Anlage 1
Auftragsverarbeitungsvertrag

zwischen

Name und Anschrift

vertreten durch

Name der vertretenden Person

im Folgenden: **Auftraggeber**

und

LuckyShot GmbH

Schönhauser Allee 163

10435 Berlin

vertreten durch

Alexander Adam

im Folgenden: **Auftragnehmer**

1. Einleitung, Geltungsbereich, Definitionen

Dieser Auftragsverarbeitungsvertrag (folgend „Vertrag“) regelt die Rechte und Pflichten von Auftraggeber und -nehmer (folgend „Parteien“) im Rahmen einer Verarbeitung von personenbezogenen Daten.

Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2. Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Auftragnehmer übernimmt folgende Verarbeitungen:

- Automatisierte Verarbeitung von Daten durch DV-Programm in der Vereinssoftware des Auftragnehmers.
- Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Dienstleistungsvertrag auf Grundlage des Kundenkontos bei campai, chapster oder Vereinsfuchs sowie den AGB und der angebotenen Leistungen in der aktuellen Version (im Folgenden „Hauptvertrag“).
- Erstellung von Redundanzen

2.2 Dauer

Die Verarbeitung beginnt mit dem Start des Hauptvertrags und erfolgt auf unbestimmte Zeit und endet, wenn der zwischen den Parteien geschlossene Hauptvertrag endet.

3. Art und Zweck der Datenverarbeitung:

3.1 Art und Zweck der Verarbeitung

Die Verarbeitung besteht in der Bereitstellung einer online Cloud-Lösung zur Verwaltung der Mitglieder und der zwischen ihnen stattfindenden Kommunikation im Verein des Auftraggebers. Dies beinhaltet auch eine Funktion zum Versand von E-Mails an die Mitglieder und Kontakte des Auftraggebers. Die Verarbeitung dient folgendem Zweck: Das DV-Programm/Verfahren des Hauptvertrages dient der Mitglieder- und Beitragsverwaltung von Vereinen.

3.2 Art der Daten

Es werden folgende Daten verarbeitet: Titel, Vorname, Nachname, Geschlecht, Geburtsdatum, Familienstand, Position (geschäftlich), Beruf, Postadresse, Telefonnummer, E-Mail-Adresse, Mitgliedsnummer, Kontoverbindung, Eintritt/Austritt Verein, Abteilung Verein, Position im Verein (ggf. von/bis), Vereinsehrungen (ggf. mit Datum), Vereinsfunktion (ggf. mit Datum), Notizen zum Mitglied, durch die vom Auftraggeber erstellte Daten.

3.3 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Mitglieder
- ggf. ehemalige Mitglieder
- Kontakte und
- Benutzer des Auftraggebers

4. Pflichten des Auftragnehmers

4.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

4.2 Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

4.3 Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

4.4 Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

4.5 Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

4.6 Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

4.7 Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

4.8 Der Auftragnehmer sichert zu, einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten bestellt zu haben, dem die erforderliche Zeit zur Erledigung seiner Aufgaben gewährt wird.

Datenschutzbeauftragter bei dem Auftragnehmer ist:

Malte Pignol
0176 2193 4003
datenschutz(at)luckyshot.io

Malte Pignol ist Wirtschaftsjurist mit Spezialisierung im europäischen Wirtschaftsrecht sowie dem Datenschutz. Als erfahrener interner und externer Datenschutzbeauftragter von kleinen und mittelständischen Unternehmen und Konzernen verfügt er über Personenzertifizierungen als Datenschutzbeauftragter, Datenschutzauditor, Informationssicherheitsbeauftragter und Information Security Lead Auditor.

5. Technische und organisatorische Maßnahmen

5.1 Die in **Anhang 1** beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen.

5.2 Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

5.3 Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

5.4 Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

5.5 Die Verarbeitung von Daten in Privatwohnungen ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit eine solche Verarbeitung erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.

5.6 Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

6. Regelungen zur Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten

6.1 Im Rahmen des Hauptvertrags verarbeitete Daten wird der Auftragnehmer nur entsprechend des vorliegenden Vertrags berichtigen, löschen oder in der Verarbeitung einschränken.

6.2 Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

6.3 Der Auftragnehmer ist berechtigt Datenverarbeitungen auszusetzen bzw. ergänzende Weisungen nicht umzusetzen, sollten durch objektive Anhaltspunkte ein gerechtfertigter Zweifel an der Rechtmäßigkeit oder Zulässigkeit der Verarbeitung bestehen. Hierzu zählen insbesondere Verstöße gegen datenschutzrechtliche Bestimmungen oder Bestimmungen des Hauptvertrags. In einem solchen Fall setzt der Auftragnehmer den Auftraggeber unverzüglich hierüber in Kenntnis.

7. Unterauftragsverhältnisse

7.1 Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer für den Rechenzentrumsbetrieb, die in **Anhang 2** genannten, Unterauftragnehmer einsetzt.

7.2 Der Auftragnehmer darf ohne Zustimmung des Auftraggebers auch weitere oder andere Unterauftragnehmer für die Verarbeitung der vertragsgegenständlichen Daten einsetzen, wenn die vertragsgegenständlichen Daten lediglich innerhalb der Bundesrepublik Deutschland oder der EU/EWR verarbeitet werden. Hierüber ist der Auftraggeber mit Namensnennung des Unterauftragnehmers schriftlich zu informieren.

7.3 Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

7.4 Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

7.5 Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.

7.6 Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der Bedingungen des Vertrags möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.

7.7 Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8. Rechte und Pflichten des Auftraggebers

8.1 Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

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

8.3 Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

8.4 Der Auftraggeber wird keine eigenhändigen Kontrollen durchführen, soweit der Auftragnehmer den angeforderten Nachweis durch Vorlage eines marktüblichen Zertifikats (etwa nach IS, DIN oder SOC-Standard) oder anderweitig führen kann. Kontrollen beim Auftragnehmer haben im Übrigen ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers statt.

9. Mitteilungspflichten

9.1 Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat ohne schuldhaftes Zögern ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen, in jedem Fall aber die gesetzlichen Fristen zu wahren. Sie muss mindestens folgende Angaben enthalten:

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

9.1.2 den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

9.1.3 eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes

personenbezogener Daten;

9.1.4 eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

9.2 Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

9.3 Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

9.4 Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10. Beendigung des Auftrags

10.1 Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

10.2 Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

10.3 Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben. Die Löschung erfolgt auf Verlangen des Auftraggebers unverzüglich, was eine Frist von bis zu vier Wochen beanspruchen kann, sofern nicht nach den jeweiligen Umständen eine frühere Löschung geboten ist. Sofern ausnahmsweise eine Löschung früher erfolgen soll, wird der Auftraggeber dies dem Auftragnehmer mit ausreichendem Vorlauf mitteilen.

11. Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

12. Sonstiges

12.1 Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur dokumentierten Freigabe (Schrift- oder Textform) durch die andere Partei als vertraulich zu behandeln.

12.2 Sofern der Zugriff auf die Daten, die der Auftraggeber dem Auftragnehmer zur Datenverarbeitung übermittelt hat, durch Maßnahmen Dritter (bspw. Maßnahmen eines Insolvenzverwalters oder Beschlagnahme durch Finanzbehörden) gefährdet wird, hat der Auftragnehmer den Auftraggeber hierüber unverzüglich zu benachrichtigen.

12.3 Im Falle von Widersprüchen zwischen den Bestimmungen des vorliegenden Vertrags und den Regelungen der Hauptvertrags gehen die Bestimmungen des vorliegenden Vertrags vor.

12.4 Nebenabreden bedürfen der mindestens der Textform.

12.5 Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

12.6 Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies nicht die Wirksamkeit der übrigen Vertragsklauseln.

12.7 Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland. Der Gerichtsstand ist der Sitz des Auftragnehmers.

Ort, Datum _____ Ort, Datum _____

_____ _____

Unterschrift Auftraggeber Unterschrift Auftragnehmer

Anlange 2:
Technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

1. Allgemeine Maßnahmen

a) Verschwiegenheitsverpflichtung für Mitarbeiter:

   Diese ist Bestandteil aller Arbeitsverträge bei campai, chapster sowie Vereinsfuchs und untersagt u.a. auch die Weitergabe persönlicher oder geschäftlicher Daten Dritter, insbesondere von Kunden des Arbeitgebers an unbefugte Dritte. Zuwiderhandlung wird mit einer Vertragsstrafe geahndet.

b) Regelmäßige Datenschutzschulungen für Mitarbeiter

c) Besonders qualifizierter Datenschutzbeauftragter: siehe 4.8

d) Orientierung an den Standards der ISO 27001

e) Auftragsverarbeitungsverträge mit Unterauftragsverarbeitern

2. Vertraulichkeit

a) Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet werden.

Da campai, chapster sowie Vereinsfuchs keine eigenen Server unterhält, verweisen wir bezüglich der Serversicherheit auf die umfassenden Maßnahmen, welche für die von uns genutzten Rechenzentren vom Betreiber Amazon Web Services („AWS") auf der Perimeter-, Infrastruktur-, Daten- sowie Umweltebene ergriffen werden. Eine detaillierte Beschreibung der von AWS ergriffenen Schutzmaßnahmen für die betriebenen Serverstandorte ist im Webauftritt des Unternehmens zu finden: https://aws.amazon.com/de/compliance/data-center/data-centers/

b) Zugangs- und Benutzerkontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Authentifikation mit Benutzername/Passwort
- Passwortvergabe:
  - min. Länge des Passworts: 12 Zeichen
  - max. Anzahl der Fehleingaben: 3
- Einsatz VPN bei Remote-Zugriffen
- Zentrales Mobile Device Management

- Richtlinien zur Clean-Desk-Policy, Passwortvergabe und zur manuellen Computersperrung

c) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass Personen nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Dokumentiertes Berechtigungskonzept vorhanden
- Zuordnung von Benutzerrechten/Erstellen von Benutzerprofilen
- Verwaltung der Rechte durch System-Administrator
- Anzahl der Administratoren auf das "Notwendigste" reduziert
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten und Datenträgern
- Verschlüsselung von Datenträgern
- Sichere Aufbewahrung von Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern
- Löschungskonzept für Daten

d) Transport- und Übertragungskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektroni*schen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.*

- Firewall: Die nach dem Stand der Technik erforderlichen Firewall-Technologien sind implementiert und werden auf dem aktuellen Stand gehalten
- Die Datenverarbeitung erfolgt in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung

3. Integrität

a) Eingabekontrolle/Verarbeitungskontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden

b) Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

- Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration

c) Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Transportverschlüsselung beim E-Mail-Versand
- Einsatz von VPN
- Websites sind https verschlüsselt

4. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und im Störfall wiederhergestellt werden können.

Innerhalb der genutzten Rechenzentren von AWS sind eine Vielzahl von Maßnahmen zum Schutz vor Störungen und Katastrophen implementiert. Diese umfassen u.a.:

- Unterbrechungsfreie Stromversorgung (USV)
- Überspannungsschutz
- Schutz gegen Umwelteinflüsse (Sturm, Wasser)
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Testen von Datenwiederherstellung
- Klimaanlage in Serverräumen
- regelmäßige Backups
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Virenschutzsystem
- Spiegelung von Festplatten (z. B. RAID-Verfahren)
- Konzept für Katastrophenfall vorhanden

5. Trennungsgebot

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

- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem
- Festlegung Technologie von Datenbankrechten
- Steuerung über dokumentiertes Berechtigungskonzept
- Trennung von Daten verschiedener Auftraggeber

6. Überprüfung, Bewertung und Evaluierung

Maßnahmen, die gewährleisten, dass regelmäßig bzw. anlassbezogen überprüft wird, ob die datenschutzrechtlichen Anforderungen erfüllt werden.

- Durchführung von Audits
- Anfertigung von Datenschutz-Folgenabschätzungen

- Ggf. Hinzuziehung weiterer Prüfer

Anlage 3
Eingesetzte Unterauftragsverarbeiter

Datenbank Hosting

AWS/ AWS3/ AWS SES
Wir verwenden den Dienst von Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, 1855 Luxemburg für unseren App-Server (auf denen die Backends laufen) sowie AWS S3 für das Hosting der hochgeladenen Dateien in unseren Apps und AWS SES für Versand von Einladungs-E-Mails innerhalb unserer Apps für unsere Nutzer.

Die Standorte der genutzten Server-/Rechenzentren befinden sich innerhalb der von AWS betriebenen "Region Frankfurt" (siehe auch https://aws.amazon.com/de/region-frankfurt/).

AWS erfüllt hohe, internationale Sicherheitsstandards und ist nach den folgend genannten Normen zertifiziert: ISO/IEC 27001:2013, 27017:2015, 27018:2014 sowie 9001:2015. Einzelheiten zu den genannten Normen sowie die Zertifizierungen sind einsehbar unter https://aws.amazon.com/de/compliance/iso-certified/

AWS "Anhang zur Datenverarbeitung" ist hier einzusehen:
https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

App Hosting
Unsere App wird von **Firebase** gehostet, eine Tochtergesellschaft der Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043.

Eine Zusammenführung dieser Daten mit anderen Datenquellen wird nicht vorgenommen.
Die Erfassung dieser Daten erfolgt auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO.

Weitere Hinweise zur Datenverarbeitung durch Firebase können unter
https://policies.google.com/privacy eingesehen werden.

Verbesserung, Wartung, Kundenservice & Gewährleistung von Dienstfunktionalitäten

Google
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, Muttergesellschaft: Google LLC, 1600 Amphitheatre Parkway, Mountain View, California 94043 USA ("Google").

Wir haben ein sog. „Data-Processing-Agreement" mit Google, Betreiber der Google Cloud Platform abgeschlossen, in dem wir Google verpflichten, die Daten unserer Kunden zu schützen, sie nicht an Dritte weiterzugeben und bei einem Transfer von personenbezogenen Daten in die USA die Regelungen der Standardvertragsklauseln gem. Art. 46 DS-GVO einzuhalten.

Weitere Informationen und die geltenden Datenschutzbestimmungen von Google können unter https://policies.google.com/privacy?hl=de&gl=de eingesehen werden.

Intercom
Wir setzen für den Kundenservice und zur Kommunikation Intercom, 3rd Floor, Stephens Ct., 18-21 St. Stephen's Green, Dublin 2 ein.

Weitere Informationen und die geltenden Datenschutzbestimmungen von Intercom können unter https://www.intercom.com/legal/privacy eingesehen werden.

Sentry
Wir verwenden den Dienst Sentry der Functional Software Inc., 132 Hawthorne Street, San Francisco, California 94107 für unsere App, um die Systemstabilität zu überwachen und Codefehler erkennen und erheben zu können. Sentry dient allein diesen Zielen und wertet keine Daten zu Werbezwecken aus. Die Daten der Nutzer, wie z.B. Angaben zum Gerät oder Fehler Zeitpunkt werden ausschließlich pseudonymisiert erhoben und lassen für uns keinen Rückschluss auf einzelne Nutzer zu. Sentry verarbeitet nur Daten zu dem jeweiligen Fehler Vorfall und verarbeitet in unserem Auftrag keinerlei allgemeine Nutzungsdaten.

Weitere Informationen und die geltenden Datenschutzbestimmungen von Sentry können unter https://sentry.io/privacy/ eingesehen werden.

Prismic
Wir verwenden den Dienst von Prismic, Data Privacy Office, New Prismic, 9 rue de la Pierre Levée, 75011, PARIS, France um Inhalte und die Bereitstellung von Content für unsere App zu gewährleisten.

Die Verwendung von Prismic dient ausschließlich dem Zweck Inhalte und einen unterbrechungsfreien Betrieb unserer App gewährleisten zu können.

Weitere Informationen und die geltenden Datenschutzbestimmungen von Prismic können unter https://prismic.io/legal/privacy eingesehen werden.

FinApi
Wir verwenden die Dienste von FinAPI GmbH, Adams-Lehmann-Str. 44, 80797 München um eine API-Schnittstelle für Bankvorgänge in unseren Plattformen zur Verfügung zu stellen damit unseren Nutzern eine Transaktionen ihrer Geschäftsvorfälle ermöglicht wird.

Die Verwendung von FinApi dient ausschließlich dem Zweck eine Bankschnittstelle in unseren Plattformen für einen Banktransfer anbieten zu können.

Weitere Informationen und die geltenden Datenschutzbestimmungen von FinApi können unter https://www.finapi.io/datenschutz/ eingesehen werden.