# Vertrag zur Auftragsverarbeitung

zwischen der Firma

_____
(Unternehmensname)

_____
(Straße und Hausnummer)

_____
(Postleitzahl und Ort)

_____
(Land)

- nachstehend Auftraggeber genannt -

und der

**Happy Contests UG**
**(haftungsbeschränkt)**

Maximilianstraße 14
86150 Augsburg
Deutschland

_____
gesetzlich vertreten durch Bernd Ulrich Morgner (Geschäftsführer)
Auftragsverarbeiter

- nachstehend Auftragnehmer genannt -

## 1. Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz im Sinne des Art. 28 DSGVO. Sie findet Anwendung auf alle Tätigkeiten, die im Zusammenhang mit den vereinbarten Leistungen das Auftragnehmers stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen.

## 2. Gegenstand und Dauer der Vereinbarung

Der Auftragnehmer erhebt, verarbeitet und nutzt personenbezogene Daten im Auftrag des Auftraggebers. Der Auftrag umfasst Folgendes:

### 2.1 Gegenstand des Auftrags

Gegenstand des Auftrags zum Datenumgang ist die Durchführung von Online Marketing-Kampagnen (nachfolgend „Applikationen“ genannt) auf den Servern von Happy Contests. Dies umfasst das Hosting der Applikationen sowie die Bereitstellung eines Administrationsbereichs zur Gestaltung, Bereitstellung und Pflege der Applikationen sowie der Nutzerverwaltung der Teilnehmer (in der Regel Kunden des Auftraggebers). Der Auftraggeber möchte zum aktuellen Zeitpunkt der Beauftragung bzw. zukünftig folgende Applikationen nutzen (bitte entsprechende Optionen ankreuzen).

- □ Online Marketing Toolbox als Flatratemodell (= unterschiedliche Applikationen)
- □ Gewinnspiele (z.B. Verlosungen, Umfragen,…)
- □ Wettbewerbe (z.B. Foto-, Video-, Ideenwettbewerbe,...)
- □ Saisonale Kampagnen (z.B. Adventskalender, Ostersuchbilder,…)
- □ Interaktive Grafiken (z.B. Digitale Landkarten, interaktive Produktbilder,…)
- □ Tippspiele (z.B. Tippspiele zur EM, WM, Bundesliga,…)
- □ Quiz / Tests (z.B. Wissensquiz, Persönlichkeitstests,…)
- □ Spiele (z.B. Glücksrad, Rubbellos,…)
- □ Sonstiges: _____

### 2.2 Dauer des Auftrags

2.2.1 Dieser Vertrag wird auf unbestimmte Zeit geschlossen und richtet sich nach der Laufzeit der vom Auftragnehmer bereitgestellten Applikationen. Mit Ausnahme von

Tippspielen kann der Auftraggeber die Dauer seiner genutzten Applikationen selbständig über den Administrationsbereich bestimmen. Bei Tippspielen ergibt sich die Vertragslaufzeit durch die Dauer des zu tippenden Sportevents (z.B. WM 2018, Bundesliga 2018/2019, EM 2020,…). Zusätzlich zur Dauer des zu tippenden Sportevents kommen eine Vorbereitungszeit (= Erwerb der Applikation ist Vertragsbeginn) und eine Nachbereitungszeit (bis maximal 1 Monat nach Ende des Sportevents).

2.2.2 Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieses Vertrags vorliegt oder der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will.

**2.3 Umfang, Art und Zweck der Datenerhebung, Datenverarbeitung oder Datennutzung**

2.3.1 Die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten dieses Auftrags erfolgen ausschließlich zweckgebunden nach Maßgabe der DSGVO, den dieser Vereinbarung zu Grunde liegenden Bestellungen, den Regelungen dieser Vereinbarung und den Weisungen des Auftraggebers.

2.3.2 Der Zweck der Datenerhebung, -verarbeitung oder -nutzung besteht in der Durchführung von kurzen Online Marketing-Kampagnen durch den Auftraggeber.

2.3.3 Zur Art der Datenerhebung, -verarbeitung oder -nutzung gehören hierbei:

(durch den Auftraggeber vollständig und richtig auszufüllen/anzukreuzen)

- □ Personenstammdaten
- □ Kommunikationsdaten (z.B. Telefon, E-Mail)
- □ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- □ Kundenhistorie
- □ Vertragsabrechnungs- und Zahlungsdaten
- □ Planungs- und Steuerungsdaten
- □ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- □ Sonstige Daten: _____

_____

_____

_____

2.3.4 Zudem hat der Auftraggeber die Möglichkeit, in den verwendeten Applikationen den Umfang, die Art und den Zweck der erhobenen, verarbeiteten und genutzten Daten selbständig zu definieren. Neben der IP-Adresse und der E-Mail-Adresse können hierfür weitere personenbezogene Daten von Adressaten der verwendeten Applikationen erfasst werden. Beispielsweise können das sein:

- Vorname / Nachname (optional einstellbar)
- Kontaktdaten / Adresse (optional einstellbar)
- Interessen und Meinungen des Teilnehmers (optional einstellbar)
- Systemprotokolldaten (IP-Adresse, Timestamp, Standortdaten, etc.)
- Sonstige Daten: _____

_____

_____

_____

**2.4 Kreis der Betroffenen**

2.4.1 Der Kreis der durch den Umgang mit den Daten Betroffenen umfasst: (durch den Auftraggeber vollständig und richtig auszufüllen/anzukreuzen)

□ Kunden

□ Interessenten

□ Abonnenten

□ Beschäftigte

□ Lieferanten

□ Handelsvertreter

□ Ansprechpartner

□ Sonstige Betroffene: _____

_____

_____

_____

2.4.2 Zudem hat der Auftraggeber die Möglichkeit, in den verwendeten Applikationen den Kreis der Betroffenen selbständig zu definieren. Je nach Einstellung des Auftraggebers können das

beispielsweise Webseiten- und Facebook Fanpage-Besucher des Auftraggebers sein sowie Besucher der Kampagnenseite der Online-Applikation.

**3. Rechte und Pflichten des Auftraggebers**

3.1 Für die Beurteilung der Zulässigkeit der Datenverarbeitung, -erhebung oder -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

3.2 Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und schriftlich festzulegen.

3.3 Der Auftraggeber ist gegenüber dem Auftragnehmer hinsichtlich der nach dieser Vereinbarung durchgeführten Auftragsverarbeitung weisungsbefugt. Der Auftraggeber behält sich das Recht vor, jederzeit ergänzende Weisungen bezüglich Zweck, Art und Umfang der Verarbeitung von Daten an den Auftragnehmer zu erteilen. Der Auftraggeber dokumentiert an den Auftragnehmer erteilte Weisungen. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

3.4 Die folgenden Mitarbeiter des Auftraggebers sind befugt, dem Auftragnehmer hinsichtlich des Auftrags Weisungen zu erteilen.

Hinweis: Weisungsbefugte Personen bitte wie im folgenden Beispiel aufführen.
Vorname Nachname, Unternehmensname, Straße & Hausnummer, Postleitzahl & Ort

_____

_____

_____

_____

_____

_____

_____

3.5 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Die Vertragspartner legen die von ihnen

eingegangen Verpflichtungen zur Geheimhaltung und zum Datenschutz auch allen Personen und Gesellschaften auf, die von ihnen im Rahmen der Zusammenarbeit beauftragt werden.

3.6 Der Auftraggeber kann sich vor Beginn der Datenverarbeitung und danach regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit überzeugen. Der dem Auftragnehmer entstehende Arbeitsaufwand durch die Kontrollen, kann dem Auftraggeber mit einem angemessenen Stundensatz in Rechnung gestellt werden.

3.7 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

**4. Rechte und Pflichten des Auftragnehmers**

4.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers und ist zur Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO verpflichtet. Der Auftragnehmer befolgt und hält die sich aus den gültigen Datenschutzgesetzen ergebenden Verpflichtungen ein. Er hat personenbezogene Daten zu berichtigen, deren Verarbeitung einzuschränken und zu löschen, wenn der Auftraggeber dies in der getroffenen Vereinbarung oder einer Weisung verlangt.

Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Explizit davon ausgenommen sind Datensicherungen.

Die dem Auftragnehmer vom Auftraggeber im Zusammenhang mit dem Auftrag überlassenen Daten verbleiben im Eigentum des Auftraggebers.

4.2 Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.

4.3 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt. Jede Verlagerung in einen anderen Mitgliedsstaat der Europäischen Union oder in einen anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum bedarf der vorherigen Zustimmung des Auftraggebers und darf nur dann erfolgen, wenn die besonderen Voraussetzungen der Art. 44 – 50 DSGVO erfüllt sind.

4.4 Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden – automatisierten – Verwaltung. Eingang und Ausgang werden dokumentiert.

4.5 Der Transfer von Daten über Datennetze oder unter Einsatz von geeigneten Datenträgern erfolgt unter Verwendung geeigneter Verschlüsselungsmethoden und unter Beachtung der hinsichtlich eines datenschutzkonformen Transfers von Daten notwendigen technischen und organisatorischen Maßnahmen.

4.6 Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

4.7 Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

4.8 Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und die vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren. Der Auftragnehmer wird den Auftraggeber bei der Durchführung von Kontrollen durch den Auftraggeber unterstützen und an der vollständigen und zügigen Abwicklung der Kontrolle mitwirken. Der dem Auftragnehmer entstehende Arbeitsaufwand durch die Kontrollen, kann dem Auftraggeber mit einem angemessenen Stundensatz in Rechnung gestellt werden.

4.9 Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

4.10 Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen. Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 31, 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers

erbringt, betreffen kann. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer gesetzlichen Pflichten zusammen.

4.11 Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

4.12 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 - 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.

**5. Technisch-organisatorische Maßnahmen**

5.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben.

Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

5.2 Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 EU-DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 EU-DSGVO zu berücksichtigen.

5.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

**6. Berichtigung, Einschränkung und Löschung von Daten**

6.1 Der Zweck der Datenerhebung, -verarbeitung oder -nutzung besteht in der Durchführung von kurzen Online Marketing-Kampagnen durch den Auftraggeber. Da der Auftraggeber hierfür selbständig definieren kann, ob und wann er Daten berichtigt, einschränkt oder löscht, darf der Auftragnehmer die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken.

Eine Ausnahme stellt das Applikationsformat „Tippspiele“ dar. Hierfür löscht der Auftragnehmer, die Daten, die über das Applikationsformat „Tippspiele“ erhoben, verarbeitet und genutzt werden, maximal 1 Monat nach offiziellem Ende des zu tippenden Sportevents. Beispiel: Finale der WM 2018 findet am 15. Juli 2018 statt -> Daten werden spätestens am 15. August 2018 gelöscht.

6.2 Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

**7. Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 EU-DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Bestellung eines Datenschutzbeauftragten. Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Fabio Marcantonio, Happy Contests UG (haftungsbeschränkt), Maximilianstraße 14, 86150 Augsburg, fabio.marcantonio@happy-contests.de bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 EU-DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Artt. 28 Abs. 3 S. 2 lit. c, 32 E-DSGVO.

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, 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.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse.

**8. Unterauftragsverhältnisse**

8.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer 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 Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

8.2 Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

8.3 Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu, die zum Zeitpunkt der Beauftragung eingesetzt werden:

| **Unterauftragnehmer** | **Anschrift / Land** | **Leistung** |
|---|---|---|
| Hetzner Online GmbH | Industriestr. 25<br>91710 Gunzenhausen<br>Deutschland | Hosting |
| dogado GmbH | Saarlandstr. 25<br>44139 Dortmund<br>Deutschland | Hosting |

8.4 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

8.5 Der Auftraggeber hat innerhalb des Einrichtungsprozesses seiner Applikation die Möglichkeit Integrationen zur Datenweitergabe zu Drittanbietern zu aktivieren (z.B. Mailchimp). Diese Integrationen sind gemäß Art. 25 DSGVO standardmäßig deaktiviert (“Privacy by default”). Aktiviert der Auftraggeber eine solche Integration werden personenbezogene Daten an Drittanbieter weitergereicht und dort verarbeitet.

Der Auftragnehmer hat mit diesen Drittanbietern keine Auftragsdatenverarbeitungsverträge gemäß dieser Vereinbarung, weshalb der Auftragnehmer für die Wahrung der Vorschriften dieser Vereinbarung bei Aktivierung von Integrationen mit Drittanbietern keine Gewähr übernimmt und diese ab Übermittlung der Daten an den Drittanbieter nicht mehr garantiert.

8.6 Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers und des Hauptauftragnehmers (mind. Textform).

**9. Unterstützung des Auftraggebers bei der Einhaltung dessen Pflichten**

9.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der EU-DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, zur Meldepflichten bei Datenpannen, zur Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören insbesondere

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie

die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,

- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung und
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

9.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

**10. Haftung**

Die Haftung von Auftraggeber und Auftragnehmer bestimmt sich im Außen- und Innenverhältnis nach den Vorgaben des Art. 82 EU-DSGVO. Etwaige abweichende Haftungsregelungen in der Leistungsvereinbarung finden keine Anwendung.

**11. Salvatorische Klausel, Gerichtsstand**

11.1 Sollte eine Bestimmung dieses Vertrags ungültig oder undurchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieses Vertrags davon unberührt. Die Parteien vereinbaren, die ungültige oder undurchsetzbare Bestimmung zu ersetzen, welche wirtschaftlich die Zielsetzung der Partien am nächsten kommt. Das Gleiche gilt im Falle einer Regelungslücke.

11.2 Als Gerichtsstand wird Augsburg vereinbart.

……...

Anlage 1: Technisch-organisatorische Maßnahmen der Happy Contests UG

Anlage 2: Technisch-organisatorische Maßnahmen der Hetzner Online GmbH

Anlage 3: Technisch-organisatorische Maßnahmen der dogado GmbH

……...

Der Auftraggeber bestätigt, dass der Vertrag zur Auftragsverarbeitung samt seinen Anlagen ohne Änderungen unterschrieben wurde.

……....., den ……
Ort Datum

_____
Firmenstempel / Unterschrift des Autraggebers

_____
Auftragnehmer: Happy Contests UG (haftungsbeschränkt)
Firmenstempel / Unterschrift

# Anlage 1: Technisch organisatorische Maßnahmen

## Happy Contests

**Allgemeine Informationen und Standorte der Datenverarbeitungsanlagen:**

Die Happy Contests UG betreibt ein Büro in der Maxpassage ®, Maximilianstraße 14, 86150 Augsburg, Deutschland.

Das Hosting der Softwareanwendungen wird bei der Hetzner Online GmbH (Dedicated Server) und bei dogado GmbH (Jelastic Cloud Hosting) durchgeführt. Die technisch organisatorischen Maßnahmen von Hetzner Online GmbH und dogado GmbH finden Sie als Anlagen beigefügt.

### 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

#### a) Zutrittskontrolle

Der Zutritt zu den Büroräumen der Happy Contests UG ist ausschließlich mit einem Sicherheitsschlüssel möglich. Alle Schlüssel zu den Büroräumen sind registriert und mit Kopierschutz versehen.

Die Weitergabe der Schlüssel ist untersagt. Ein Verlust des Schlüssels ist sofort zu melden. Dies wird bei Aushändigung der Schlüssel an alle Mitarbeiter per Unterschrift bestätigt.

Das Gebäude wird zu Ende der Bürozeiten durch einen Wach- und Schließdienst betreut, welcher eine Verriegelung des Zugangs zum Bürogebäude sicherstellt.

Die Rechenzentren der Hetzner Online GmbH sind nach ISO/IEC 27001 zertifiziert. https://www.hetzner.de/pdf/FOX_Zertifikat_de.pdf

Unbefugten wird somit der Zutritt zu den Datenverarbeitungsanlagen nicht ermöglicht.

#### b) Zugangskontrolle

Alle Rechner der Happy Contests UG sind mit Passwort geschützt. Des Weiteren sind Bildschirmschoner mit Passwortaufforderung konfiguriert.

Passwörter müssen Mindest-Komplexitätsanforderungen der unternehmensweiten Richtlinie entsprechen und müssen regelmäßig geändert werden.

Zur Übertragung von Passwort und Nutzerdaten werden ausschließlich verschlüsselte https-Verbindungen eingesetzt. Der Zugriff auf die Server erfolgt ausschließlich über eine verschlüsselte SSH-Verbindung.

**c) Zugriffskontrolle**

Alle Dienste der Happy Contests UG sind mittels Benutzername / Passwort gesichert. Der Zugriff auf personenbezogene Daten sowie das Verändern von Daten ist ausschließlich dem Auftraggeber und den Administratoren der Happy Contests UG möglich.

Sollte ein automatischer Export personenbezogener Daten an ein System des Auftraggebers vereinbart sein, wird dies über eine Schnittstelle gelöst. Die Aktivierung der Export-Funktion und Konfiguration der Zielsysteme für den Export werden hierbei ausschließlich und nur bei ausdrücklichem Wunsch des Auftraggebers durch Administratoren der Happy Contests UG durchgeführt.

Der Zugriff auf die Server ist ausschließlich Mitarbeitern der Happy Contests UG vorbehalten. Der Zugriff ist mittels Benutzername und Passwort gesichert, wobei jeder Mitarbeiter seine eigenen Zugangsdaten bekommt. Diese geben dem Mitarbeiter ausschließlich die Zugriffsrechte, welche er für seine Aufgabengebiete benötigt.

**d) Trennungskontrolle**

Das System der Happy Contests UG ist mandantenfähig und stellt sicher, dass Daten verschiedener Auftraggeber getrennt sind.

Das Produktivsystem wird physikalisch und logisch getrennt von Testsystemen betrieben.

**e) Pseudonymisierung (Art. 32 Abs. 1 lit. a EU-DSGVO; Art. 25 Abs. 1 EU-DSGVO)**

Eine Pseudonymisierung erfolgt nicht. Der Auftraggeber benötigt die personenbezogenen Daten in nicht-pseudonymisierter Form.

**2. Integrität (Art. 32 Abs. 1 lit. b EU-DSGVO)**

**a) Weitergabekontrolle**

Der Zugriff auf personenbezogene Daten ist ausschließlich dem Auftraggeber sowie Administratoren der Happy Contests UG möglich. Zur Authentifizierung wird der OAuth2 Standard verwendet. Die Übermittlung der Zugangsdaten sowie der personenbezogenen Daten erfolgt hierbei ausschließlich über SSL-verschlüsselte Verbindungen.

**b) Eingabekontrolle**

Sämtliche Aktivitäten werden auf den Servern mittels Logfiles protokolliert. Dabei werden IP-Adresse, Zeitpunkt, Art sowie Inhalte der Aktivitäten festgehalten.

**3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)**

Zur Datensicherung werden täglich automatische Backups der Datenbank erzeugt. Die Backups werden dabei auf einem separaten Server abgelegt und gesichert. Des Weiteren werden Datenbanklogs der letzten 30 Tage gesichert.

Somit ist eine Wiederherstellung bei Verlust oder zufälliger sowie mutwilliger Zerstörung stets möglich.

Zur Sicherheit vor physischen Defekten der Festplatten werden diese im RAID betrieben, wobei die Daten auf mehrere Festplatten gespiegelt abgelegt werden.

Zur Sicherung des Quellcodes wird ein verteiltes Versionsverwaltungswerkzeug eingesetzt und die Quellen auf mehreren Servern gesichert. Dadurch ist die Wiederherstellung jedes Codestandes stets möglich.

**4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d EU-DSGVO; Art. 25 Abs. 1 EU-DSGVO)**

**a) Datenschutz-Management:**

Jede Neuentwicklung durchläuft einen standardisierten Qualitäts- und Abnahmeprozess, wobei insbesondere hohen Wert auf datenschutzrechtliche Aspekte gelegt werden. Jede Abnahme erfolgt hierbei im 4-Augenprinzip. Des Weiteren werden Neuentwicklungen stets

zuerst auf einem separaten Testsystem geprüft, bevor diese in das Produktivsystem überführt werden.

**b) Incident-Response-Management:**

Datenschutzrechtliche Vorfälle werden stets mit höchster Priorität behandelt, um die schnellstmögliche Wiederherstellung der Serviceleistung zu gewähren.

**c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO):**

Das System erfasst, ausgenommen der IP-Adresse der User, ausschließlich Daten welche vom Auftraggeber explizit angefordert werden. Den konkreten Umfang verwaltet der Auftraggeber durch Einstellungen im Administrationsbackend.

**d) Auftragskontrolle**

Es erfolgt keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers in Form einer Auftragsbestätigung.

Fabio Marcantonio – Datenschutzbeauftragter Happy Contests

# Anlage 2: Technisch organisatorische Maßnahmen

## Hetzner GmbH

# Technisch-organisatorische Maßnahmen nach Art. 32 DSGVO

**Hinweis:** Happy Contests nutzt „Dedicated Server“

**I. Vertraulichkeit**

**Zutrittskontrolle**

Datacenter-Parks in Nürnberg und Falkenstein

- elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um den gesamten Datacenter-Park
- 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, Sicherheitsschleusen und Serverräumen
- Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters

Verwaltung

- elektronisches Zutrittskontrollsystem mit Protokollierung
- Videoüberwachung an den Ein- und Ausgängen

**Zugangskontrolle**

bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"

- Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
- Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem Auftraggeber dort eine Zwei-Faktor- Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.

bei Hauptauftrag "Managed Server", "Webhosting", "Storage Box"

- Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter vom Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert

**Zugriffskontrolle**

bei internen Verwaltungssystemen des Auftragnehmers

- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
- Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers

bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"

- Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.

bei Hauptauftrag "Managed Server", "Webhosting", "Storage Box"

- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
- Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
- Für übertragene Daten/Software ist einzig der Auftraggeber in Bezug auf Sicherheit und Updates zuständig.

**Datenträgerkontrolle**

Datacenter-Parks in Nürnberg und Falkenstein

- Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
- Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum (Falkenstein) zerstört (geschreddert).

**Trennungskontrolle**

bei internen Verwaltungssystemen des Auftragnehmers

- Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
- Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"

- Die Trennungskontrolle obliegt dem Auftraggeber.

bei Hauptauftrag "Managed Server", "Webhosting", "Storage Box"

- Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
- Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

**Pseudonymisierung**

Für die Pseudonymisierung ist der Auftraggeber verantwortlich

**II. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**

**Weitergabekontrolle**

- Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.

- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
- Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.

**Eingabekontrolle**

bei internen Verwaltungssystemen des Auftragnehmers

- Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
- Änderungen der Daten werden protokolliert.

bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"

- Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.

bei Hauptauftrag "Managed Server", "Webhosting", "Storage Box"

- Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
- Änderungen der Daten werden protokolliert.

**III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)**

**Verfügbarkeitskontrolle**

bei internen Verwaltungssystemen des Auftragnehmers

- Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
- Einsatz von Festplattenspiegelung bei allen relevanten Servern.
- Monitoring aller relevanten Server.
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Dauerhaft aktiver DDoS-Schutz.

bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"

- Datensicherung obliegt dem Auftraggeber.

- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Dauerhaft aktiver DDoS-Schutz.

bei Hauptauftrag "Managed Server", "Webhosting", "Storage Box"

- Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
- Einsatz von Festplattenspiegelung.
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Einsatz von Softwarefirewall und Portreglementierungen.
- Dauerhaft aktiver DDoS-Schutz.

**Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);**

- Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

**IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)**

- Das Datenschutz-Managementsystem und das Informationssicherheits-managementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.
- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).

Auftragskontrolle

- Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.

- Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
- Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.

# Anlage 3: Technisch organisatorische Maßnahmen

## dogado GmbH

## Technisch-organisatorische Maßnahmen nach Art. 32 DSGVO

**Präambel**

Die dogado GmbH vermietet die Datenverarbeitungsanlage an den Auftraggeber. Dies beinhaltet dieVermietung von Hard- und Software, sowie die Bereitstellung von Anbindungen an das Internet sowie weitere Dienste entsprechend der jeweiligen Vereinbarung. Der Auftraggeber entscheidet allein und ausschließlich darüber, welche personenbezogene Daten in welcher Weise verarbeitet werden. Die hierfür erforderlichen Programme zur Datenverarbeitung werden durch den Auftraggeber erstellt und eingesetzt. Die dogado GmbH sorgt für die technische Einsatzbereitschaft des Systems entsprechend den vertraglichen Vereinbarungen und führt Buch darüber, welche Anlagen durch den Auftraggeber in welchem Umfang genutzt werden. Die Datenverarbeitung erfolgt durch den Auftraggeber. Die dogado GmbH hat keinerlei Einfluss auf die durch den Auftraggeber durchgeführten Datenverarbeitungsvorgänge.

**Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)**

**Zutrittskontrolle**

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen in den Rechenzentren

1. Zutrittskontrollsystem

Ein Schließsystem in Form einer mindestens 1-Faktor-Authentifizierung (z.B. Transponder, Chipkarte, Klingelsystem mit Personenkontrolle per Bild und Ton) ermöglicht den Zutritt zu Datenverarbeitungsanlagen erst nach positiver Zutrittsprüfung.

2. Schlüsselregelung

Schlüsselausgaben an Personen zum Zutritt zu Datenverarbeitungsanlagen werden dokumentiert.

3. Protokollierung der Besucher

Besucher, die Zutritt zu Datenverarbeitungsanlagen erhalten (z.B. im Falle von Hardware-Austausch durch den Hersteller) werden in einem Besucherbuch erfasst.

4. Einbruchmeldeanlage

Der Zutritt zu Datenverarbeitungsanlagen ist per Einbruchmeldeanlage abgesichert.

5. Videoüberwachung

Datenverarbeitungsanlagen werden per Videoüberwachung gesichert.

**Zugangskontrolle**

Keine unbefugte Systembenutzung

1. Passwortvergabe

Ein Zugang zu den Datenverarbeitungssystemen ist grundsätzlich nur mittels einer Kombination aus einem Benutzernamen und dem zugeordneten Passwort möglich.

2. Passwortrichtlinie

Passwörter für Datenverarbeitungsanlagen müssen Mindest-Komplexitätsanforderungen der unternehmensweiten Richtlinie entsprechen; Passwörter von Mitarbeitern müssen regelmäßig geändert werden.

3. Administrativer Zugriff

Sämtliche Datenverarbeitungssysteme sind zu Wartungszwecken ausschließlich über freigegebene IP-Adressbereiche und verschlüsselt erreichbar (z.B. VPN-Beschränkungen).

4. Firewall

Schutz der Infrastruktur durch Firewalls (Soft- und/oder Hardware), Beschränkungen ungenutzter Ports sowie Benutzername und Passwort vor unberechtigten Zugriffen geschützt. Systeme, die Hauptvertragsleistungen bereitstellen, werden, entsprechend der jeweiligen Vereinbarung im Hauptvertrag, mit einer Firewall ausgestattet.

5. Einsatz von Anti-Viren-Software

Systeme, die zum Zugriff auf Datenverarbeitungssysteme genutzt werden, sind mit einer Anti-Viren-Software ausgestattet. Diese Software wird regelmäßig auf die neuesten Virus-Definitionen aktualisiert. Systeme, die Kundenleistungen bereitstellen, werden, entsprechend der jeweiligen Vereinbarung im Hauptvertrag, mit einer Anti-Viren-Software ausgestattet.

6. Verschlüsselung von mobilen Datenträgern
Sofern mobile Datenträger oder mobile Geräte zum Einsatz kommen, werden die Inhalte verschlüsselt.

**Zugriffskontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

1. Zuordnung von Benutzerrechten
Der Zugriff auf Datenverarbeitungssysteme wird für Personen auf die jeweils mindestensnotwendigen Daten durch Vergabe entsprechender Benutzerrechte eingeschränkt. Die Datenverarbeitung selbst erfolgt durch den Kunden Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

2. Sichere Aufbewahrung von Datenträgern
Datenträger, die personenbezogene Daten enthalten, werden verschlossen gelagert

3. Verwaltung der Rechte durch einen eingeschränkten Personenkreis
Ausschließlich berechtigte Systemadministratoren sind in der Lage, Rechte anderer Personen zu Datenverarbeitungssystem zu verwalten. Der Kreis der berechtigten Systemadministratoren wird auf die kleinstmögliche Auswahl von Personen reduziert. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

4. Protokollierung der Zugriffe
Zugriffe auf Dienste (z. B. Webdienste) werden DSGVO-konform in Log-Files protokolliert. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat jedoch keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

5. Ordnungsgemäße Vernichtung von Datenträgern
Datenträger, die personenbezogene Daten enthalten werden gemäß DIN 66399 vernichtet.

6. Regelmäßige Wartung der Datenverarbeitungssysteme

**Trennungskontrolle**
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

1. Festlegung von Datenbankrechten
Der Zugriff von Systemen und Benutzern auf Datenbanken wird auf die jeweils notwendigen Daten eingeschränkt.

2. Trennung von Produktiv- und Testsystemen
Produktiv- und Testumgebungen werden isoliert voneinander betrieben. Ein Zugriff einer Umgebung auf Daten der jeweils anderen Umgebung wird durch den Einsatz von z.B. getrennten Datenbanksystemen und Serversystemen unterbunden.

3. Logische Mandantentrennung
Durch den Einsatz unterschiedlicher softwareseitiger Mechanismen wird eine Trennung der Daten von Mandanten gewährleistet.

**Integrität (Art. 32 Abs. 1 lit. b DSGVO)**

**Weitergabekontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

1. Transport
Sofern personenbezogene Daten weitergegeben werden, findet dies grundsätzlich verschlüsselt statt. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

**Eingabekontrolle**
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

1. Zuordnung von Benutzerrechten
Der Zugriff auf Datenverarbeitungssysteme wird für Personen auf die jeweils mindestens notwendigen Daten durch Vergabe entsprechender Benutzerrechte eingeschränkt.

2. Protokollierung von Dateneingaben
Die Datenverarbeitung erfolgt durch den Kunden, Seitens des Auftragnehmers besteht kein Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme. Die Eingabekontrolle der Daten kann daher ausschließlich durch den Kunden umgesetzt werden.

3. Nachvollziehbarkeit der Eingabe

Die Datenverarbeitung erfolgt durch den Kunden. Seitens des Auftragnehmers besteht kein Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme. Die Eingabekontrolle kann daher ausschließlich durch den Kunden umgesetzt werden. Bei Änderungen durch den Auftragnehmer werden die Administrationszugriffe adäquat protokolliert.

**Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**

**Verfügbarkeitskontrolle**

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust

1. Unterbrechungsfreie Stromversorgung in Serverräumen (Rechenzentren) Serverräume sind durch unterbrechungsfreie Stromversorgungen geschützt. Der Schutz ist zweistufig aufgebaut. Bei Bedarf wird ein Notstrom-Aggregat automatisch aktiviert, das die Stromversorgung der Serverräume übernimmt.

2. Klimaanlagen in Serverräumen (Rechenzentren)

Eine für den Betrieb von Serversystemen angemessene Temperatur und Luftfeuchtigkeit wird in Serverräumen durch ausreichend dimensionierte Klimaanlagen gewährleistet.

3. Feuer- und Rauchmeldeanlagen in Serverräumen (Rechenzentren)

Durch den Einsatz von Feuer- und Rauchmeldeanlagen wird ein Brand frühzeitig erkannt. Feuerlöschanlagen löschen auftretende Brände.

4. Datensicherungskonzept und Aufbewahrung von Datensicherungen

Datensicherungen von personenbezogenen Daten werden nur nach Vereinbarung bzw. gemäß des abgeschlossenen Hauptvertrages angefertigt und auf separaten und für Datensicherungen dediziert eingesetzten Systemen aufbewahrt.

5. Monitoring

Systemkritische Instanzen werden durch Monitoring überwacht. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)**

**Datenschutz-Management**

Der Auftragnehmer etabliert ein Datenschutzmanagement, das den Schutz der personenbezogenen Daten sicherstellt.

**Incident-Response-Management**

Regelmäßige Überprüfung der IT-Infrastruktur. Der Auftragnehmer etabliert einen Vorfallreaktionsplan.

**Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)**

Der Auftragnehmer stellt innerhalb seiner Möglichkeiten sicher, dass durch Voreinstellung nur Daten, die für den jeweiligen bestimmten Verarbeitungszweck unbedingt erforderlich sind, verarbeitet werden. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

**Auftragskontrolle**

Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers

1. Auswahl von geeigneten Auftragnehmern

Bei der Auswahl von Auftragnehmern, die personenbezogene Daten im Auftrag verarbeiten, werden nur solche Auftragnehmer ausgewählt, die mindestens die gesetzlich vorgeschriebenen Anforderungen an die Verarbeitung von personenbezogenen Daten einhalten.

2. Überwachung der Auftragnehmer

Der Auftragnehmer wird regelmäßig auf die Einhaltung der zugesicherten technischen und organisatorischen Maßnahmen bei der Verarbeitung von personenbezogenen Daten überprüft.