DIE SCHITTIGS

Vereinbarung zur Auftragsdatenverarbeitung

gemäß Art. 28 Abs. 3 DSGVO

Die Vertragsparteien

- im Folgenden: Auftraggeber -

und

Die Schittigs GmbH
Erthalstr. 9
63739 Aschaffenburg

- im Folgenden: Auftragsverarbeiter –

schließen folgenden Vertrag:

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Vereinbarung die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform dient der besseren Verständlichkeit und beinhaltet keine Wertung.

1. Allgemeine Bestimmungen und Auftragsgegenstand

1.1. Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragsverarbeiter (Art.

28 DSGVO). Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Vereinbarung sind Anlage 1 zu entnehmen.

1.2. Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er allein ist für Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge nach Art. 6 DSGVO und die Wahrung der Betroffenenrechte verantwortlich.

1.3. Die Verarbeitung der Daten durch den Auftragsverarbeiter findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR-Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung des Auftraggebers.

1.4. Die Vergütung wird außerhalb dieses Vertrags vereinbart.

2. Vertragslaufzeit und Kündigung

Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3.1. Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragsverarbeiter zu. In dieser Rolle kann er insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragsverarbeiter ist verpflichtet, den Weisungen des Auftraggebers Folge leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.

3.2. Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragsverarbeiter substantiiert anzweifelt, ist der Auftragsverarbeiter berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.

3.3. Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisung sind auf Verlangen des Auftragsverarbeiters schriftlich oder in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragsverarbeiter hat Person,

Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

3.4. Der Auftraggeber benennt auf Verlangen des Auftragsverarbeiters eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragsverarbeiter unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4.1. Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren oder durch Dritte kontrollieren zu lassen. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragsdatenverarbeiter einen Vergütungsanspruch geltend machen. Dies gilt, sofern Kontrollen beim Auftragsdatenverarbeiter mehr als einen Personentag in Anspruch nehmen oder externe Kosten entstehen. Externe Kosten werden ohne Aufschlag weiter belastet. Er wird dem Auftraggeber insbesondere die für die Kontrollen relevanten Auskünfte vollständig und wahrheitsgemäß erteilen, ihm die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme/ -systeme gewähren sowie Vorort-Kontrollen ermöglichen. Sofern der Auftraggeber der Verarbeitung der Daten außerhalb der Geschäftsräume (z.B. Privatwohnung) zugestimmt hat, hat der Auftragsverarbeiter dafür zu sorgen, dass der Auftraggeber auch diese Räume zu Kontrollzwecken begehen darf.

4.2. Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragsverarbeiters nicht mehr als erforderlich beeinträchtigen. Insbesondere sollen Vor-Ort-Kontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Vorlauffrist erfolgen, sofern der Kontrollzweck einer vorherigen Ankündigung nicht widerspricht.

4.3. Die Ergebnisse der Kontrollen und Weisungen sind von beiden Vertragsparteien in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragsverarbeiters

5.1. Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragsverarbeiter erfolgt ausschließlich auf Grundlage der vertraglichen

Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedstaatlicher Rechtsvorschriften zulässig (z.B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragsverarbeiter dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.2. Der Auftragsverarbeiter hat bei der Auftragsdurchführung sämtliche gesetzlichen Vorschriften einzuhalten. Er hat insbesondere die nach Art. 32 DSGVO notwendigen technischen und organisatorischen Maßnahmen implementieren und das nach Art. 30 Abs. 2 DSGVO erforderliche Verzeichnis von Verarbeitungstätigkeiten zu führen.

5.3. Sofern der Auftragsverarbeiter nach der DSGVO oder sonstigen gesetzlichen Vorschriften zur Benennung eines Datenschutzbeauftragten verpflichtet ist, bestätigt er, dass er einen solchen in Einklang mit den gesetzlichen Vorschriften ausgewählt hat und sichert dem Auftraggeber zu, diesen unter Angabe seiner Kontaktdaten zu benennen (z.B. per E-Mail). Änderungen über Person und / oder Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber unverzüglich mitzuteilen.

5.4. Die Datenverarbeitung außerhalb der Betriebsstätten des Auftragsverarbeiters oder der Subunternehmer und / oder in Privatwohnungen (z.B. Fernzugriff oder Homeoffice des Auftragsverarbeiters) ist nur mit ausdrücklicher Zustimmung des Auftraggebers gestattet.

5.5. Der Auftragsverarbeiter hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

5.6. Der Auftragsverarbeiter wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

6. Technische und organisatorische Maßnahmen

6.1. Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 2 dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt und mit dem Auftraggeber abgestimmt.

6.2. Der Auftragsverarbeiter wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen. Erforderliche Anpassungen werden vom Auftragsverarbeiter dokumentiert und dem Auftraggeber auf Nachfrage zur Verfügung gestellt. Wesentliche Änderungen, durch die das Schutzniveau verringert werden könnte, sind vorab mit dem Auftraggeber abzustimmen.

7. Unterstützungspflichten des Auftragsverarbeiters

7.1. Der Auftragsverarbeiter wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Reichweite der Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung.

7.2. Der Auftragsverarbeiter wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

8. Mitteilungspflichten des Auftragsverarbeiters

8.1. Verstöße gegen diesen Vertrag, gegen die Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragsverarbeiter selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

8.2. Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten nach Art. 33 und 34 DSGVO zu unterstützen. Eigenständige Meldungen an Behörden oder Betroffene nach Art. 33 und 34 DSGVO darf der Auftragsverarbeiter erst nach vorheriger Weisung des Auftraggebers durchführen.

8.3. Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragsverarbeiter um Auskunft, Berichtigung, Sperrung oder Löschung, wird der Auftragsverarbeiter die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragsverarbeiter dem Ersuchen des Betroffenen ohne Zustimmung des Auftraggebers nachkommen.

8.4. Der Auftragsverarbeiter wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragsverarbeiter den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

9. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen). Der Auftraggeber ist berechtigt, die Maßnahmen des Auftragsverarbeiters in geeigneter Weise zu überprüfen. Hierzu ist er insbesondere berechtigt, die einschlägigen Löschprotokolle und die betroffenen Datenverarbeitungsanlagen vor Ort in Augenschein zu nehmen.

10. Datengeheimnis und Vertraulichkeit

10.1. Der Auftragsverarbeiter ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln und einschlägige Geheimnisschutzregeln, denen der Auftraggeber unterliegt (z.B. § 203 StGB), zu beachten. Der Auftraggeber ist verpflichtet, den

Auftragsverarbeiter bei Auftragserteilung auf ggf. bestehende besondere Geheimnisschutzregeln hinzuweisen.

10.2. Der Auftragsverarbeiter verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragsverarbeiter aufnehmen.

10.3. Der Auftragsverarbeiter wird die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise dokumentieren. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

11. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

11.1. Als Unterauftragsverhältnisse sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsdatenverarbeiter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragsdatenverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

11.2. Der Auftragsdatenverarbeiter setzt nur Subunternehmer ein, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen im Sinne von Art. 32 DSGVO so durchgeführt werden, dass die Verarbeitung im Einklang mit dieser Vereinbarung erfolgt. Es obliegt dem Auftragsdatenverarbeiter, die Zusammenarbeit mit dem Subunternehmer entsprechend Art. 28 DSGVO vertraglich auszugestalten und regelmäßig zu kontrollieren. Alle Unterlagen, die Eignung und Kontrolle der Subunternehmer belegen, sind dem Auftraggeber auf Verlangen zugänglich zu machen. Zudem ist der Auftragsdatenverarbeiter für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Subunternehmer verantwortlich. Er haftet gegenüber dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.

11.3. Die durch den Auftragsdatenverarbeiter eingesetzten Subunternehmer sind in Anlage 3 aufgeführt.

11.4. Die Auslagerung auf weitere Subunternehmer oder die Ersetzung der aufgeführten Subunternehmer ist zulässig, soweit der Auftragsdatenverarbeiter dies dem Auftraggeber eine angemessene Zeit vorab in Textform anzeigt und der Auftraggeber nicht bis zum Zeitpunkt der Auslagerung oder Ersetzung gegenüber dem Auftragsdatenverarbeiter in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO oder eine andere rechtsgültige Garantie zur Gewährleistung des Datenschutzes und der Datensicherheit zugrunde gelegt wird. Im Falle des Einspruchs steht dem Auftragsdatenverarbeiter ein außerordentliches Kündigungsrecht sowohl hinsichtlich dieser Vereinbarung als auch bezüglich der Leistungsvereinbarung zu.

12. Schlussbestimmungen

12.1. Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

12.2. Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

12.3. Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

12.4. Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

_____, den _____ Aschaffenburg, den _____

Ort Datum

_____ _____

Unterschrift (Auftraggeber) Unterschrift (Auftragsverarbeiter)

Anlage 1 – Auftragsdetails

I. Umfang, Art und Zweck der Datenverarbeitung

Datenverarbeitungszweck ist das Bereitstellen eines Online Countdownkalenders unter tuerchen.com. Um diesen Zweck zu erfüllen, geben wir die hochgeladenen Inhalte und angegebene personenbezogene Daten auf tuerchen.com an unseren Serverbetreiber netcup GmbH weiter. Rechnungsdaten werden zur Zahlungsabwicklung an unseren Partner easybill weitergegeben. Die im Rahmen von Gewinnspielen u.ä. erhobenen E-Mail-Adressen von Nutzern des Kalenders werden an den Auftraggeber weitergegeben.

II. Art der Daten

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

- IP-Adressen
- Bestelldaten
- Bilder und Texte
- E-Mail-Adressen
- Adressdaten

III. Kreis der von der Datenverarbeitung Betroffenen

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

- Websitebesucher (Nutzer des Kalender)
- Auftraggeber (Käufer des Kalenders)

IV. Art des Zugriffs

Der Zugriff auf die betroffenen Daten geschieht in folgender Weise:
Der Auftraggeber erteilt dem Auftragsverarbeiter mit Erstellung eines Kalenders den Auftrag, die in Punkt II. beschriebenen Daten weiter zu geben, um ihm die Möglichkeit der Nutzung des Online Countdownkalenders zu ermöglichen. Außerdem darf der Auftragsverarbeiter die Nutzerdaten bei Teilnehmern von Gewinnspielen u.ä. abfragen, um sie dem Auftraggeber zur Verfügung zu stellen.

Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

Der Auftragsverarbeiter setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt.

I. Zweckbindung und Trennbarkeit

Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Berechtigungskonzept
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen / Datenfeldern / Signaturen
- Trennung von Produktiv- und Testsystem

II. Vertraulichkeit und Integrität

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des Auftragsverarbeiters:

1. Verschlüsselung

Die im Auftrag verarbeiteten Daten bzw. Datenträger werden in folgender Weise verschlüsselt:

- Passwörter und Zugangsdaten werden mit der Ellyptischen Kurve P521 verschlüsselt

Pseudonymisierung:

- „Pseudonymisierung“ bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt (z.B. Verwendung von Fantasienamen oder Hashes, die ohne zusätzliche Informationen keiner bestimmten Person zugeordnet werden können)
  -> IOTA Blockchain

2. Zutrittskontrolle:
Es wurden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern:

- Manuelles Schließsystem
- Videoüberwachung der Zugänge (Selbst gehostets System, Zugriff nur durch CTO und Administrator, Aufzeichnung außerhalb der Geschäftszeiten)
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Reinigungspersonal
- Sichtschutz gegen Einsicht an den Fenstern

3. Zugangskontrolle:
Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Passwort-Richtlinien (Mindestlänge, Komplexität etc.)
- Zwei-Faktor-Authentifizierung
- Authentifikation mit Benutzername / Passwort
- Einsatz von VPN-Technologie bei der Übertragung von Daten
- Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- Einsatz einer Software-Firewall
- Einsatz selbst-gehosteter Software im eigenen Netzwerk

4. Zugriffskontrolle:
Es wurden folgende Maßnahmen getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werde können:

- Berechtigungskonzept laut Mitarbeiterhandbuch
- Verwaltung der Rechte durch Systemadministrator

- regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)
- Anzahl der Administratoren ist das „Notwendigste“ reduziert
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Einsatz von Aktenvernichtern
- Zusätzliche Sicherung der Aktenschränke mit Schließsystemen

5. Eingabekontrolle:
Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

6. Auftragskontrolle:
Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Vorherige Prüfung und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
- Legitimation: Schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart

7. Transport- bzw. Weitergabekontrolle:
Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können:

- Einsatz von VPN-Tunneln

- Verschlüsselung der Kommunikationswege (z.B. Verschlüsselung des E-Mail-Verkehrs)

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuerlöschgeräte nahe der Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Backup- & Recovery-Konzepts
- Testen von Datenwiederherstellung

IV. Organisatorische Datenschutzmaßnahmen

- schriftliche interne Verhaltensregeln, von den Mitarbeitern unterzeichnet
- Schulung der Mitarbeiter zu Verhalten hinsichtlich Datenschutz und Softwareaktualität

V. Datensparsamkeit

Folgende Maßnahmen gewährleisten die Datensparsamkeit zusätzlich

- Regelmäßige Löschroutinen für interne Daten (z.B. Bewerberdaten alle 6 Monate) sowie für Corona-Impf- & Test-Daten (alle 6 Monate)
- Speicherung der Kundendaten nur soweit dem Projektstand erforderlich

V. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von 1 Jahr und anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen.

Anlage 3 – Liste der Subunternehmer

Hauptleistungen Kalender-Besucher

- Netcup GmbH: Daimler Str. 25, 76185 Karlsruhe
  Zweck: Hosting
- Mailgun (EU-Server): Mailgun Technologies, Inc., 112 E Pecan St #1135, San Antonio, TX 78205
  Zweck: Versand von E-Mails bei Funktion ‘Kalender melden’. Dies kann, muss aber nicht genutzt werden.

Hauptleistungen türchen.com Kunden und Kalender-Bearbeiter

- Zoho Corporation GMBH("Zoho"): Trinkausstr. 7, 40213 Düsseldorf
  Zweck: Ticketmanagement zur Beantwortung von Supportanfragen
- Netcup GmbH: Daimler Str. 25, 76185 Karlsruhe
  Zweck: Hosting
- easybill GmbH, Düsselstr. 21, 41564 Kaarst
  Zweck: Rechnungsstellung
- CleverReach GmbH & Co. KG, Schafjückenweg 2 26180 Rastede
  Zweck: Versand von Newslettern für angemeldete Nutzer
- Mailgun (EU): Mailgun Technologies, Inc., 112 E Pecan St #1135, San Antonio, TX 78205
  Zweck: Versand von E-Mails zum Vertragsschluss und bei Supportanliegen