Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO

zwischen

KUNDE

– im Folgenden Auftraggeber genannt –

und der Infopark AG, Kitzingstraße 15, 12277 Berlin

– im Folgenden Auftragnehmer genannt –

§ 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) Gegenstand
Der Auftragnehmer übernimmt folgende Verarbeitungen:

- 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 beruht auf dem Infopark-Angebot 201xxxxxx vom 201x-xx-xx (im Folgenden „Hauptvertrag“).

(2) Dauer
Die Verarbeitung richtet sich nach der Laufzeit des Hauptvertrages.

§ 3 Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

(1) Art und Zweck der Verarbeitung
Die Verarbeitung ist folgender Art: Erfassen, Organisation, Speicherung, vertragsgemäße Verwendung, Löschen von Daten.

Die Verarbeitung dient folgendem Zweck:

- Content-Bearbeitung und -Auslieferung
- Fehleranalyse
- Verfügbarkeitsüberwachung
- Performance-Analyse
- Analyse der Kundenbesuche und Optimierung der Website (nur Einbindung des Codes - Auswertung erfolgt durch den Auftraggeber)
- Bereitstellung von Kartenmaterial zur Anfahrtsbeschreibung und Standortsuche

(2) Art der Daten
Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien

- ☐ 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)
- ☐ Empfänger und Versender von Nachrichten, die an die Auftraggeberin gerichtet sind oder von dieser ausgehen

(3) Kategorien der betroffenen Personen
Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst:

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Ansprechpartner
- ☐ Empfänger und Versender von Nachrichten, die an die Auftraggeberin gerichtet sind oder von dieser ausgehen

§ 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 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.

(3) 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. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten (Anlage 1).
Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gemäß

Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

(4) 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.

(5) 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.

(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
Als Datenschutzbeauftragter ist beim Auftragnehmer bestellt:
Herr Stephan Hartinger
Coseco GmbH
Telefon: 08232 80988-70
E-Mail: datenschutz@coseco.de
Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

(7) 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.

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.
In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.
Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten 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. daten- schutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt §3 Abs. 10 entsprechend.

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

§ 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 sind dem Auftragnehmer entstehende und nachzuweisende Aufwände und Kosten vom Auftraggeber zu ersetzen.

§ 8 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener

Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.
Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen, wenn dies im Vertrag vereinbart ist. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 9 Subunternehmer

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

(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. 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 hiermit gemäß Art. 28 Abs. 2-4 DSGVO als „allgemein schriftliche Genehmigung“ der Beauftragung der in Anlage 2 genannten Subunternehmer zu.

(5) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

(6) Der Auftragnehmer informiert den Auftraggeber vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen diese Änderung Einspruch zu erheben (Art. 28 Abs. 2 DSGVO). Erfolgt kein Einspruch innerhalb von 14 Tage ab Bekanntgabe, gilt die Zustimmung zur Änderung als gegeben.

§ 10 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 Anlage 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 Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

Auftraggeber	Auftragnehmer
	Berlin,
Ort, Datum, Unterschrift	Ort, Datum, Unterschrift

Anlage 1

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 Serverräumen 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 AG 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
  - Protokollierung fehlerhafter Passworteingaben.
- Jeder Berechtigte verfügt über ein eigenes, nur ihm bekanntes Passwort, welches nicht weitergegeben werden darf. Bei eventuellem Bekanntwerden des Passwortes muss dieses umgehend geändert werden.
- 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;
- Verschlüsselte Datenübertragung (SSL/SSH);
- 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.
- Mobile Datenträger dürfen nicht eingesetzt werden. Mobile Backup-Medien kommen nicht zum Einsatz.
- Am Arbeitsplatz werden keine Datenträger vorgehalten. Entwickler haben nur Zugriff auf fiktive Testdaten. Mit Entstörung beauftragtes Personal kann auf realen 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);
  - das Datenbankprinzip, Trennung über Zugriffsregelung;
  - Trennung von Test- und Produktionsdaten;
  - Trennung von Entwicklungs- und Produktionsprogrammen.

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

Technische und organisatorische Maßnahmen:

- Als Auftragsverarbeiter trifft die Infopark AG, 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 durch mehrfaches Überschreiben zerstört (Regelung durch das Rechenzentrum).
- Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten bei der Übertragung wird verhindert durch:
  - SSL- bzw. SSH-Verschlüsselung der Datenübertragung;
  - Vollständigkeitsüberprüfung, soweit relevant;
  - Aufbau der Transportverbindung nur zwischen definierten und durch Zertifikate 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);
  - 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:
  - Einsatz von RAID-Festplattensystemen;
  - softwareseitigen Ausschluss: Aufteilung der Server zur unabhängigen und eigenständigen Erfüllung der Aufgaben (Shared-Nothing-Architektur);
  - mehrfache inkrementelle Datenbank- und Systembackups;
  - Backups nach einem Zeitplan der die Veränderungen der Daten durch Nutzung angemessen reflektiert;
  - Mehrfache, getrennte Ablage der Backup-Daten;
  - zusätzliche Maßnahmen des Rechenzentrums.
- Eine Planung für den Katastrophenfall liegt vor.
- Das System wird an geographisch getrennten Rechenzentren betrieben (Verfügbarkeitszonen).

Belastbarkeit der Systeme

Technische und organisatorische Maßnahmen:

- Folgende Sicherheitsmaßnahmen existieren:
  - Hardware- und Software-Firewall;
  - 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, 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 Datenschutz Handbuch
- Alle Mitarbeiter werden in regelmäßig Abständen zum Thema Datenschutz per E-Learning 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 technisch- organisatorischen Maßnahmen werden jährlich (Audit) durch den Datenschutzbeauftragten überprüft und gegebenenfalls angepasst.

(c) Datenschutzes durch Technikgestaltung

- Auswahl datenschutzfreundlicher Technologie bei der Beschaffung

Anlage 2

Subunternehmer

Folgende Subunternehmer sind für die Erbringung von Teilleistungen tätig.

- Subunternehmer 1 (Firma, Kontaktdaten)
- Subunternehmer 2 (Firma, Kontaktdaten)