Vertrag zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

DeepL SE
Maarweg 165
50825 Köln
Deutschland

(im Folgenden als „**Auftragsverarbeiter**“ bezeichnet)

verpflichtet sich gegenüber

Scopewire Data GmbH
Leihbühl 21
33165 Lichtenau
Germany

(im Folgenden als „**Verantwortlicher**“ bezeichnet)

(im Folgenden zusammen als „**die Parteien**“ bezeichnet)

nach Maßgabe der folgenden Bestimmungen.

Allgemeine Bestimmungen

§ 1 Anwendungsbereich und Begriffsbestimmung

Der Auftragsverarbeiter hat mit dem Verantwortlichen einen Vertrag unter Einbeziehung der Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters geschlossen („Hauptvertrag“) und gewährt dem Verantwortlichen auf dieser Basis Zugang zu den im Hauptvertrag genannten Diensten, insbesondere zu seinem KI-basierten Übersetzungsservice DeepL Pro, (nachfolgend „DeepL Dienste“ genannt). Im Rahmen der Nutzung der DeepL Dienste kann der Verantwortliche personenbezogene Daten i.S.d. Art. 4 Nr. 1 Datenschutz-Grundverordnung (EU) 2016/679 („DSGVO“) an den Auftragsverarbeiter zur Verarbeitung (z.B. zur Übersetzung) durch die DeepL Dienste übermitteln. Der vorliegende Vertrag zur Auftragsverarbeitung („Vertrag“) regelt die Rechte und Pflichten der Parteien hinsichtlich einer solchen Verarbeitung von personenbezogenen Daten.

Sofern in diesem Vertrag weitere Begriffe verwendet werden, die in der DSGVO definiert sind, haben sie dieselbe Bedeutung wie es in der DSGVO festgelegt ist.

§ 2 Gegenstand, Umfang und Ort der Auftragsverarbeitung

1. Gegenstand, Dauer und Umfang

Die vom Verantwortlichen übermittelten personenbezogenen Daten werden für die Dauer des Hauptvertrags zu dem dort vereinbarten Zweck und Umfang, sprich der Erbringung der Dienstleistung im Rahmen der DeepL Dienste, verarbeitet.

2. Arten der verarbeiteten personenbezogenen Daten

Verarbeitet werden alle Arten von personenbezogenen Daten, die der Verantwortliche zur Verarbeitung (z.B. Übersetzung) an die DeepL Dienste übermittelt. Der Auftragsverarbeiter hat keinen Einfluss auf die Art der übermittelten Daten, daher können personenbezogenen Daten verschiedenster Art verarbeitet werden. Neben allgemeinen personenbezogenen Daten können dies auch besondere Kategorien personenbezogener Daten sein.

3. Kreis der Betroffenen

Der Kreis der Betroffenen ergibt sich ebenfalls aus den Texten, die der Verantwortliche als Inhalt an die DeepL Dienste übermittelt und kann daher nicht abschließend festgelegt werden. Es können unterschiedliche Personengruppen betroffen sein, wie beispielsweise die Daten von Kunden, Beschäftigten oder Bewerbern des Verantwortlichen.

4. Ort der Datenverarbeitung

Zurzeit werden die vertraglich vereinbarten DeepL Dienste in einem der Mitgliedsstaaten der Europäischen Union (EU) oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) erbracht. Eine vollständige oder teilweise Verlagerung der Dienstleistung in ein Drittland sowie die Inanspruchnahme eines Unterauftragsverarbeiters in einem Drittland wird nur dann erfolgen, wenn die besonderen Anforderungen der Artikel 44 ff. DSGVO eingehalten werden (z. B. Angemessenheitsentscheidung der EU-Kommission, Standardvertragsklauseln, genehmigte Verhaltenskodizes) und eine entsprechende Weisung des Verantwortlichen, die auch in den Account-Einstellungen erteilt werden kann, vorliegt.

§ 3 Sonstige Regelungen

Sollte die auftragsgemäße Erfüllung des Auftragsgegenstandes gemäß § 1 dieser Vereinbarung beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder ein Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Beteiligte unverzüglich darüber informieren, dass die Verfügungsbefugnisse an den Daten ausschließlich beim Verantwortlichen liegen.

Bei etwaigen Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags den Regelungen des Hauptvertrags vor.

Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

Jede Veränderung dieser Vereinbarung einschließlich ihrer Kündigung sowie die Änderung dieser Klausel bedarf der Schriftform, wobei die elektronische Form genügt.

Auftragsverarbeitung gemäß Art. 28 DSGVO

§ 4 Weisungsgebundene Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn er ist durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Verarbeitung verpflichtet; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Durch den Abschluss dieses Vertrags weist der Verantwortliche den Auftragsverarbeiter an, die personenbezogenen Daten des Verantwortlichen in dem Umfang zu verarbeiten, der erforderlich ist, um die Verpflichtungen aus dem Hauptvertrag zu erfüllen.

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die DSGVO oder sonstige Datenschutzbestimmungen verstoßen.

§ 5 Vertraulichkeits-/ Verschwiegenheitspflicht

Der Auftragsverarbeiter wird zur Durchführung des Vertrages nur Personen beschäftigen, die er zur Vertraulichkeit verpflichtet hat oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 6 Sicherheit der Verarbeitung / Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Der Auftragsverarbeiter ergreift alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Artikel 32 DSGVO, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Diese werden in Anlage 2 spezifiziert.

Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieses Vertrags sind diese durch den Auftragsverarbeiter fortlaufend an die Anforderungen dieses Vertrags anzupassen und dem technischen Fortschritt entsprechend weiterzuentwickeln. Das Sicherheitsniveau der hier und in Anlage 2 festgelegten technischen und organisatorischen Maßnahmen darf nicht unterschritten werden.

Der Auftragsverarbeiter verpflichtet sich, Änderungen der technischen und organisatorischen Maßnahmen, die einen wesentlichen Einfluss auf das gewährleistete Sicherheitsniveau haben, als Ergänzung der Anlage 2 schriftlich zu dokumentieren, was auch in einem elektronischen Format erfolgen kann, und dem Verantwortlichen zur Kenntnis zu geben.

§ 7 Inanspruchnahme der Dienste weiterer Auftragsverarbeiter

Der Auftragsverarbeiter nimmt derzeit die in Anlage 1 genannten externen Unterauftragsverarbeiter in Anspruch. Der Verantwortliche erteilt hiermit explizit seine Zustimmung zur Beauftragung der in der Anlage aufgeführten externen Unterauftragsverarbeiter sowie aller verbundenen Unternehmen (wie im Hauptvertrag definiert), die gegebenenfalls als Unterauftragsverarbeiter eingesetzt werden.

Der Auftragsverarbeiter ist zudem grundsätzlich berechtigt, weitere Unterauftragsverarbeiter in Anspruch zu nehmen. Der Auftragsverarbeiter wird dies nur tun, wenn er den Verantwortlichen zuvor

über die beabsichtigte Änderung informiert hat. Gegen derartige Veränderungen kann der Verantwortliche innerhalb von zwei (2) Wochen Einspruch erheben.

Nimmt der Auftragsverarbeiter die Dienste eines Unterauftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, stellt der Auftragsverarbeiter sicher, dass dem Unterauftragsverarbeiter im Wege eines schriftlich abzuschließenden Vertrags im Wesentlichen dieselben Datenschutzpflichten auferlegt werden, wie sie in diesem Vertrag festgelegt sind. Der Vertrag kann auch elektronisch abgeschlossen werden und muss insbesondere hinreichende Garantien dafür bieten, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Unterauftragsverarbeiters.

§ 8 Mitwirkungs-/ Unterstützungspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen (Berücksichtigung von Betroffenenrechten hinsichtlich der Gewährleistung von Transparenz; Recht auf Auskunft; Recht auf Berichtigung und Löschung; Recht auf Einschränkung der Verarbeitung; Mitteilungsrecht bei Berichtigung und Löschung sowie Einschränkung der Verarbeitung; Recht auf Datenübertragbarkeit; Widerspruchsrecht; Rechte bei automatisierten Einzelfallentscheidungen).

§ 9 Unterstützung zur Pflichterfüllung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten (Gewährleistung der Sicherheit der Verarbeitung; Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörden; Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person; Datenschutz-Folgenabschätzung; vorherige Konsultation).

Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten i.S.d. Art. 4 Nr. 12 DSGVO bekannt wird und die Verletzung personenbezogene Daten betrifft, die der Verantwortliche zur Verarbeitung (z.B. zur Übersetzung) an die DeepL Dienste übermittelt hat, meldet er dies dem Verantwortlichen unverzüglich nach Kenntnis von einem solchen Vorfall. Der Auftragsverarbeiter stellt dem Verantwortlichen ausreichende Informationen zur Verfügung, damit der Verantwortliche möglichen Melde- oder Informationspflichten gegenüber der Aufsichtsbehörde sowie gegenüber den Betroffenen nachkommen kann.

§ 10 Löschung und Rückgabe personenbezogener Daten

Der Auftragsverarbeiter verarbeitet die vom Verantwortlichen übermittelten personenbezogenen Daten nur so lange, wie es zur Erfüllung der gemäß dem Hauptvertrag geschuldeten Leistung erforderlich ist und löscht diese anschließend datenschutzkonform.

§ 11 Pflichtennachweis und Unterstützung bei Überprüfungen

Der Auftragsverarbeiter wird dem Verantwortlichen auf dessen Anforderung alle erforderlichen und beim Auftragsverarbeiter vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.

Der Verantwortliche ist berechtigt, den Auftragsverarbeiter bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Vor-Ort-Inspektionen. Der Verantwortliche darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragsverarbeiter.

Für Überprüfungen in Gestalt von Vor-Ort-Inspektionen ist der Verantwortliche im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 10 bis 18 Uhr) berechtigt, die Geschäftsräume des Auftragsverarbeiters, in denen Daten des Verantwortlichen verarbeitet werden, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragsverarbeiters zu betreten. Der Verantwortliche hat den Auftragsverarbeiter rechtzeitig (in der Regel mindestens zwei Wochen vorher) über eine Vor-Ort-Inspektion und alle mit der Durchführung der Vor-Ort-Inspektion zusammenhängenden Umstände zu informieren.

Der Auftragsverarbeiter ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Verantwortlichen, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragsverarbeiters sind oder wenn der Auftragsverarbeiter durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Verantwortliche ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragsverarbeiters, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragsverarbeiters, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten. Zur Durchführung von Überprüfungen sind nur fachkundige Personen zugelassen, die sich legitimieren können und im Hinblick auf die Betriebs- und Geschäftsgeheimnisse sowie Prozesse des Auftragsverarbeiters zur Verschwiegenheit verpflichtet sind.

Nach Wahl des Auftragsverarbeiters kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrag anstatt durch eine Überprüfung (einschließlich einer Vor-Ort-Inspektion) auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten IT-Sicherheit oder Datenschutz-Zertifizierung – z. B. nach BSI-Grundschutz („Prüfungsbericht“) – erbracht werden, wenn der Prüfungsbericht es dem Verantwortlichen in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

Köln	Lichtenau 2/4/2024
	Ort, Datum
Jan Mirko Schäfer	Holm Egerland
DeepL SE	Firma Scopewire Data GmbH
Jan Mirko Schäfer	Name Holm J. Egerland
General Counsel	Titel Geschäftsführer

Anlagen

Anlage 1

Liste der eingesetzten externen Unterauftragsverarbeiter

Name des eingesetzten Unterauftragsverarbeiters	Zur Verfügung gestellter Service	Art der verarbeiteten Daten	Ort der Datenverarbeitung
keine *			

* Der Auftragsverarbeiter setzt derzeit keine externen Unterauftragsverarbeiter ein, die den Auftragsverarbeiter bei der Verarbeitung personenbezogener Daten im Rahmen dieses Vertrages unterstützen.

Anlage 2

Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Unter Berücksichtigung des

- Stands der Technik,
- der Implementierungskosten und
- der Art, des Umfangs, der Umstände und
- der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

trifft der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw. unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Vorausgestellt zu den einzelnen Maßnahmen sei das grundlegende Sicherheitskonzept der DeepL SE:

Sofern nicht ausdrücklich abweichend in diesem Vertrag (z.B. in Anlage 1, hinsichtlich der Beauftragung von Unterauftragsverarbeitern) angegeben, werden die zur Verarbeitung (z.B. zur Übersetzung) an die DeepL Dienste übermittelten Daten ausschließlich in Ländern innerhalb des europäischen Wirtschaftsraumes (EWR) verarbeitet. Die Daten werden auf dem Übertragungsweg ins Rechenzentrum durch kryptografische Verfahren nach dem heutigen Stand der Technik verschlüsselt. Auf den Systemen der DeepL SE werden die Daten nur für die Dauer der Verarbeitung gespeichert. Während dieser Speicherung und auch während der Übertragung zum Benutzer sind die Daten verschlüsselt. Sobald die von den DeepL Diensten verarbeiteten Daten zum Benutzer übertragen wurde, werden die Daten auf den Systemen unwiderruflich gelöscht.

Die DeepL Server werden ausschließlich von Mitarbeitern der DeepL SE administriert (Co-Location Modell). Durch den Standort in einem hochmodernen, ISO/IEC 27001 zertifizierten Rechenzentrum bietet die DeepL SE den höchsten Standard bzgl. Zutrittskontrolle und Ausfallsicherheit.

Der Auftragsverarbeiter ergreift folgende Maßnahmen:

1. Pseudonymisierung

Eine Pseudonymisierung sorgt dafür, dass personenbezogene Daten nur noch durch Hinzuziehung zusätzlicher Informationen einer spezifischen Person zugeordnet werden können.

Der Auftragsverarbeiter erhält im Rahmen der Vertragserfüllung keine strukturierten Daten. Vielmehr erhält er Texte, die zwecks Verarbeitung durch die DeepL Dienste klar und nicht pseudonymisiert sein müssen. Daher ist im Rahmen der Vertragserfüllung die Pseudonymisierung keine geeignete Maßnahme für den Auftragsverarbeiter.

2. Maßnahmen zur Verschlüsselung

Mit der Verschlüsselung werden die Daten vor der Kenntnisnahme durch unbefugte Dritte geschützt. Dabei werden Daten während des Transports zum Benutzer und der Speicherung durch eine Verschlüsselung geschützt. Im Einzelnen bestehen insbesondere folgende Maßnahmen:

- Die Übermittlung von Daten zwischen dem Benutzer des DeepL-Pro-Dienstes und den Rechnern der DeepL SE wird im öffentlichen Internet nur verschlüsselt durchgeführt (Gesicherte

Datenweitergabe über SSL, TLS). Die erlaubten Verschlüsselungsverfahren werden nach dem Stand der Technik ausgewählt.

- Soweit Daten auf Festplatte gespeichert werden, sind diese immer entsprechend des Standes der Technik verschlüsselt.

3. Maßnahmen zur Sicherstellung von Vertraulichkeit

Neben der Verschlüsselung werden weitere Maßnahmen ergriffen, um die Vertraulichkeit der personenbezogenen Daten zu sichern. Hierbei wird regelmäßig zwischen Maßnahmen zur Zutritts-, Zugangs- und Zugriffskontrolle unterschieden:

a. Zutrittskontrolle

Die Maßnahmen der Zutrittskontrolle stellen sicher, dass ein Unbefugter sich keinen Zutritt in Gebäude oder einzelne Räume verschaffen kann, in denen personenbezogene Daten verarbeiten werden. Im Einzelnen bestehen insbesondere folgende Maßnahmen:

- Zutrittskontrollierter und eingezäunter Bereich
- Zentrale Zugriffsberechtigung für die Zutrittskontrolle
- Einbruchmeldeanlage
- Gebäude-im-Gebäudebau
- Mehrere Sicherheitszonen
- Sehr eingeschränkter Zugang zu Serverhallen
- Videoüberwachungssystem (intern und extern)
- Sicherheitspatrouillen
- Direkte Alarme an den diensthabenden Sicherheitsbeauftragten

b. Zugangskontrolle

Mit den Maßnahmen der Zugangskontrolle wird sichergestellt, dass keine unbefugte Benutzung der Systeme erfolgen kann, mit denen die personenbezogenen Daten verarbeitet werden. Im Einzelnen bestehen insbesondere folgende Maßnahmen:

- Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmens-netzwerk
- Autorisierungsprozess für Zugangsberechtigungen
- Begrenzung der befugten Benutzer
- Kennwortverfahren (hohe Komplexität durch entsprechende Schlüssel)
- Token
- Zwei-Faktor- Authentifizierung
- Protokollierung des Zugangs
- Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität
- Firewall
- Host IDS/IPS

c. Zugriffskontrolle

Die Maßnahmen zur Zugriffskontrolle stellen sicher, dass innerhalb des Systems nur befugte Personen die jeweiligen personenbezogenen Daten verarbeiten können. Insbesondere erhalten die Mitarbeiter nur Zugriff auf die personenbezogenen Daten, die sie für die Erledigung ihrer Aufgaben im Unternehmen des Auftragsverarbeiters benötigen. Im Einzelnen bestehen insbesondere folgende Maßnahmen:

- Verwaltung und Dokumentation von differenzierten Berechtigungen
- Jährliche Re-Zertifizierungen der Berechtigungen
- Protokollierungen von Zugriffen
- Genehmigungsroutinen
- Profile/Rollen
- Zugriffsgruppen und geplanter Zugriff

4. Maßnahmen zur Sicherstellung von Integrität

Zum Schutz vor unrechtmäßiger oder ungewollter Veränderung bzw. Löschung von personenbezogenen Daten werden technische und organisatorische Maßnahmen eingesetzt, die die Integrität sichern. Im Einzelnen bestehen insbesondere folgende Maßnahmen:

- Zugriffsrechte
- Sicherstellung Integrität durch Verschlüsselung von abgespeicherten Daten
- Systemseitige Protokollierungen
- Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- Protokollierung von Datenübertragung oder Datentransport

5. Maßnahmen zur Sicherstellung und Wiederherstellung von Verfügbarkeit

Die personenbezogenen Daten werden durch Maßnahmen zur Sicherstellung und Wiederherstellung der Verfügbarkeit vor zufälliger oder mutwilliger Zerstörung bzw. Verlust gesichert. Die Maßnahmen sind dabei so gewählt, dass Schadensereignisse, die zu einem Datenverlust führen können (z.B. Virenbefall, Überhitzung) bereits präventiv verhindert werden, aber auch so, dass bei einem Zwischenfall der Datenbestand möglichst vollständig wiederhergestellt werden kann. Die Maßnahmen beziehen sich auf die kurze Zeitspanne, in der die Daten überhaupt auf den Servern der DeepL SE liegen. Im Einzelnen bestehen insbesondere folgende Maßnahmen:

- Sicherheitskonzept für Software- und IT-Anwendungen
- Redundante Struktur
- Bedarfsgerechtes Einspielen von Sicherheits-Updates
- Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
- Klimatisiertes Rechenzentrum
- Schutz vor Schadsoftware
- Firewall
- Notfallplan

6. Maßnahmen zur Sicherstellung der Belastbarkeit

Die Systeme zur Datenverarbeitung müssen belastbar sein, um einen unbefugten Zugriff oder den Verlust bzw. die Veränderung von personenbezogenen Daten zu verhindern. Im Einzelnen bestehen insbesondere folgende Maßnahmen:

- Notfallplan für Maschinenausfall
- Redundante Stromversorgung
- Ausreichende Kapazität von IT-Systeme und Anlagen
- Logistisch gesteuerter Prozess zur Verhinderung von Leistungsspitzen
- Redundante Systeme/Anlagen

7. Maßnahmen zur Gewährleistung der Wirksamkeitskontrolle

Mit den Maßnahmen zur Wirksamkeitskontrolle werden die getroffenen Sicherungsmaßnahmen regelmäßig überprüft. Sind Maßnahmen nicht mehr zeitgemäß oder aus anderen Gründen nicht mehr ausreichend, werden sie nachgebessert oder ersetzt. Im Einzelnen bestehen insbesondere folgende Maßnahmen:

- Verfahren für regelmäßige Kontrollen/Audits
- Notfalltests (z.B. zum Ausfall von Systemen)

8. Weisungskontrolle / Auftragskontrolle

Die Maßnahmen der Weisungs- bzw. Auftragskontrolle dienen grundsätzlich dazu sicherzustellen, dass sich der Auftragsverarbeiter bei der Erbringung seiner Dienstleistung an die Weisungen des Verantwortlichen hält, aber auch dazu die Tätigkeit der eingesetzten Unterauftragsverarbeiter regelmäßig zu überprüfen und sicherzustellen, dass diese die personenbezogenen Daten nur nach den gegebenen Weisungen verarbeiten. Derzeit werden die in Anlage 1 genannten Unterauftragsverarbeiter

eingesetzt. Die eigenen Mitarbeiter hat der Auftragsverarbeiter auf die Vertraulichkeit verpflichtet und sensibilisiert.

Sonstiges

Sowohl die DeepL SE als auch die von der DeepL SE genutzten Rechenzentren verfügen über ein zertifiziertes Informations-Sicherheits-Managementsystem gemäß ISO/IEC 27001.