherstellbarkeit

Maßnahmen zur Gewährleistung einer permanenten Verfügbarkeit und zur schnellen Wiederherstellung der Verfügbarkeit und Zugänglichkeit von Daten im Falle eines physischen oder

technischen Vorfalls.

Der Auftragsverarbeiter führt fortlaufend redundante und verteilte Datensicherung durch. Die redundanten Sicherungen werden jeweils für einen Zeitraum von 30 Tagen bereitgehalten.

Für eine ununterbrochene Lesemöglichkeit wird insbesondere die Datenbank im Swarm-Mode betrieben. Dies bedeutet, dass die Daten ständig auf verteilten Servern verarbeitet werden können und insoweit eine nahezu zeitlich ununterbrochene Schreib- und Datenverarbeitungsmöglichkeit durch die verteilten Server ermöglicht wird.

i) Auftragskontrolle

Maßnahmen, um zu gewährleisten, dass im Falle der Auftragsverarbeitung personenbezogener Daten die Daten streng im Einklang mit den Anweisungen des für die Verarbeitung Verantwortlichen verarbeitet werden. Es soll also gewährleistet werden, dass keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Verantwortlichen stattfindet. Hierzu setzt der Auftragsverarbeiter folgende Maßnahmen um:

- Unmittelbare Anweisungen des Verantwortlichen
- Überwachung der Vertragsausführung
- Für alle Mitarbeiter geltende interne Richtlinien
- Eindeutige Vertragsgestaltung
- Strenge Auswahl etwaiger Subunternehmer zur Auftragsverarbeitung
- Nachkontrolle der eigenen Mitarbeiter und der etwaigen Subunternehmer
- Detaillierte Regelung zum Auftragsverhältnis mit etwaigen Subunternehmern (insbesondere wirksame Kontroll- und Zugriffs- und Löschungsrechte)
- Trennung von Produktions- und Entwicklungsumgebung

j) Hinweise zu weiteren technischen und organisatorischen Maßnahmen des Auftragsverarbeiters

Eine pseudonymisierte Nutzung (Art. 32 Abs., 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) der Flixcheck Anwendung im Rahmen der Versendung eines Checks ist grundsätzlich möglich: Die Nutzung der Flixcheck Anwendung ist insoweit schon bei Versendung eines Checks ohne konkreten Bezug zu einem Namen möglich. Es wird insoweit seitens des Auftragsverarbeiters empfohlen, eine derartige pseudonymisierten Check-Versand durchzuführen. Hierdurch ist eine datenschutzfreundliche Verarbeitung möglich, denn diese Maßnahme zur Reduzierung personenbezogener Hinweise während der Datenverarbeitung erfolgt in einem Maß, dass der persönliche Bezug zur betroffenen Person im Rahmen dieses Verarbeitungsschrittes ohne Hinzuziehung weiterer Informationen unmöglich ist.

Die Mitarbeiter des Auftragsverarbeiters werden regelmäßig zu Themen des Datenschutzes geschult. Diese Schulungen werden komplett inhouse realisiert, sodass eine genaue Abstimmung auf die beim Auftragsverarbeiter maßgeblichen Fragen möglich ist. Es werden im Rahmen dieser Schulungen auch individuelle Fragen eingehend behandelt.

Alle Mitarbeiter des Auftragsverarbeiters, die im Rahmen ihrer Tätigkeit mit der Verarbeitung personenbezogener Daten in Berührung kommen sind auf den vertraulichen Umgang mit personenbezogenen Daten verpflichtet. Dies geschieht regelmäßig bereits bei der Einstellung neuer Mitarbeiter mittels einer vertraglichen Verpflichtungserklärung, die jeder Mitarbeiter abzugeben hat.

Der Auftragsverarbeiter hat einen Beauftragten für den Datenschutz bestellt. Dieser trägt gemeinsam mit seinen Stellvertretern Sorge für die fristgemäße Beantwortung von Anfragen Betroffener bzw. die diesbezügliche Zusammenarbeit mit dem Verantwortlichen.

Der Auftragsverarbeiter unterhält ein Verzeichnis von Verarbeitungstätigkeiten i. S. d. Art. 30 und 2 DSGVO. Dieses Verarbeitungsverzeichnis ist nicht öffentlich.

Der Auftragsverarbeiter prüft regelmäßig, nötigenfalls durch Durchführung eines Datenschutzfolgen-Abschätzung-Pre-CHECKS, ob und inwieweit die Durchführung einer Datenschutzfolgen-Abschätzung (DSFA) notwendig ist. Ist dies der Fall, nimmt der

Auftragsverarbeiter, sofern und soweit er hierfür verantwortlich ist, eine solche Abschätzung (ggf. in Abstimmung mit dem Verantwortlichen) vor und informiert den Verantwortlichen über die Durchführung und das Ergebnis. Sofern und soweit der Verantwortlichen diesbezüglich in der Verpflichtung ist, hat dieser die DSFA auf eigene Kosten durchzuführen und dem Auftragsverarbeiter die Durchführung zu dokumentieren.

Weitere Maßnahmen für die regelmäßige Bewertung der Sicherheit der Datenverarbeitung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO), um dauerhaft eine sichere Datenverarbeitung in Einklang mit den Gesetzen zu gewährleisten:

- Dokumentation der Anweisungen des Verantwortlichen an den Auftragsverarbeiter
- Dokumentation der Anweisungen des Auftragsverarbeiters an etwaige Subunternehmer
- Datenschutzfreundliche Voreinstellungen (bspw. Pseudonymisierter Betrieb der Flixcheck Anwendung, Passwortschutz der versendeten Checks)
- bereichsspezifische Datenschutzleitlinien, insbesondere Richtlinien zum Umgang mit personenbezogenen Daten und der zugehörigen IT für alle Mitarbeiter.
- Bestellung eines externen Datenschutzbeauftragten.
- Regelmäßige Schulung und Aufklärung der Mitarbeiter des Auftragsverarbeiters, um das Problembewusstsein zu fördern
- Richtlinien für Mitarbeiter, wie mit möglichen Sicherheitsvorfällen umzugehen ist
- Verfahren, wie die verantwortliche Stelle mit festgestellten oder gemeldeten Sicherheitsvorfällen umzugehen hat, insbesondere, wann der Datenschutzbeauftragte und die Datenschutzbehörde zu involvieren ist.
- Dokumentierte Prozedur bei Datenschutzverletzungen

Der Auftraggeber benennt vorliegend Anne Seggewiß als weisungsberechtigten Ansprechpartner.

Hinweis: Zur besseren Lesbarkeit wird innerhalb dieses Vertrages auf die männliche Form abgestellt. Es sind gleichsam alle Geschlechter umfasst.

✔ Der Vertrag wurde am 2.3.2022 erfolgreich abgeschlossen.

Weitere Sprachen

Hinzufügen

Speichern