

Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU-Datenschutz-Grundverordnung (AVV) gem. Art. 28 Abs. 3 EU- DSGVO

zwischen

[Träger]

Auftraggeber

und

IESP – Institut für Elementar- und Schulpädagogik
Rosengartenstrasse 1a
CH-8037 Zürich

Auftragnehmer

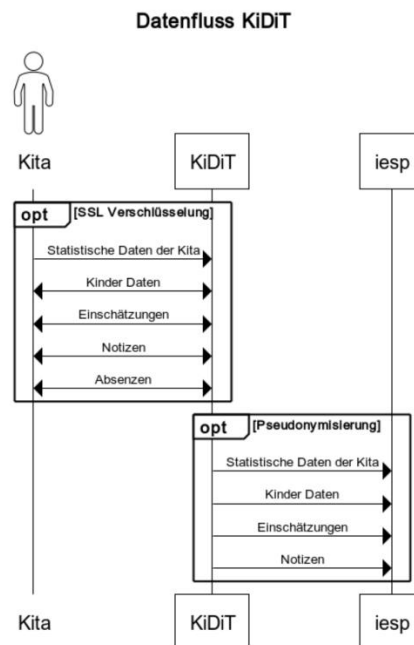
zur Nutzung des Beobachtungsinstruments KiDiT[®] (KinderDiagnoseTool) durch Einrichtungen bzw. pädagogisches Personal des Trägers.

1. Einleitung, Geltungsbereich, Definitionen

1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer im Rahmen einer beauftragten Verarbeitung von personenbezogenen Daten.
2. Dieser Vertrag findet auch auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer personenbezogene Daten des Auftraggebers bzw. bei ihm beschäftigter Mitarbeiter*innen verarbeiten.
3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU-Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden **zumindest in Textform** zu erfolgen haben, ist die Textform nach § 126b BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2. Gegenstand und Dauer der Verarbeitung, Art und Zweck der Datenverarbeitung

1. Die Verarbeitung von personenbezogenen Daten beruht auf dem zwischen den Parteien bestehenden Lizenzvertrag (ggf. auch mehreren) zur Nutzung des KiDiT-Systems (im Folgenden Hauptvertrag).
2. Der vorliegende Vertrag ist an den Hauptvertrag gekoppelt, beginnt und endet mit diesem bzw. bei mehreren Hauptverträgen, sobald der letzte endet.
3. Die folgenden Verarbeitungsvorgänge werden genutzt: Erfassen, Ordnen, Speichern, Verknüpfen.
4. Die Verarbeitung dient folgendem Zweck: Nutzbarkeit spezifischer Funktionen des KiDiT-Systems, insbesondere der Auswertungsfunktion.



3. In KiDiT erfasste Daten und betroffene Personengruppen

Betroffene Personengruppen sind beim Auftraggeber betreute Kinder und dort tätige Mitarbeitende.

Von Kindern werden folgende Arten von Daten verarbeitet:

- Nickname
- Geschlecht (m/w/k.a.)
- Etwaiges Geburtsdatum

Von Mitarbeitenden werden folgende Arten von Daten verarbeitet:

- E-Mail-Adresse
- Kontakt und Kontaktadresse für die Rechnungslegung
- Kundennummer

4. Pflichten des Auftragnehmers

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, sofern die Mitteilung ihm nicht gesetzlich verboten ist. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen Zwecke.
2. Der Auftraggeber hat die Möglichkeit, die personenbezogenen Daten „auf Knopfdruck“ zu anonymisieren und dem Auftragnehmer zu übermitteln. Erst nach durch den Auftraggeber ausgelöster Anonymisierung und damit sicheren Entfernung des Personenbezugs darf der Auftragnehmer diese nicht mehr personenbezogenen Daten für wissenschaftliche und insbesondere statistische Zwecke verarbeiten und diese Auswertung auch den Nutzern/Auftraggebern als Vergleichsmaßstab zur Verfügung stellen.
3. Der Auftragnehmer bestätigt, dass ihm die einschlägigen allgemeinen datenschutzrechtlichen Vorschriften bekannt sind und er die Grundsätze einer ordnungsgemäßen Datenverarbeitung beachtet.
4. Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, sind schriftlich zur Vertraulichkeit verpflichtet, soweit sie nicht bereits einer gesetzlichen Geheimhaltungspflicht unterliegen. Die eingesetzten Personen werden vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht. Diesbezügliche Schulungs- und Sensibilisierungsmaßnahmen sind regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass die Personen laufend angemessen angeleitet und überwacht werden.
5. Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung einer gegebenenfalls erforderlichen Datenschutzfolgeabschätzung durch Hergabe der relevanten und von ihm vorgehaltenen Informationen zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.
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.
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.
8. Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

9. Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung von personenbezogenen Daten in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

5. Technische und organisatorische Maßnahmen

1. Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.
2. 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. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.
3. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, informiert der Auftragnehmer den Auftraggeber unverzüglich.
4. Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
5. Kopien oder Duplikate werden nicht ohne Wissen des Auftraggebers erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, etwa für Sicherungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
6. Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Auftraggeber jederzeit, aber nicht häufiger als alle 12 Monate, auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

6. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

1. Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
2. Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7. Unterauftragsverhältnisse

Der Auftraggeber stimmt der Beauftragung von Subunternehmern zu, soweit dies zur Erfüllung des Hauptvertrags notwendig ist. Derzeit ist der Provider [Kilian Hann, Future Connection GmbH, muenchen@fconnection.com] als Subunternehmer beauftragt, das KiDiT-System auf einem Webserver zu hosten.

3. Die Zustimmung ist nur wirksam, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.
4. 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.
5. Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.
6. Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus. Über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter wird der Auftraggeber vom Auftragnehmer informiert, um gegebenenfalls gegen derartige Änderungen Einspruch zu erheben.
7. 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.
8. Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich auf dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Kapitel 4.9. dieses Vertrages genannten Bedingungen 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.
9. Der Auftragnehmer hat die Einhaltung der Pflichten durch den Subunternehmer regelmäßig angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber auf Anforderung vorzulegen.
10. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.
11. 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

1. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
2. Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert zumindest in Textform. In Eilfällen können Weisungen mündlich erteilt werden, müssen aber unverzüglich nachweisbar bestätigt werden.
3. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
4. 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.
5. Kontrollen beim Auftragnehmer haben 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, aber nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5.6. dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9. Mitteilungspflichten

1. Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
 - a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie personenbezogenen Datensätze;
 - b. den Namen und die Kontaktdaten der Anlaufstelle für weitere Informationen;
 - c. Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - d. 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
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.

3. Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
4. Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10. Weisungen

Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor. Weisungsberechtigte Personen des Auftraggebers sind:

Vorname, Name:

Organisationseinheit:

Telefon:

E-Mail:

Weisungsempfänger beim Auftragnehmer sind:

Catherine Walter-Laager

IESP, Geschäftsführung

mail@kidit.ch

Kilian Hann

Future Connection GmbH

muenchen@fconnection.com

Für Weisung zu nutzende Kommunikationskanäle:

per E-Mail an mail@kidit.ch

Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

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 solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber dennoch bestätigt oder geändert wird.

11. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 S. 2 lit. g DSGVO

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 in Form eines Datenexports 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. Sofern Daten physisch vorhanden sind, erfolgt die Vernichtung gemäß DIN 66399. Hierbei gilt mindestens Schutzklasse 1.
2. Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.
3. Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.
4. 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.

12. Vergütung

Die Vergütung des Auftragnehmers wird über den Lizenzwerb geregelt (Lizenzvertrag). Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

13. Haftung

Für die Haftung gelten die Bestimmungen des Art. 82 DSGVO.

14. Sonderkündigungsrecht

1. Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist außerordentlich kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.
2. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.
3. Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung berechtigt

15. Schlussbestimmungen

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 schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
2. Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
3. Für Nebenabreden ist mindestens Textform erforderlich.
4. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
5. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlage 1 – 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.

Die Maßnahmen müssen im Interesse beider Parteien so konkret wie möglich beschrieben werden! Sie sind Maßstab für Kontrollen durch den Auftraggeber und auch für die Frage entscheidend, ob möglicherweise ein Pflichtverstoß vorliegt. In dieser Anlage wird ganz maßgeblich festgelegt, was der Auftragnehmer zu leisten und nachzuweisen hat und was nicht. Unklare oder interpretationsfähige Umschreibungen sind dringend zu vermeiden!

Für die Vernichtung gem. DIN 66399 gilt Schutzklasse 1.

Zutrittskontrolle

Der Auftragsverarbeiter wird insbesondere die folgenden Maßnahmen treffen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

Die im Zugriff der Future Connection GmbH befindlichen Datenverarbeitungsanlagen (Server) liegen im Rechenzentrum der ionos SE, welches diesbezüglich nach ISO 27001 zertifiziert ist

Zugriffskontrolle

Der Auftragsverarbeiter wird insbesondere die folgenden Maßnahmen treffen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsbeziehung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Zugriffe auf die Systeme sind durch personenbezogene SSH Keys geregelt.
- Zugriffe Auf Dateisystem Ebene bedürfen einer SSH Verbindung mit obiger Authentifizierung.

Weitergabekontrolle

Der Auftragsverarbeiter wird insbesondere die folgenden Maßnahmen treffen, um zu 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:

Sämtliche Übertragungen finden SSL verschlüsselt statt

Einzelne Instanzen von Kunden des Auftraggebers sind auf Betriebssystemebene voneinander getrennt

Eingabekontrolle

Der Auftragsverarbeiter wird insbesondere die folgenden Maßnahmen treffen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Benutzerdaten werden versioniert gespeichert, d.h. jede Mutation wird explizit festgehalten (Journal)

Auftragskontrolle

Der Auftragsverarbeiter wird insbesondere die folgenden Maßnahmen treffen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Trennung der Systeme
- o.g. Zugriffskontrollen
- personenbezogene Daten werden nur durch ausgewählten Personenkreis (CEO, CTO) bearbeitet

Verfügbarkeitskontrolle

Der Auftragsverarbeiter wird insbesondere die folgenden Maßnahmen treffen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Backups der Systeme mit personenbezogenen Daten der Kunden des Auftraggebers werden im Rechenzentrum selbst erstellt und verwahrt (getrennte Feuerschutzzone)

Datentrennung

Der Auftragsverarbeiter wird insbesondere die folgenden Maßnahmen treffen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- n/a personenbezogene Daten werden im System nur zu einem Zweck (Login) verwendet