Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO

zwischen	und
Firma Straße Ort	Infopark Group GmbH Kitzingstraße 15 12277 Berlin
vertreten durch Unternehmensleitung Herr / Frau	vertreten durch Unternehmensleitung Herr Bernd Völcker
im Folgenden: **Auftraggeber**	im Folgenden: **Auftragnehmer**

§ 1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

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

(3) 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

(1) Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Auftrag/Vertrag (im Folgenden „Hauptvertrag“). Der Gegenstand der Auftragsverarbeitung ergibt sich aus dem Hauptvertrag.

(2) Die Laufzeit dieser vertraglichen Vereinbarung richtet sich nach der Laufzeit des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieser vertraglichen Vereinbarung.

§ 3 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in **Anlage 1** näher spezifizierten personenbezogenen Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist ebenfalls in **Anlage 1** dargestellt.

§ 4 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

(2) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(3) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

(4) Soweit Weisungen oder Hinweise nach dieser vertraglichen Vereinbarung zu erfolgen haben, sind diese an die in **Anlage 4** genannten Personen zu richten. Jede Partei kann die angegebenen Kontaktpersonen durch Erklärung in Textform gegenüber der anderen Partei ändern. Die Änderung wird umgehend nach Zugang der Änderungserklärung wirksam.

(5) Ziehen Einzelweisungen Mehrkosten nach sich, insbesondere wenn diese über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind diese dem Auftragnehmer zu vergüten.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

(3) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der in **Anlage 2** festgelegten technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen jedoch nicht unterschritten werden.

(4) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

(5) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(7) Der Auftragnehmer hat einen qualifizierten Beauftragten für den Datenschutz bestellt, dessen Name und Kontaktdaten in **Anlage 4** zu vermerken ist.

(8) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(9) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO obliegt dem Auftragnehmer eine Beweislast nach Art. 82 DSGVO, die Mitwirkungspflichten nach Art. 28 DSGVO sowie die allgemein geltenden Rechenschafts- und Transparenzpflichten nach Art. 5. Der Auftragnehmer verpflichtet sich den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner gesetzlichen Pflichten und im Hinblick auf seine Mithaftung zu unterstützen.

§ 6 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt §5 Abs. 9 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen in **Anlage 4**.

§ 7 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

(2) Bei der Erbringung der Unterstützungsleistungen nach Abs. 1 dem Auftragnehmer entstehenden und nachzuweisenden Aufwände und Kosten sind vom Auftraggeber zu ersetzen.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören. Anlasslose Vor-Ort-Kontrollen wird der Auftraggeber mindestens zwei Wochen im Voraus ankündigen; anlasslose Vor-Ort-Kontrollen dürfen einmalig pro Kalenderjahr durchgeführt werden.

(2) Der Auftragnehmer wird dem Auftraggeber auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung der Verpflichtungen aus diesem Vertrag und zur Erfüllung bestehender datenschutzrechtlicher Verpflichtungen, inklusive der Rechenschaftspflicht, aufzeigen. Hierzu gewährleistet der Auftragnehmer dem Auftraggeber die für die Durchführung der Kontrolle vom Auftragnehmer benötigten Zugangs-, Auskunfts- und Einsichtsrechte. Der Auftragnehmer verpflichtet sich insbesondere, dem Auftraggeber Zugang zu den Datenverarbeitungseinrichtungen und anderen Dokumenten zu gewähren, um die Kontrolle und Überprüfung der relevanten Datenverarbeitungseinrichtungen und andere Dokumentationen zu ermöglichen, die mit der Erhebung oder Verarbeitung von Daten des Auftraggebers im

Zusammenhang stehen. Der Auftraggeber nimmt hierbei Rücksicht auf die Betriebsabläufe und berechtigten Geheimhaltungsinteressen des Auftragnehmers.

§ 9 Subunternehmer

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat. Gleiches gilt für die Ersetzung eines bestehenden Unterauftragnehmers.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Keiner Zustimmung bedarf die Einschaltung von Unterauftragnehmern, bei denen der Unterauftragnehmer lediglich eine Nebenleistung zur Unterstützung bei der Leistungserbringung nach dem Hauptvertrag in Anspruch nimmt, auch wenn dabei ein Zugriff auf die Daten des Auftraggebers nicht ausgeschlossen werden kann; dazu zählen insbesondere Telekommunikationsleistungen, Post- oder Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Der Auftragnehmer wird mit solchen Unterauftragnehmern branchenübliche Geheimhaltungsvereinbarungen treffen.

(3) Eine solche vorherige Zustimmung darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund verweigert werden.

(4) Der Auftraggeber stimmt der Beauftragung der in **Anlage 3** genannten Subunternehmern zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO.

§ 10 Beendigung des Hauptvertrags

(1) Der Auftraggeber kann den Hauptvertrag sowie diesen Vertrag ohne Einhaltung von Kündigungsfristen kündigen, wenn ein schwerwiegender, schuldhafter Verstoß vom Auftragnehmer gegen datenschutzrechtliche Bestimmungen oder Festlegungen dieses Vertrages vorliegt, wenn der Auftragnehmer rechtmäßige Weisungen des Auftraggebers missachtet oder wenn der Auftragnehmer den Zutritt des Auftraggebers oder eines entsprechend Beauftragten zu den Betriebsräumen, in denen Daten auf Grund dieses Vertrages verarbeitet werden, vertragswidrig verweigert.

(2) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht eines Mitgliedstaats für den Auftragnehmer eine Verpflichtung zur Speicherung der

personenbezogenen Daten besteht – vollständig vernichten bzw. unwiderruflich löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer.

(3) Die Löschung/Vernichtung ist in geeigneter Weise – etwa durch eine Protokollierung – zu dokumentieren. Die Dokumentation der Löschung/Vernichtung ist auf Anforderung vorzulegen.

(4) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende vertraglichen Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 11 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser vertraglichen Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser vertraglichen Vereinbarung zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser vertraglichen Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der vertraglichen Vereinbarung im Übrigen nicht.

(4) Es gilt deutsches Recht.

Ort, _____

(Auftraggeber)

Berlin, _____

(Auftragnehmer)

Anlage 1	Beschreibung der personenbezogenen Daten / Datenkategorien und Beschreibung der Kategorien betroffener Personen
Anlage 2	Technische und organisatorische Maßnahmen des Auftragnehmers
Anlage 3	Genehmigte Subunternehmer
Anlage 4	Weisungsberechtigte und Weisungsempfänger sowie Kontaktdaten der Datenschutzbeauftragten

Anlage 1

Beschreibung der personenbezogenen Daten / Datenkategorien und Beschreibung der Kategorien betroffener Personen

1. Verarbeitete Datenarten/-kategorien

Folgende Datenarten oder Kategorien von Daten sind Gegenstand der Auftragsverarbeitung:

- Personenstammdaten (z.B. Vorname und Nachname)
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Adressdaten
- IP-Adresse
- Bewerberdaten (z.B. Zeugnisse, Zertifikate, Referenzen)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Vertragsabrechnungs- und Zahlungsdaten
- Kundenhistorie
- Bankdaten
- Kreditkartendaten
- IT-Daten (z.B. IT-Benutzernamen, Logdateien, Zugriffsrechte)
- Support-Ticket-Daten (z.B. Help-Desk- oder Kundensupport-Ticket-System)

2. Beschreibung der Kategorien betroffener Personen

Folgende Kategorien von Personen (Inhaber/Eigentümer der Daten) sind von der Auftragsverarbeitung betroffen:

- Kunden
- Ansprechpartner
- Interessenten
- Abonnenten
- Lieferanten
- Bewerber

3. Umfang, Art und Zweck der Verarbeitung von personenbezogenen Daten

Folgende Leistungen werden im Rahmen der Auftragsverarbeitung erbracht. Der Auftragnehmer übernimmt folgende Verarbeitungen:

- Speicherung von Inhalten für die Websites des Auftraggebers in Scrivito
- Speicherung von Kundendaten (genaue Daten werden im konkreten Projekt bestimmt und sind Änderungen unterworfen)
- Speicherung von Kontakten zur Authentifizierung und Autorisierung in Scrivito (und auf der Website)

- Vom Auftraggeber explizit beauftragte Verarbeitungen, beispielsweise Fehleranalysen im Bedarfsfall

Die Verarbeitung dient folgendem Zweck:

- Content-Bearbeitung und -Auslieferung (z.B. durch das Content Management System Scrivito)
- Authentifizierung, Autorisierung, Nutzerdatenverwaltung (z.B. Stammdaten und Passwort ändern)
- Fehleranalyse
- Verfügbarkeitsüberwachung
- Performance-Analyse
- Analyse der Kundenbesuche und Optimierung der Website
- Interessenten/Lead-Erfassung auf Websites (z.B. Kontaktformulare, Newsletter-Signup etc.)

Anlage 2

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

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

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen ist zu reduzieren.

Zutrittskontrolle

Technische und organisatorische Maßnahmen:

- Die Zutrittskontrolle zu den Server-Räumen wird durch die räumliche Struktur des jeweiligen Rechenzentrums und die dort durch den Betreiber eingesetzten Kontrollsysteme gewährleistet.
- Während der Zeiten des Geschäftsbetriebs ist der Zutritt zu den Räumen der Infopark Group GmbH in Berlin durch einen individualisierten elektronischen Schlüssel (Transponder) gesichert.
- Außerhalb der Zeiten des Geschäftsbetriebs werden die Räume permanent durch einen externen Dienstleister (Sicherheitsdienst) überwacht (Schließung der Türen und Bewegungsmeldung).
- Zusätzlich werden die Außentüren des Gebäudes außerhalb der Zeiten des Geschäftsbetriebs mechanisch geschlossen.
- Während der Zeiten des Geschäftsbetriebs erfolgt eine Zutrittskontrolle durch Personal im Empfangsbereich.
- Permanent werden Eingangsbereiche und der Technikbereich durch eine optische Raumüberwachung (Video) gesichert.

Zugangskontrolle

Technische und organisatorische Maßnahmen:

- Die unbefugte Nutzung der DV-Systeme wird verhindert durch:
  - Passwortvergabe und
  - Two-Factor Authentication (soweit möglich)
  - Sicherheitsvorgaben für Passwörter (soweit möglich).
- Jeder Berechtigte verfügt über eigene, sichere/lange, nur ihm bekannte Passwörter je Dienst, welche nicht weitergegeben werden dürfen und durch einen zentralen Passwortmanager verwaltet werden. Bei eventuellem Bekanntwerden des Passwortes muss dieses umgehend geändert werden.
- Wann immer möglich, wird eine Two-Factor Authentication zwingend gefordert.
- Für alle relevanten Aktivitäten auf der DV-Anlage werden automatisch Protokolle erstellt.

- Die Protokolle werden vom Systemadministrator regelmäßig stichprobenartig sowie bei Auffälligkeiten (z. B. besonders hohe Aktivität) ausgewertet.
- Die Datenübertragung von und zum DV-System wird bei kritischen Aktivitäten (z. B. Systempflege, Softwareupdates, Backups) durch folgende Maßnahmen gegen Nutzung durch Unbefugte gesichert:
  - Überprüfung bekannter öffentlicher Schlüssel bei Kontaktaufnahme (soweit möglich);
  - Verschlüsselte Datenübertragung (SSH/TLS - wo möglich via Public/Private Key Authentication);
  - Protokollierung der Systemnutzung und Protokollauswertung.

Zugriffskontrolle

Technische und organisatorische Maßnahmen:

- Das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern wird verhindert durch:
  - softwareseitigen Ausschluss (Berechtigungskonzept);
  - softwareseitige Überwachung unplausibler Nutzung (Monitoring);
  - gesicherte Schnittstellen;
  - weitere Kontrollmechanismen des Rechenzentrums.
- Berechtigungen werden nur durch einen kleinen Kreis von Mitarbeitern des Managements nach dem Least-Privilege-Prinzip vergeben.
- Mobile Datenträger dürfen nicht eingesetzt werden. Mobile Backup-Medien kommen nicht zum Einsatz.
- Am Arbeitsplatz und in den Geschäftsräumen werden keine Datenträger vorgehalten. Entwickler haben nur Zugriff auf fiktive Testdaten. Mit Entstörungen beauftragtes Personal kann auf reale Daten zugreifen, soweit dies zur Entstörung notwendig ist.
- Die Einschränkung der Zugriffsmöglichkeit des zur Benutzung eines DV-Systems Berechtigten ausschließlich auf die seiner Zugriffsberechtigung unterliegenden Daten wird gewährleistet durch:
  - automatische Prüfung der Zugriffsberechtigung mittels Passwort;
  - ausschließliche Menüsteuerung je nach Berechtigung;
  - differenzierte Zugriffsberechtigung auf Anwendungsprogramme;
  - differenzierte Verarbeitungsmöglichkeiten (Lesen/Ändern/Löschen).

Trennungskontrolle

Technische und organisatorische Maßnahmen:

- Personenbezogene Daten dürfen nur für den Zweck genutzt werden, für den sie ursprünglich erhoben wurden.
- Dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können, wird gewährleistet durch:
  - softwareseitigen Ausschluss (Mandantentrennung; Multitenancy-Architektur);
  - Trennung über Zugriffsregelung;

- Trennung von Test- und Produktionsdaten;
- Trennung von Entwicklungs- und Produktionsumgebungen.

Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Technische und organisatorische Maßnahmen:

- Als Auftragsverarbeiter trifft die Infopark Group GmbH, zusätzlich zu Maßnahmen die durch den Verantwortlichen im Rahmen der Beauftragung vorgenommen werden, keine weiteren Maßnahmen zur Pseudonymisierung.

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

Weitergabekontrolle

Technische und organisatorische Maßnahmen:

- Ein physischer Versand von Datenträgern ist nicht vorgesehen.
- Private Datenträger dürfen nicht im Rechenzentrum eingesetzt werden (Regelung durch das Rechenzentrum).
- Nicht mehr benötigte magnetische Datenträger werden zunächst durch mehrfaches Überschreiben und anschließend mechanisch zerstört (Regelung durch das Rechenzentrum).
- Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten bei der Übertragung wird verhindert durch:
  - TLS- bzw. SSH-Verschlüsselung der Datenübertragung;
  - Vollständigkeitsüberprüfung, soweit relevant;
  - Aufbau der Transportverbindung nur zwischen definierten und durch Zertifikate (soweit möglich) gesicherten Systemen.
- Die Transportverfahren bestätigen den Empfang der Daten softwareseitig automatisch.
- Alle zum Transport vorgesehenen sensitiven Daten werden verschlüsselt.
- Die Weitergabe personenbezogener Daten erfolgt durch Nutzung folgender Dienste:
  - regelmäßig WWW (HTTPS/TLS);
  - andere Dienste und Transportverfahren, die dem gewünschten Zweck und dem aktuellen Stand der Sicherheitstechnik äquivalent oder besser entsprechen.
- An welchen Stellen Datenübermittlung durch Einrichtungen zur Datenübertragung vorgesehen ist, kann der Dokumentation der Übermittlungsstellen und -wege entnommen werden.

Eingabekontrolle

Technische und organisatorische Maßnahmen

- Ob und von wem Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind, kann nachträglich überprüft und festgestellt werden durch:

- Benutzeridentifikation;
- Protokollierung eingegebener Daten (Verarbeitungsprotokoll).

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

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Nichtverfügbarkeit von im Auftrag verarbeiteten Daten ist zu reduzieren.

Verfügbarkeitskontrolle

Technische und organisatorische Maßnahmen:

- Dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind, wird gewährleistet durch:
  - verteilte Datenhaltung und -verarbeitung über mehrere physisch getrennte Rechenzentrums-standorte hinweg;
  - regelmäßige Datenbank- und Systembackups;
  - zusätzliche Maßnahmen des Rechenzentrums.
- Eine Planung für den Katastrophenfall liegt vor.

Belastbarkeit der Systeme

Technische und organisatorische Maßnahmen:

- Folgende Sicherheitsmaßnahmen existieren:
  - Firewalls und Virtual Private Networks;
  - Intrusion Detection System;
  - Programme die das Eindringen von Viren verhindern bzw. das Eindringen erkennen.

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

Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu betreiben.

Auftragskontrolle

Technische und organisatorische Maßnahmen:

- Es wird keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B. eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht sowie Nachkontrollen, durchgeführt.

- Die Verarbeitung personenbezogener Daten im Auftrag nur entsprechend den Weisungen des Auftraggebers wird gewährleistet durch schriftliche Vereinbarungen zum Datenschutz zwischen Auftraggeber und Auftragnehmer bzw. Rechenzentrum.
- Über gravierende Änderungen im Verfahrensablauf wird der Auftraggeber durch den Auftragnehmer informiert.
- Die Sicherung der Fernwartung entfällt, da keine Fernwartung beim Auftraggeber vorgesehen ist.

Innerbetriebliche Organisation

Technische und organisatorische Maßnahmen:

(a) Datenschutzmanagement

- Nur Mitarbeiter die auf die Einhaltung der datenschutzrechtlichen Vorgaben verpflichtet wurden, dürfen die für ihren Aufgabenbereich entsprechenden Daten verarbeiten.
- Es existieren interne Verhaltensrichtlinien sowie ein Datenschutzhandbuch.
- Alle Mitarbeiter werden in regelmäßig Abständen zum Thema Datenschutz geschult und sensibilisiert.
- In einem Organigramm sowie in Stellenbeschreibungen sind Verantwortlichkeiten und Befugnisse der einzelnen Mitarbeiter festgelegt und im Unternehmen bekannt gemacht. Dieses wird in regelmäßigen Abständen von der obersten Leitung im Rahmen der ISO 9001 Zertifizierung überprüft.

(b) Störfallmanagement

- Die Einhaltung der technischen und organisatorischen Maßnahmen werden jährlich durch den Datenschutzbeauftragten überprüft und gegebenenfalls angepasst (Audit).

(c) Datenschutz durch Technikgestaltung

- Auswahl datenschutzfreundlicher Technologie bei der Beschaffung

Anlage 3

Genehmigte Subunternehmer

Bei den folgenden Unternehmen handelt es sich um genehmigte Subunternehmer.

Anschrift des Subunternehmers	Leistung	Länder, in denen Daten verarbeitet werden
Amazon Web Services, Inc. 410 Terry Avenue North Seattle, WA 98109, USA	Hosting und Betrieb	USA
Github Inc. 88 Colin P Kelly Jr St San Francisco, CA 94107, USA	Quellcodeverwaltung	USA
Google, Inc. 1600 Amphitheatre Pkwy Mountain View CA 94043, USA	E-Mail-Kommunikation	USA
Honeybadger Industries LLC 11410 NE 124th Street #246, Kirkland, WA 98034, USA	Fehler-Tracking	USA
Intercom R&D Unlimited Company 18-21 St. Stephen's Green Dublin 2, Irland	Chat-Kommunikation	Irland
Loggly, Inc. 535 Mission St, Ste 2100 San Francisco, CA 94105, USA	Log-Analyse und -Monitoring	USA
Netlify Inc. 2325 3rd Street, Suite 215 San Francisco, CA 94107, USA	Hosting JavaScript- und HTML-Code	USA
Netsuite / Oracle Inc. 500 Oracle Parkway Redwood Shores, CA, 94403, USA	Buchhaltung/ ERP	USA

Pingdom AB Kopparbergsvägen 8 72213 Västerås, Schweden	Availability/Performance Monitoring	Schweden
Segment.io, Inc. 100 California Street, Suite 700 San Francisco, CA 94111, USA	Dienstorchestrierung Analytics	USA
Slack Technologies, Inc. 155 5th St, 6th Floor San Francisco, CA 94103, USA	Chat-Kommunikation	USA
Stripe, Inc. 510 Townsend Street San Francisco, CA 94103, USA	Zahlungsverkehr	USA

Anlage 4

Weisungsberechtigte und Weisungsempfänger sowie Kontaktdaten der Datenschutzbeauftragten

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner die Nachfolger bzw. die Vertreter mitzuteilen.
(Bitte Daten eintragen):

1. Weisungsberechtigte und Weisungsempfänger

Auftraggeber

Name	Telefon	E-Mail

Auftragnehmer

Name	Telefon	E-Mail

2. Datenschutzbeauftragter

Auftraggeber

Name	Telefon	E-Mail

Auftragnehmer

Stephan Hartinger Coseco GmbH	+49 8232 80988-70	datenschutz@coseco.de