

Vertrag zur Auftragsverarbeitung zwischen

Kunde

– nachfolgend Verantwortlicher genannt –

und

Cornelsen Verlag GmbH

Mecklenburgische Straße 53

14197 Berlin

– nachfolgend Auftragsverarbeiter genannt –

§ 1 Gegenstand und Dauer des Auftrags

- (1) Diese Vereinbarung formuliert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien im Rahmen der Nutzung der Onlinewörterbücher und KI-gestützter Textkorrektur auf www.duden.de, mentor.duden.de, api.duden.de und schulwörterbuch.duden.de. Sie findet Anwendung auf alle Tätigkeiten, die mit der Nutzung dieser Services in Zusammenhang stehen und bei denen der Auftragsverarbeiter oder durch den Auftragsverarbeiter beauftragte Dritte mit personenbezogenen Daten des Verantwortlichen in Berührung kommen können.
- (2) Der Auftragsverarbeiter führt die im Anhang 1 beschriebenen Dienstleistungen für den Verantwortlichen durch. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen werden dort beschrieben.
- (3) Dieser Vertrag wird mit Zustimmung des Verantwortlichen zu den Allgemeinen Geschäftsbedingungen (AGB) des Auftragsverarbeiters wirksam und gilt, solange der Auftragsverarbeiter für den Verantwortlichen personenbezogene Daten verarbeitet.

§ 2 Weisungen des Verantwortlichen

- (1) Der Verantwortliche ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.
- (2) Der Auftragsverarbeiter verarbeitet die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen des Verantwortlichen und im Rahmen der getroffenen Vereinbarungen. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn der Verantwortliche dies anweist.
- (3) Die Verarbeitung erfolgt nur auf Weisung des Verantwortlichen, es sei denn, der Auftragsverarbeiter ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

- (4) Grundsätzlich können Weisungen mündlich erteilt werden. Mündliche Weisungen sind anschließend von dem Verantwortlichen zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn der Auftragsverarbeiter dies verlangt.
- (5) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Vorschriften verstößt, hat sie den Verantwortlichen unverzüglich darauf hinzuweisen.

§ 3 Technische und organisatorische Maßnahmen

- (1) Der Auftragsverarbeiter verpflichtet sich, für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen zu treffen und im Anhang 3 dieses Vertrages zu dokumentieren. Die Sicherheitsmaßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
- (2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. Der Auftragsverarbeiter darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss der Auftragsverarbeiter dem Verantwortlichen nur wesentliche Anpassungen mitteilen.
- (3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung aller gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. Der Auftragsverarbeiter hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten des Verantwortlichen mitzuwirken. Der Auftragsverarbeiter wirkt bei der Erstellung einer Datenschutz-Folgenabschätzung und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden mit. Er hat dem Verantwortlichen alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen.

§ 4 Pflichten des Auftragsverarbeiters

- (1) Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.
- (2) Der Auftragsverarbeiter bietet hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Rechten der betroffenen Person steht.
- (3) Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.
- (4) Der Auftragsverarbeiter darf im Rahmen der Auftragsverarbeitung nur dann auf personenbezogene Daten des Verantwortlichen zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.
- (5) Soweit gesetzlich vorgeschrieben, bestellt der Auftragsverarbeiter einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden dem Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt.

- (6) Der Auftragsverarbeiter darf die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.
- (7) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seine bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann, z.B. die Information und Auskunft an die betroffene Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. Der Auftragsverarbeiter benennt einen Ansprechpartner, der den Verantwortlichen bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsverarbeitung entstehen, unterstützt und teilt dem Verantwortlichen dessen Kontaktdaten unverzüglich mit. Soweit der Verantwortliche besonderen gesetzlichen Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten unterliegt, unterstützt der Auftragsverarbeiter den Verantwortlichen hierbei. Auskünfte an die betroffene Person oder Dritte darf der Auftragsverarbeiter nur nach vorheriger Weisung des Verantwortlichen erteilen. Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber dem Auftragsverarbeiter geltend macht, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

§ 5 Berechtigung zur Begründung von Unterauftragsverhältnissen

- (1) Der Auftragsverarbeiter darf Unterauftragnehmer nur beauftragen, wenn er den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informiert, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Einspruch darf nur aus wichtigem Grund erfolgen.
- (2) Ein Unterauftragsverhältnis liegt insbesondere vor, wenn der Auftragsverarbeiter weitere Auftragnehmer in Teilen oder im Ganzen mit Leistungen beauftragt, auf die sich dieser Vertrag bezieht. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen oder Reinigungskräfte. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten den Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
- (3) Ein Zugriff auf Daten darf durch den Unterauftragnehmer erst dann erfolgen, wenn der Auftragsverarbeiter durch einen schriftlichen Vertrag sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den Unterauftragnehmern gelten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den datenschutzrechtlichen Vorschriften erfolgt. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer sicher, dass Maßnahmen zur Herstellung eines angemessenen Schutzniveaus gemäß Art. 45 ff. DSGVO (z.B. Standarddatenschutzklauseln, Genehmigte Zertifizierungsmechanismus, Angemessenheitsbeschluss der Kommission) vorliegen.
- (4) Die Inanspruchnahme der in Anhang 2 zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragnehmer gilt als genehmigt, sofern die in § 5 Abs. 3 dieses Vertrages genannten Voraussetzungen umgesetzt werden.

§ 6 Kontrollrechte des Verantwortlichen

Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche oder eine von ihm beauftragte Person berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und Anforderung von relevanten Unterlagen, die Einsichtnahme in die Verarbeitungsprogramme oder durch Zutritt zu den Arbeitsräumen des Auftragsverarbeiters zu den ausgewiesenen Geschäftszeiten nach vorheriger Anmeldung. Durch geeignete und gültige Zertifikate zur IT-Sicherheit (z.B. IT-Grundschutz, ISO 27001) kann auch der Nachweis einer ordnungsgemäßen Verarbeitung erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht die Pflicht des Auftragsverarbeiters zur Dokumentation der Sicherheitsmaßnahmen im Sinne des § 3 dieser Vereinbarung.

§ 7 Mitzuteilende Verstöße des Auftragsverarbeiters

Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Verantwortlichen mit sich bringen, sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten des Verantwortlichen. Gleiches gilt, wenn der Auftragsverarbeiter feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. Dem Auftragsverarbeiter ist bekannt, dass der Verantwortliche verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person unverzüglich zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung seiner Meldepflichten unterstützen. Er wird die Verletzungen dem Verantwortlichen unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

- a) eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,
- b) Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,
- c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
- d) eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

§ 8 Beendigung des Auftrags

- (1) Nach Abschluss der Auftragsverarbeitung hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.
- (2) Der Verantwortliche kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragsverarbeiter einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und dem Verantwortlichen aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

§ 9 Regelungen für Berufsgeheimnisträger

Der Auftragsverarbeiter (Dienstleister) wird vom Kunden für die Zurverfügungstellung von Online-Wörterbüchern sowie von KI-gestützter Textkorrektur beauftragt. Er verpflichtet sich gegenüber dem Kunden zur Verschwiegenheit über alle im Rahmen der Vereinbarung bekanntwerdenden Tatsachen

und ist über die strafrechtlichen Folgen gemäß § 203 StGB belehrt. Der Auftragsverarbeiter (Dienstleister) wird nur insoweit Kenntnis von Geheimnissen erlangen, wie es zur Dienstleistung erforderlich ist. Er kann Unterauftragnehmer (Subunternehmer) einsetzen, muss diese jedoch - soweit möglich - schriftlich zur Verschwiegenheit verpflichten und auf Anfrage des Kunden entsprechende Nachweise vorlegen.

§ 10 Schlussbestimmungen

- (1) Sollte das Eigentum des Verantwortlichen bei dem Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Verantwortlichen ausgeschlossen.
- (2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind in Textform abzufassen, dies kann schriftlich oder in einem elektronischen Format erfolgen.
- (3) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

Anhang 1: Auflistung der beauftragten Dienstleistungen und Kontaktdaten des Datenschutzbeauftragten

Gegenstand der Verarbeitung	Bereitstellung und Betrieb von Online-Wörterbüchern, sowie KI-Tools und Textverarbeitungssoftware zur Textkorrektur auf den digitalen Plattformen von duden.de.
Art und Zweck der Verarbeitung; Art der personenbezogenen Daten	<p>Für jeden Nutzer der Plattform wird ein Nutzerprofil eingerichtet, bei dessen Einrichtung die folgenden personenbezogenen Daten/Informationen erfasst werden:</p> <p>Nutzer</p> <p>Name, Vorname, E-Mail-Adresse, Passwort, Unternehmensdaten und Unternehmenszugehörigkeit (im B2B-Bereich)</p> <p>Die E-Mail-Adresse wird zu folgenden Zwecken genutzt:</p> <ul style="list-style-type: none"> • Verifizierung im Anmeldeprozess • Versenden eines Verifizierungslinks, wenn das Passwort vergessen wurde • zum Zwecke der Kommunikation im Rahmen der Nutzung der Plattform <p>Nutzungsdaten</p> <p>Nutzer können Wörterbucheinträge auf personalisierten Merklisten hinterlegen. Die Zuordnung der Wörterbucheinträgen zu Nutzenden erfolgt pseudonymisiert.</p> <p>Die Eingabe der Nutzer werden an eine Software der Auftragnehmerin übergeben, dort anonymisiert, bevor die Eingabe an Textverarbeitungssoftware und ein Sprachmodell übergeben wird, das Antworten/ Ausgaben an den Nutzer zurückliefert. Die Texte werden nach der Prüfung umgehend gelöscht und nicht gespeichert. Eine Einsichtnahme in die Texte bzw. Weiterleitung oder -verarbeitung erfolgt nicht. Das System wird permanent verbessert und das Verhalten analysiert und überwacht.</p> <p>In der kostenlosen Version der KI-gestützten Textkorrektur werden die korrigierten Texte für maximal 14 Tage gespeichert und zu Zwecken der Qualitätssicherung ausgewertet.</p>
Kategorien betroffener Personen	Nutzer

Erster Ansprechpartner für Datenschutzfragen beim Auftragsverarbeiter	Thomas Schiller Datenschutzkoordinator der Cornelsen Gruppe Cornelsen Verlag GmbH, Mecklenburgische Straße 53, 14197 Berlin Tel: +49 30 897 85-8471 E-Mail: datenschutz@cornelsen.de
Name und Kontaktdaten des Datenschutzbeauftragten der Auftragsverarbeiters	datenschutz nord GmbH E-Mail: office@datenschutz-nord.de Telefon: 0421/6966320

Anhang 2: Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

Unterauftragnehmer	Verarbeitungsstandort	Art der Dienstleistung
Amazon Web Services Germany GmbH, Krausenstraße 38, 10117 Berlin	DE (vertraglich festgelegt)	Cloud-Computing für Anwendungen (SaaS), Plattform (PaaS) und Infrastruktur (IaaS)
Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn	DE	Cloud-Computing für Anwendungen (SaaS), Plattform (PaaS) und Infrastruktur (IaaS)
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA	DE (vertraglich festgelegt)	KI-Funktionen

Anhang 3: Technisch-organisatorische Sicherheitsmaßnahmen

I. Pseudonymisierung / Anonymisierung und Verschlüsselung

Personenbezogene Daten werden soweit möglich pseudonymisiert in den IT-Systemen verarbeitet. Kann die Verarbeitung auch anonym erfolgen, wird der Personenbezug aufgelöst. Soweit technisch umsetzbar, wird zusätzlich eine Verschlüsselung für die Übermittlung und Speicherung eingesetzt.

II. Vertraulichkeit

1. Zugangskontrolle

- Maßnahmen zur Absicherung der physischen Räumlichkeiten mit IT-Systemen
 - Zutrittskontrollsystem (inkl. Berechtigungssystem), Ausweisleser, Magnetkarte, Chipkarte
 - Schließsystem / Schlüsselvergabe (Chips) gemäß Rollenkonzept
 - Türsicherung (elektrische Türöffner usw.)
 - Überwachungseinrichtung / Alarmanlage
 - EMA (Einbruchmeldeanlage) für das Rechenzentrum
 - Personenempfang/-Kontrolle am Empfang der Bürogebäude bzw. durch zuständige Mitarbeiter, Tragepflicht von Besucherausweisen
 - Ständige Begleitung Externer/Gäste im Haus, im Rechenzentrum Führung eines Besucherprotokolls
- Maßnahmen zur Verhinderung der unbefugten Nutzung von IT-Systemen (Zugang)
 - Zuordnung von Benutzerrechten
 - Authentifikation mit Benutzername / Passwort
 - Vergabe von Passwörtern gemäß Passwortrichtlinie (Komplexitätsregeln)
 - Einsatz von Firewallsystemen
 - Begrenzung der Anmeldeversuche

2. Datenträgerkontrolle

Implementierte Maßnahmen zur Verhinderung des unbefugten Lesens, Kopierens, Verändern oder Löschens von Datenträgern:

- Nur berechnigte Personen haben Zugang zu Räumen mit Datenträgern. Absicherung gemäß Beschreibung unter Punkt 1
- Sichere Aufbewahrung von Datenträgern (abgeschottete Bereiche, gesicherte Ablage)
- Definierter Prozess zur Vernichtung/Entsorgung von Datenträgern gemäß Datenschutzbestimmungen
- Vermeidung der Nutzung von Datenträgern soweit möglich – Datenaustausch überwiegend über WAN / LAN
- Mobile Geräte (Notebooks, Handy, Tablet) sind verschlüsselt und mit Passwörtern / bzw. PIN gesichert
- Anweisung zur zentralen Datenhaltung auf File-Server / keine lokale Speicherung von Daten auf mobilen Geräten (Notebooks, Handy, Tablet).

3. Speicherkontrolle

Eingeführte Maßnahmen zur Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderungen und Löschung von personenbezogenen Daten:

- Differenzierte Berechtigungskonzepte für den Zugriff auf IT-Systeme
- Berechtigungsvergabe/-Anforderungen nur durch Befugte (IT-Prozess)
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei Eingabe, Änderung und Löschung von Daten
- Administratorrechte beschränkt auf das Notwendigste
- Einsatz von Aktenvernichtern und Sammelbehältern zur Vernichtung von papierhaften Unterlagen mit personenbezogenen Daten

4. Benutzerkontrolle

Maßnahmen zur Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte:

- Externer Datenaustausch wird über abgesicherte Leitungen (MPLS-WAN / VPN) durchgeführt
- Authentifikation mit Benutzername / Passwort
- Vergabe von Passwörtern gemäß Passwortrichtlinie (Komplexitätsregeln)
- Führung eines Verzeichnisses von Verarbeitungstätigkeiten mit Übersicht aller Empfänger, gegenüber denen personenbezogene Daten offengelegt werden
- Absicherung der Zugänge (u. a. VPN, WLAN, FTP-Server) und Nutzung nur durch berechtigte Personen
- Sensibilisierung der Mitarbeiter durch Schulungen und Gefährdungsanalysen

5. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben:

- Differenzierte Berechtigungskonzepte für den Zugriff auf IT-Systeme
- Berechtigungsvergabe/-Anforderungen nur durch Befugte (IT-Prozess)
- Administratorrechte beschränkt auf das Notwendigste
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- ausschließliche Verwendung individualisierter Accounts

6. Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können:

- Trennung von Produktiv- Support- und Testsystemen
- Logische Mandantentrennung
- Getrennte Speicherung auf gesonderten Systemen (bzw. Datenträgern)
- Speicherung in unterschiedlichen Tabellen gem. ERM bei Datenbankgestützten Systemen
- Festlegung von Datenbankrechten

- Anwendung dezidierter Berechtigungskonzepte

7. Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur durch entsprechende Weisungen des Auftraggebers verarbeitet werden können:

- Schriftliche Weisungen an den Auftragnehmer in Form eines AV-Vertrags (Auftragsverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter auf die Vertraulichkeit gem. DSGVO
- Kontrolle der Benennung eines Datenschutzbeauftragten durch den Auftragnehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer
- Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

III. Integrität

1. Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können:

- Regelmäßige Updates der IT-Komponenten und Systeme
- Entwicklungs- / Testsysteme und Supportsysteme getrennt von Produktivsystemen
- Nur Einsatz getesteter und abgenommener Software gemäß Change-Prozess
- Monitoring der IT-Systeme
- Nutzung von transaktionsbasierten Verarbeitungen und Safe Points soweit möglich
- Redundante Speicherung soweit möglich (Serversysteme), zeitnahe Backups und Archivierungen
- Zeitnahe Löschung von veralteten Daten um Inkonsistenzen zu vermeiden

2. Übertragungskontrolle

Maßnahmen zur Gewährleistung der Überprüfung und Feststellung, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden:

- Datenaustausch wird über abgesicherte Leitungen (MPLS-WAN / VPN) durchgeführt
- Führung einer Übersicht über alle Datenübermittlungen an Dritte
- Protokollierung sämtlicher Datenübertragungen mit allen Details
- Datenübertragungen nur über gesicherte und explizit dafür vorgesehene Transportwege (VPN, FTP-Server, etc.)

3. Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten nur auf Grund von Berechtigungsanforderungen gemäß IT-Prozess und auf Basis der Berechtigungskonzepte

- Nachvollziehbarkeit

4. Transportkontrolle

Maßnahmen zur Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

- Datenaustausch wird über dedizierte Leitungen durchgeführt
- Führung einer Übersicht über alle Datenübermittlungen an Dritte
- Beim physischen Transport geeignete Transportbehälter und Versandwege, Nutzung verschlüsselter Datenträger
- Datenübertragungen nur über gesicherte und explizit dafür vorgesehene Transportwege (VPN, FTP-Server, etc.)

IV. Verfügbarkeit und Belastbarkeit

1. Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind:

- Backup-Verfahren gemäß Datensicherungskonzept inkl. Recoverytests
- Räumlich getrennte Aufbewahrung von Sicherungsduplikaten
- Hochverfügbarkeitskonzept beim Server- und Storagebetrieb
- Notfallpläne zur Wiederherstellung der Systeme und Daten
- Absicherung des RZ gemäß Sicherheitsrichtlinie und bauliche Maßnahmen
 - Unterteilung in verschiedene geschlossene Brandabschnitte
 - USV und Notstromerzeugung
 - Klimakontrolle und Brandfrüherkennung mit automatischer Löschanlage
 - Mehrfache Anbindung (WAN)
 - Einbruchmeldeanlage
- Anweisung zur zentralen Datenhaltung auf File-Server / keine lokale Speicherung von Daten auf mobilen Geräten (Notebooks, Handy, Tablet, ...).

2. Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

- Monitoring aller Systeme, Anwendungen und Datenbanken sowie der dazu gehörigen Infrastruktur
- Historische Aufzeichnung von Messpunkten und grafisches Reporting in Messkurven
- Alarmierungen im Störfall
- 24/7-IT-Betrieb mit Einsatz von Rufbereitschaft
- Präventivmaßnahmen für sicheren und stabilen Betrieb (Security-Maßnahmen gemäß Sicherheitsrichtlinie, regelmäßige Updates der IT-Komponenten)

V. Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können:

- Regelmäßige Durchführung von Datensicherungen gemäß Sicherungskonzept

- Regelmäßige Wiederherstellungstests (Rücksicherungen)
- Duplizierung von Sicherungen und Lagerung außerhalb des RZ
- Dokumentationen zum Recovery von Systemen und dem Wiederanlauf von Systemen
- Notfallpläne für Störungsfälle
- Regelmäßige Durchführung von Übungen zum Recovery von Systemen
- Langzeitarchivierung/-recherche von Daten/Dokumenten gemäß der gesetzlichen Bestimmungen und den definierten Löschrufen

VI. Überprüfung und Wirksamkeit

1. Systemlandschaft

Es erfolgt eine regelmäßige Überprüfung und Analyse bzw. die Anpassung der Systeme an den Geschäftsbetrieb. Eingesetzte Software wird mit Updates aktuell gehalten und neue Programmversionen zeitnah eingesetzt.

Neue Software wird neben der fachlichen Nutzung / Einsatzfähigkeit auch auf Wirksamkeit hinsichtlich Datenschutz und Datensicherheit bewertet.

Erkenntnisse über Schwachstellen bei Hard- und Software werden mit der eigenen Systemlandschaft abgeglichen und Maßnahmen zur Beseitigung oder Risikominimierung – bis zur Beseitigung umgesetzt.

Die eingesetzte Hardware wird durch Service- und Wartungsverträge abgesichert. Der Austausch von Hardware erfolgt regelmäßig hinsichtlich der zu erwartenden Einsatzdauer oder Instandsetzbarkeit / Ersatzteilbeschaffung.

2. Mitarbeiter

Durch regelmäßige Schulungen werden unsere Mitarbeiter sensibilisiert. Über benannte Kontakte (Datenschutzbeauftragter, Administratoren, Vorgesetzte) werden Rückmeldungen zu Abläufen und Maßnahmen gegeben bzw. Gefahren aufgezeigt.

3. Neue Prozesse / Prozessänderungen

Ein Change-Prozess ermöglicht - neben der fachlichen Beurteilung - auch die Bewertung der notwendigen Anpassungen und Erweiterungen der bestehenden Maßnahmen. Zur Absicherung der geplanten Verarbeitung und der Einbindung in das Sicherheitskonzept werden diese stetig weiterentwickelt.