Empolis Industrial Knowledge

Auftragsverarbeitungsvertrag

Betrieb & Datensicherheit

Empolis Information Management GmbH

Europaallee 10

D-67657 Kaiserslautern

Inhaltsverzeichnis

1 Betrieb der Lösung

1.1 Rechenzentrum: Zertifizierung und Richtlinien

Empolis betreibt die Software auf Basis der Amazon Web Services (AWS) in der Region Frankfurt am Main. Die AWS Rechenzentren und Services sind Stand heute nach den Standards ISO 27001, ISO 27017, ISO 27018 und dem deutschen Cloud Computing Compliance Controls Catalog (C5) des BSI zertifiziert. Der Standard ISO 27001 definiert die Anforderungen an die Etablierung, Implementierung, den Betrieb, das Monitoring, die Überprüfung, die Wartung und Verbesserung eines dokumentierten Managementsystems für Informationssicherheit im Zusammenhang mit den gesamten Geschäftsrisiken einer Organisation. Im Ergebnis gewährleistet der Standard somit Best Practices für Sicherheitsprozesse, welche dem Schutz von Informationsressourcen dienen.

1.2 Datenzugriff und -übertragung

Der Zugriff auf die Software erfolgt ausschließlich browserbasiert. Um Daten nach dem Stand der Technik abhörsicher zu übertragen, wird HTTPS als Protokoll verwendet. Die Verschlüsselung der Daten geschieht mittels SSL/TLS[1]. Der Standard Port für HTTPS ist 443. Dieser muss für die Nutzer geöffnet sein.

[1] https://tools.ietf.org/html/rfc2818

2 Datensicherheit

2.1 Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

2.2 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

- Art der Daten: Konto-, Zugriffs- und Kundendaten
- Art und Zweck der Datenverarbeitung: Einsatz eines durch Empolis bereitgestellten Wissensmanagementsystems für den Bereich Service
- Kategorien betroffener Personen: Benutzer des Systems

Detaillierte Informationen finden Sie auf den folgenden Webseiten:

https://esc-eu-central-1.empolisservices.com/doc/de/legal/privacy-policy.html
https://www.service.express/agb/

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüberhinausgehende Verpflichtungen ergeben.

2.3 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 DS-GVO).
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 (Ein-

zelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

2.4 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) DS-GVO 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 DS-GVO) 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.

   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 gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Artt. 33 bis 36 DS-GVO genannten Pflichten.
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.
7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO 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.
10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

2.5 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 DS-GVO, gilt Kap. 2.4 Abs. 10 entsprechend.
3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

2.6 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.

2.7 Nachweismöglichkeiten

1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach, beispielsweise durch: Durchführung eines Selbstaudits, unternehmensinterne Verhaltensregeln einschließlich eines externen Nachweises über deren Einhaltung, Zertifikat zu Datenschutz und/oder Informationssicherheit (z. B. ISO 27001), genehmigte Verhaltensregeln nach Art. 40 DS-GVO, Zertifikate nach Art. 42 DS-GVO oder andere, zu vereinbarende Nachweise.
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.

2.8 Subunternehmer (weitere Auftragsverarbeiter)

1) Der Auftragnehmer setzt für die Verarbeitung folgende Unterauftragsverarbeiter ein:

Vertragspartner	Zwecke	Vorliegende Vereinbarung
Amazon Web Services EMEA SARL, Luxemburg	Technische Infrastruktur	Standardvertragsklauseln
Amplitude, Sonalight Inc., USA (Daten liegen auf Servern in Deutschland)	Tool für Benutzer-Monitoring	Standardvertragsklauseln
CleverReach GmbH & Co. KG, Rastede	Tool für Benutzer-Benachrich-tigungen	Auftragsverarbeitungsvertrag
Enozom Software, Ägypten	SW-Entwicklung	Standardvertragsklauseln
Lamano GmbH & Co. KG, Berlin ("Lamapoll")	Tool für Benutzer-Feedback	Auftragsverarbeitungsvertrag
Logicline GmbH, Sindelfingen	SW-Entwicklung	Auftragsverarbeitungsvertrag
Microsoft Ireland Operations Ltd., Irland	Technische Infrastruktur (Ge-nAI, optional)	Auftragsverarbeitungsvertrag
Sendbird Inc., USA (Daten liegen auf Servern in Deutschland)	Tool für Chat-Funktion (optional)	Standardvertragsklauseln
Verlinked GmbH, Paderborn	Integration von Maschinenda-ten (optional)	Auftragsverarbeitungsvertrag

Tabelle 1: Subunternehmer

2) Der Auftragnehmer ist verpflichtet, den Auftraggeber rechtzeitig vorab über die Beauftragung neuer Unterauftragsverarbeiter oder eine Änderung einer bestehenden Unterbeauftragung in Textform zu informieren. Der Auftraggeber kann der entsprechenden Maßnahme bei Vorliegen berechtigenden Grundes innerhalb von vier Wochen nach Veröffentlichung gemäß Satz 1 widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln besteht, dass der Unterauftragsverarbeiter die vereinbarte Leistung entsprechend den anwendbaren gesetzlichen Bestimmungen zum Datenschutz oder gemäß den Vereinbarungen der Parteien erbringt. Sofern dem Auftragnehmer aufgrund des Widerspruchs die weitere Erbringung der von ihm geschuldeten Leistungen nicht möglich oder zumutbar ist, ist er zu einer Kündigung des Hauptvertrages aus wichtigem Grund berechtigt. Er wird dem Auftraggeber über die Kündigungsabsicht vorab informieren.
3) Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

2.9 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.

2.10 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

Eine zwischen den Parteien im Hauptvertrag zur Leistungserbringung vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart ist.

3 Technische und organisatorische Maßnahmen gemäß DSGVO

3.1 Anforderungen

1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentier-ten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.
3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

3.2 Umsetzung

3.2.1 Vertraulichkeit

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

3.2.1.1 Zutrittskontrolle

Für die Büroräume der Empolis Information Management GmbH existieren entsprechende Gebäudesicherungen an den Standorten sowie ein dokumentiertes Ausweis-/Schlüsselsystem für alle Mitarbeiter. Zum Teil sind Videoüberwachungsanlagen installiert. Betriebsfremde betreten das Unternehmen nur nach Vereinbarung bzw. nur mit Begleitung. Regelmäßig tätige Dienstleister, die ihre Aufgaben auch

außerhalb der Geschäftszeiten ausüben (z. B. Reinigungskräfte) sind auf Vertraulichkeit verpflichtet. Empolis Information Management GmbH ist nach ISO 9001 sowie nach DIN ISO/IEC 27001 zertifiziert.

Der Zugang zu Gebäuden, Data Floors und dedizierten Kundenbereichen der beauftragten Rechenzentren ist nur über individuell programmierte Zugangskarten mit biometrischer oder visueller Identifikation möglich, so dass jeweils nur eine einzelne Person gesicherten Zutritt erhält. Das Rechenzentrum ist an 365 Tagen im Jahr 24 Stunden durch Wachpersonal besetzt. Zusätzlich werden die Eingangsbereiche und Außenanlagen sowie alle sensiblen Bereiche im Inneren durch Kameras überwacht.

3.2.1.2 Zugangskontrolle

Alle Systeme der Empolis Information Management GmbH sind passwortgeschützt. Die Mitarbeiter müssen ihre Passwörter komplex gestalten; diese Vorgabe kann nicht umgangen werden. Es gilt eine Betriebsvereinbarung zum Umgang mit elektronischen Medien, darüber hinaus sind alle Mitarbeiter mit Beginn des Beschäftigtenverhältnisses auf Geheimhaltung verpflichtet.

Der Zugang zu dedizierten Kundenbereichen im beauftragten Rechenzentrum ist nur über individuell programmierte Zugangskarten mit biometrischer und visueller Identifikation möglich, so dass jeweils nur eine einzelne Person gesicherten Zutritt erhält.

3.2.1.3 Zugriffskontrolle

Die Systeme der Empolis Information Management GmbH sind mit einem differenzierten Rollen- und Berechtigungskonzept gegen unberechtigte Nutzung jeglicher Art abgesichert.

Empolis Information Management GmbH führt im beauftragten Rechenzentrum grundsätzlich keine Tätigkeiten mit unmittelbaren Zugriffsmöglichkeiten auf die IT-Systeme des Auftraggebers und auf dort gespeicherte oder verarbeitete Daten aus. Im Rahmen des Auftragsverhältnisses zwischen Auftraggeber und Empolis Information Management GmbH sind insoweit in der Regel keine datenschutzrelevanten Tätigkeiten vorgesehen, sondern ausschließlich Tätigkeiten des System-Monitorings und der Fehlerbehebung im Störungsfall, die in der Regel vom Auftraggeber gemeldet werden.

3.2.1.4 Verwendungszweckkontrolle

Empolis Information Management GmbH hält die Kundendaten durch eine interne Mandantentrennung vollständig voneinander getrennt vor. Auch sind Produktiv- von Testumgebungen voneinander abgegrenzt. Empolis Information Management GmbH ist nach DIN ISO/IEC 27001 zertifiziert.

Für die beauftragten Rechenzentren gelten analoge Zertifizierungen: DIN ISO/IEC 27001, TÜV-geprüftes Rechenzentrum, Datacenter Star Audit, PCI DSS approved.

3.2.1.5 Pseudonymisierung

(Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Dies ist definiert als die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen. Diese Aufgabe obliegt dem Auftraggeber.

3.2.2 Integrität

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

3.2.2.1 Weitergabekontrolle

Empolis Information Management GmbH arbeitet grundsätzlich über sichere VPN-Verbindungen.

Empolis Information Management GmbH führt im beauftragten Rechenzentrum grundsätzlich keine Tätigkeiten mit unmittelbaren Zugriffsmöglichkeiten auf die IT-Systeme/Daten des Auftraggebers und auf dort gespeicherte oder verarbeitete Daten aus. Ausnahmen bilden die Wartungszugriffe für das Systemmonitoring und die Fehlerbehebung. Die physikalischen Sicherheitsvorkehrungen sind unter den Punkten Zutrittskontrolle bzw. Zugangskontrolle beschrieben. Zugriffe durch den Auftraggeber laufen über dedizierte, sichere Verbindungen.

3.2.2.2 Eingabekontrolle

Empolis Information Management GmbH arbeitet innerhalb seiner Systeme mit angemessenen Systemprotokollierungen; die Eingaben in die dem Auftraggeber bereitgestellten Software-Systeme nimmt ausschließlich der Auftraggeber selbst vor.

Empolis Information Management GmbH führt im beauftragten Rechenzentrum grundsätzlich keine Tätigkeiten mit unmittelbaren Zugriffsmöglichkeiten auf die IT-Systeme/Daten des Auftraggebers und auf dort gespeicherte oder verarbeitete Daten aus. Die physikalischen Sicherheitsvorkehrungen sind unter den Punkten Zutrittskontrolle bzw. Zugangskontrolle beschrieben. Zugriffe durch den Auftraggeber laufen über dedizierte, sichere Verbindungen.

3.2.2.3 Auftragskontrolle

Empolis Information Management GmbH führt den Auftrag ausschließlich auf Basis des abgeschlossenen Vertrags und des dazugehörenden Anhanges aus. Subunternehmer werden sorgfältig ausgewählt und überwacht.

3.2.2.4 Organisationskontrolle

Empolis Information Management GmbH arbeitet nach einem ISO-9001-zertifizierten Qualitätsmanagementsystem und ist darüber hinaus gemäß DIN ISO/IEC 27001 zertifiziert. Die damit verbundenen Zielsetzungen, Prozessbeschreibungen und kontinuierlichen Verbesserungsaktivitäten sichern die Einhaltung gesetzlicher Vorgaben und einen organisierten und nachvollziehbaren Umgang mit Daten und Informationen.

3.2.2.5 Qualitätsicherung und Training von Standard-Software

Von den vorstehenden Vereinbarungen unberührt bleiben die Nutzungsbedingungen der Standard-Software und die hieraus resultierende Nutzung der Daten des Auftraggebers für Zwecke der Qualitätssicherung und des Trainings. Zu diesem Zweck wird unter Beachtung des Auftragsverarbeitungsvertrages und der Vorgaben zur Sicherheit der Verarbeitung gemäß Art 32 DSGVO auf die Kundendaten zugegriffen und diese entsprechend verarbeitet.

3.2.3 Verfügbarkeit und Belastbarkeit

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

3.2.3.1 Verfügbarkeitskontrolle

Die Systeme der Empolis Information Management GmbH sind durch angemessene Back-up-Verfahren, eine unterbrechungsfreie Stromversorgung sowie aktuelle Virenschutz- und Fire-Wall-Vorkehrungen geschützt. Empolis Information Management GmbH ist nach DIN ISO/IEC 27001 zertifiziert.

Die beauftragten Rechenzentren sind ebenfalls so ausgewählt, dass durch ihre Zertifizierungen (DIN ISO/IEC 27001 oder vergleichbar) und die zugesicherten SLAs eine angemessene Verfügbarkeit gewährleistet ist.

3.2.3.2 Rasche Wiederherstellbarkeit

(Art. 32 Abs. 1 lit. c DS-GVO)

Diese Anforderung wird durch die Zertifizierungen der Empolis Information Management GmbH gemäß DIN ISO/IEC 27001 erfüllt.

3.2.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Diese Anforderung wird durch die Zertifizierungen der Empolis Information Management GmbH gemäß DIN ISO/IEC 27001 erfüllt.