Auftragsverarbeitungsvertrag (AVV)

Version: AVV FC1.2

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

zwischen

KUNDE

– nachfolgend „Auftraggeber“ genannt –

und

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

– nachfolgend „Auftragnehmer“ genannt –

1. Vertragsgegenstand

Im Rahmen der Leistungserbringung der Anwendung „flixcheck“ (nachfolgend auch: „Hauptvertrag“) ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als verantwortliche Stelle 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. Es gelten die bisherigen AGB des Auftragnehmers. Hinsichtlich der datenschutzrechtlichen Regelungen ist dieser AVV als vorrangig zu behandeln und ergänzt bzw. ersetzt bei etwaigen Erweiterungen und/oder Abweichungen zu den bisherigen Vereinbarungen diese entsprechend.

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 Auftraggeber weist auf Anfrage des Auftragnehmers diesen durch gesonderte Vereinbarung oder unter Bezugnahme auf diesen Vertrag an, Auftraggeber-Daten in anonymisierter Form neu zu aggregieren, so dass eine Identifizierung einzelner betroffener Personen nicht mehr möglich ist, folglich keine personenbezogene Daten erzeugt werden. Die Nutzung der auf diese Weise und in dieser Form erzeugten, anonymisierten Daten steht ausschließlich dem Auftragnehmer zum Zweck der bedarfsgerechten Gestaltung, der Weiterentwicklung und der Optimierung seiner

Dienste zu. Die Parteien stimmen darin überein, dass insoweit anonymisiert aggregierte Auftraggeber-Daten nicht mehr als Auftraggeber-Daten im Sinne dieses Vertrags gelten. Die dieser Aggregation zugrunde liegenden Auftraggeber-Daten bleiben zudem im unveränderten Originalbestand bestehen, unterliegen weiterhin den geltenden gesetzlichen Datenschutzbestimmungen sowie diesem Vertrag und gelten insoweit unbeschadet der durchgeführten Aggregation als Auftraggeber-Daten.

2.4

Der Auftragnehmer darf die Auftraggeber-Daten im Rahmen des datenschutzrechtlich Zulässigen für eigene Zwecke auf eigene Verantwortung verarbeiten und nutzen, wenn eine gesetzliche Erlaubnisvorschrift oder eine Einwilligungserklärung des Betroffenen dies gestattet. Auf solche Datenverarbeitungen findet dieser Vertrag keine Anwendung.

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.

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 oder einer gesonderten Vereinbarung, 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 hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten.

6. Sicherheit der Verarbeitung

6.1

Der Auftragnehmer wird – wie der Auftraggeber – 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

Zusätzliche technische und organisatorische Maßnahmen, die über die vertraglich vereinbarten Maßnahmen hinaus gehen, sind – soweit nicht etwas anderes vereinbart ist – bei Mehraufwand für den Auftragnehmer vom Auftraggeber zu vergüten. Eine entsprechend angemessene Vergütung ist insoweit gesondert zu vereinbaren. Bei Maßnahmen, deren Umsetzung der Auftragnehmer nicht oder nur mit unverhältnismäßig hohem Mehraufwand realisieren kann, kann der Auftragnehmer den Vertrag kündigen.

7. Inanspruchnahme weiterer Auftragsverarbeiter

7.1

Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter – sog. Unterauftragsverarbeiter – 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. Nicht als Unterauftragsverhältnisse in diesem Sinne sind insbesondere solche Aufträge, für die der Auftragnehmer Dritte zur Erbringung einer Nebenleistung zur Unterstützung bei der Auftragsdurchführung hinzuzieht, sofern hierdurch keine personenbezogenen Daten des Auftraggebers bzw. der Vertragspartner des Auftraggebers betroffen sind.

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 EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern vom 5.2.2010 zu schließen. Der Auftraggeber erklärt sich bereit, an der Erfüllung der Voraussetzungen nach Art. 49 DSGVO im erforderlichen Maße mitzuwirken.

7.5

Die Beauftragung von Sub-Unterauftragsverarbeiter ist nach Maßgabe der Ziffer 7.1 bis 7.4 entsprechend zulässig.

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 den betroffenen Personen zustehenden Rechte 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.

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.

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

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden.

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, durch angemessene Maßnahmen zu überprüfen. Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Etwaige Kosten, welche für weitergehende Überprüfungen anfallen, hat der Auftraggeber zu übernehmen.

11.3

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.

11.4

Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrage anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren)

oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit - z.B. nach BSI-Grundschutz - („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

12. Vertragsdauer und Kündigung

12.1

Die Laufzeit und Kündigung dieses Vertrags richtet 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.

13. Haftung

13.1

Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag, den AGB des Auftragnehmers sowie etwaigen Zusatzvereinbarungen. 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.

13.2

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.

14. Schlussbestimmungen

14.1

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.

14.2

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

Plauen, den 1.12.2020
Bestätigt von IP 193.98.119.41
Ort, Datum
Unterschrift Auftraggeber

Der Vertrag wurde digital am 1.12.2020, 16:12 Uhr von Martin Röder über die IP-Adresse 193.98.119.41 mit der E-Mail-Adresse service@vision-makler.de bestätigt.

Essen, den 1.12.2020

Ort, Datum
Unterschrift Auftragnehmer

Anlage 1: Einzelheiten der Auftragsverarbeitung

1.1 Kategorien von Verarbeitungen:

Cloud-Speicherdienst, SaaS

1.2 Beschreibung der betroffenen personenbezogenen Daten und Datenkategorien:

Die durch die Verarbeitung betroffenen personenbezogenen Daten und Datenkategorien ergeben sich jeweils durch die konkrete Art der Nutzung der Anwendung „flixcheck“ seitens des Auftraggebers sowie der „Check-Empfänger“. Der Auftraggeber kann die Datenfelder und insoweit die Abfrage der einzelnen Checks fixieren und so die Eingabe der „Check-Empfänger“ lenken. Die „Check-Empfänger“ konkretisieren dann die betroffenen personenbezogenen Daten und Datenkategorien mit ihrer Eingabe final. Der Auftraggeber hat dabei die Nutzungsbedingungen des Auftragnehmers zu beachten.

1.3 Beschreibung der betroffenen Personen / Betroffenengruppen

Die durch die Verarbeitung betroffenen Personen ergeben sich jeweils durch die konkrete Art der Nutzung der Anwendung „flixcheck“ seitens des Auftraggebers sowie der „Check-Empfänger“. Der Auftraggeber kann die Datenfelder und insoweit die Abfrage der einzelnen Checks fixieren und so die Eingabe der „Check-Empfänger“ lenken. Die „Check-Empfänger“ konkretisieren dann die betroffenen personenbezogenen Daten und Datenkategorien mit ihrer Eingabe final. Der Auftraggeber hat dabei die Nutzungsbedingungen des Auftragnehmers zu beachten.

Anlage 2: Weiteren Auftragsverarbeiter

Die vertraglich vereinbarten Leistungen werden unter Einschaltung nachfolgend genannter Subunternehmer durchgeführt:

- Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn
- Limbozz GmbH, Blücherstraße 18, 46397 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

Anlage 3: Technisch und organisatorische Maßnahmen (TOM)

Der Auftragnehmer trifft zum angemessenen Schutz der Daten des Auftraggebers unmittelbar erforderliche technische und organisatorische Maßnahmen. Ergänzend zu diesen Maßnahmen

werden von den Subunternehmern weitere technische und organisatorische Maßnahmen realisiert.

Insbesondere folgende Sicherheitsvorkehrungen werden vom Auftragnehmer umgesetzt:

a) Zutrittskontrolle

Die Zutrittskontrolle betrifft insbesondere Maßnahmen, die Unbefugten den physischen Zugang zu Datenverarbeitungsanlagen, mit denen der Auftragnehmer personenbezogene Daten verarbeitet, sowie zu Dateien und Speichermedien, die personenbezogene Daten beinhalten, verwehren. Der Auftragnehmer setzt insoweit insbesondere folgende Maßnahmen hierzu um:

Geschäftsrelevante Unterlagen (Verträge, Rechnungen, etc.), Systemdaten, personenbezogene Daten mit Bezug zu Vertragsdaten werden vom Auftragnehmer 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 Auftragnehmer 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 Auftragnehmers 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 Auftragnehmers 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 Auftragnehmers übergeben und von diesen vertraulich behandelt und verschlossen aufbewahrt. Der Schlüssel wird nicht online abgelegt bzw. gespeichert.

Der Auftragnehmer bzw. die Mitarbeiter des Auftragnehmers speichern keine relevanten Daten auf lokalen Endgeräten. Insoweit trägt der Auftragnehmer 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 Auftragnehmers 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 Auftragnehmer 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 Auftragnehmer 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 Auftragnehmers 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 Auftragnehmers 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 Auftragnehmer 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 Auftragnehmer 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) Weitergabekontrolle

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

Der Auftragnehmer 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

e) Eingabekontrolle

Um zu gewährleisten, dass der Auftragnehmer 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.

f) 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 Auftraggebers stattfindet. Hierzu setzt der Auftragnehmer folgende Maßnahmen um:

- Unmittelbare Anweisungen des Auftraggebers
- 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

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 Auftragnehmer 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 Notfallpläne seitens der Subauftragsverarbeiter bestehen.

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 Auftragnehmer führt fortlaufend redundante und verteilte Datensicherung durch. Die redundanten Sicherungen werden jeweils für einen Zeitraum von 30 Tagen bereit gehalten.

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.

h) Trennungskontrolle

Getrennte Verarbeitung von pb 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 Auftragnehmer verarbeitet die Daten auf Serversystemen, die durch ein System logischer und physischer Zugriffskontrollen im Netzwerk logisch getrennt sind.

Hinweise zu weiteren technischen und organisatorischen Maßnahmen des Auftragnehmers:

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

Alle Mitarbeiter des Auftragnehmers, 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 Auftragnehmer 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 Auftragnehmer unterhält ein Verzeichnis von Verarbeitungstätigkeiten i. S. d. Art. 30 Abs. 1 und 2 DSGVO. Dieses Verarbeitungsverzeichnis ist nicht öffentlich.

Der Auftragnehmer prüft regelmäßig, nötigenfalls durch Durchführung eines Datenschutzfolgen-Abschätzung-Pre-CHECKS, ob und inwieweit die Durchführung eines Datenschutzfolgen-Abschätzung (DSFA) notwendig ist. Ist dies der Fall, nimmt der Auftragnehmer, sofern und soweit er hierfür verantwortlich ist, eine solche Abschätzung (ggf. in Abstimmung mit dem Auftraggeber) vor und informiert den Auftraggeber über die Durchführung und das Ergebnis. Sofern und soweit der Auftraggeber diesbezüglich in der Verpflichtung ist, hat dieser die DSFA auf eigene Kosten durchzuführen und dem Auftragnehmer 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 Auftraggebers an den Auftragnehmer
- Dokumentation der Anweisungen des Auftragnehmers 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 Auftragnehmers, 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

Anlage 4: Weisungsberechtigte Personen

Sofern und soweit nichts Abweichendes geregelt ist, ist der Auftraggeber als Verantwortlicher im Sinne des Art 4 lit. 7 DSGVO weisungsberechtigte Person. Insoweit sind alle Gesellschafter einer GbR bzw. Partner einer Partnerschaftsgesellschaft, der Inhaber einer Firma und die gesetzlichen Vertreter (Organe) einer juristischen Person weisungsberechtigt. Hinterlegt der Auftraggeber zum

Zeitpunkt des Vertragsschlusses dieses AVV einen abweichenden Ansprechpartner in seinen Stammdaten, so ist dieser ebenfalls weisungsberechtigt.

Weisungsempfänger beim Auftragnehmer sind Andreas Baum und David Simons.

Der Auftraggeber benennt vorliegend Martin Röder als weisungsberechtigten Ansprechpartner.

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