Online-Variante

Vereinbarung zur Verarbeitung von Daten im Auftrag

zwischen

Kunden der Datenschutzakademie, die Verantwortliche nach Art. 4 Nr. 7 DSGVO sind
gem. Auftragsbestätigung / Vertrag
– Verantwortlicher –
- nachfolgend Auftraggeber genannt -

und

Datenschutzberatung Moers GmbH
Neue Straße 22
34369 Hofgeismar
– Auftragsverarbeiter –
- nachfolgend Auftragnehmer genannt -

§ 1 Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrags ist die Bereitstellung von Datenschutz-Schulungen via e-Learning für Mitarbeiter des Auftraggebers sowie die Durchführung der damit verbundenen Verwaltungs- und Dokumentationstätigkeiten.

(2) Die Laufzeit dieses Auftrags beginnt mit dem Zeitpunkt des Beginns der Verarbeitung und endet mit Beendigung des Vertrags.
Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 2 Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten sind die Bereitstellung einer E-Learning-Plattform zur Schulung von Mitarbeitern im Bereich Datenschutz.

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

(2) Gegenstand der Verarbeitung personenbezogener Daten können folgende Datenarten/- kategorien sein: Name, Kontaktdaten, Authentifizierungsdaten, IT-Nutzungsdaten, Qualifikationsdaten, Schulungsergebnisse.

(3) Die Kategorien der durch die Verarbeitung betroffenen Personen können umfassen: Mitarbeiter, Auszubildende, Praktikanten, Rentner, ehemalige Mitarbeiter.

§ 3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

(3) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

(4) Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(5) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erfolgen.

(6) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

(7) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 4 Technisch-organisatorische Maßnahmen

(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 dokumentierten 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 [Einzelheiten in Anlage 1].

(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.

(4) Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO).

§ 5 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

§ 6 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); 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 (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

(2) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Eine physische Trennung ist nicht zwingend erforderlich.

(3) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 34 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.

b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem

Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 3 dieses Vertrages.

(4) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DS-GVO).

§ 7 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung durchführen.

§ 8 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unten der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
teamnext GmbH & Co. KG	Humboldtstr. 4, 34117 Kassel, Deutschland	Hosting Software in einem externen Rechenzentrum
STRATO AG	Pascalstr. 10, 10587 Berlin, Deutschland	Domain Hosting

Die weitere Auslagerung auf Unterauftragnehmer sowie der Wechsel von bestehenden Unterauftragnehmern ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

Sämtliche vertragliche Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

§ 9 Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgeabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§ 10 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 11 Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Technische und organisatorische Maßnahmen

Datenschutzberatung Moers GmbH
Neue Straße 22
34369 Hofgeismar

Als nicht-öffentliche Stelle, die personenbezogene Daten erhebt, verarbeitet oder nutzt, müssen wir technische und organisatorische Maßnahmen treffen, die erforderlich sind, um die Ausführung der Datenschutzvorschriften zu gewährleisten. Insbesondere sind Vertraulichkeit, Integrität, Verfügbarkeit und Systembelastbarkeit im Zusammenhang mit der Datenverarbeitung sicherzustellen. Die nachstehenden technischen und organisatorischen Maßnahmen sind dazu in unserem Unternehmen umgesetzt.

Hinsichtlich der Sicherheitsmaßnahmen im Rechenzentrum wird auf das Sicherheitskonzept des Unterauftragsverarbeiters verwiesen. Dieser gibt an: „Für seine Rechenzentren hat STRATO durchgängig seit 2004 die TÜV-Zertifizierung nach ISO 27001. Die DIN ISO/IEC 27001 (kurz ISO 27001) ist international die bekannteste Norm zum IT-Sicherheitsmanagement. Sie legt die Anforderungen an ein System zum IT-Sicherheitsmanagement fest. Ziel der Normumsetzung ist der Nachweis, dass adäquate und angemessene Sicherheitsmaßnahmen gewählt werden, die Informationswerte schützen und Vertrauen bei Interessenten wecken. ISO 27001 gilt für die Entwicklung und den Betrieb von Internetprodukten und Internetdienstleistungen sowie der dazugehörigen Rechenzentren. Die Zertifizierung umfasst ein systematisches Sicherheitskonzept sowie zahlreiche Sicherheitsmaßnahmen in der IT-Infrastruktur selbst, in der Sekundärtechnik und in der Prozesskette. Das Sicherheitskonzept orientiert sich an festgelegten Standards und wird regelmäßig überprüft. Zu unseren Sicherheitsmaßnahmen gehören Datenspiegelung zwischen beiden Rechenzentren, batteriegestützte unterbrechungsfreie Stromversorgung, Notstromdiesel für bis zu vier Wochen durchgängig autonomen Betrieb, Laser-Feuermelder und Löschgas, Zutritts- und Zugangsregeln, Verpflichtungen und Schulungen der Mitarbeiter sowie regelmäßige Analysen neuer Sicherheitsanforderungen.“[1]

1. Vertraulichkeit

Zutrittskontrolle/Gebäudeabsicherung

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B. Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.

- Chipkarten-/Transponder-Schließsystem
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sicherheitsschlösser
- Personenkontrolle beim Pförtner / Empfang
- Sorgfältige Auswahl von Reinigungspersonal

[1] Quelle: https://www.strato.de/faq/vertrag/fragen-zur-auftragsverarbeitungsvertrag-avv-und-der-neuen-eu-datenschutzgrundverordnung-dsgvo/#tuev-zertifizierung, abgerufen am 14.10.2019.

Zugangskontrolle/Absicherung Systemzugang

Keine unbefugte Systembenutzung, z.B. (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

- Zuordnung von Benutzerrechten
- Einsatz von individuellen Benutzernamen
- Vorgaben für sichere Passwörter
- Authentifikation mit Benutzername/ Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie (Fernzugriff)
- Gehäuseverriegelungen am Server
- Einsatz von Intrusion-Detection-Systemen
- Verschlüsselung von mobilen Datenträgern
- Einsatz von zentraler Smartphone-Administrations-Software (z. B. zum Fern-Löschen)
- Verschlüsselung von Smartphone-Inhalten
- Verschlüsselung von Datenträgern in Laptops
- Sichere Passwörter für Smartphones

Zugriffskontrolle/Sicherstellung von Zugriffsberechtigungen

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das Notwendigste reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Ordnungsgemäße Vernichtung von Papier (Einsatz von Aktenvernichtern)
- Physische Löschung von Datenträgern vor Wiederverwendung
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Protokollierung der Vernichtung
- Verschlüsselung von Datenträgern
- Einsatz von Anti-Viren-Software
- Einsatz einer Software-Firewall
- Einsatz einer Hardware-Firewall

Trennungskontrolle/Maßnahmen zur Zwecktrennung von Daten

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing, physikalisch oder virtuell getrennte Systeme.

- Logische Mandantentrennung (softwareseitig)

- Erstellung eines Berechtigungskonzepts
- Trennung von Produktiv- und Testsystem
- Keine Produktivdaten in Testsystemen

Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt 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.

- Verarbeitung von Daten in pseudonymisierter (oder anonymisierter) Form

2. Integrität

Weitergabekontrolle/Sicherheit beim Datentransfer

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- E-Mail-Verschlüsselung
- Beim physischen Transport: sichere Transportbehälter/-verpackungen
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen
- Verschlüsselung externer Datenträger bei Weitergabe (CDs, USB-Sticks etc.)
- Verschlüsselte Datenübermittlung (z.B. via https / FTPS/ TLS)

Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B. Protokollierung, Dokumentenmanagement:

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Protokollierung der Eingabe, Änderung und Löschung von Daten

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle/Schutz von Daten vor zufälliger Zerstörung und Verlust

- Unterbrechungsfreie Stromversorgung (USV)
- Schutzsteckdosenleisten in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Backup- und Recoverykonzepts
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Erstellen eines Notfallplans
- Serverräume nicht unter sanitären Anlagen
- Regelmäßige Sicherung von Systemzuständen
- Regelmäßige Sicherung von Dateibeständen
- Regelmäßige Sicherung von Datenbanken

Rasche Wiederherstellbarkeit

- Wiederherstellung nach Backup- und Recoverykonzept
- Kontrolle des Notfallplans
- Testen von Datenwiederherstellung

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management

- Die Grundsätze in Datenschutz (Erhebung, Verarbeitung oder Nutzung personenbezogener Daten) sind einer unternehmensinternen Richtlinie festgelegt.
- Es ist ein Datenschutzbeauftragter schriftlich benannt.
- Der DSB ist bei der Datenschutzfolgeabschätzung eingebunden.
- Der DSB ist im Organigramm eingebunden.
- Schulung von Mitarbeitern.
- Verpflichtung der Mitarbeiter auf datenschutzkonformen Umgang mit personenbezogenen Daten.
- Verpflichtung der Mitarbeiter auf das Fernmeldegeheimnis.
- Die interne Verarbeitungsübersicht der Verarbeitungsprozesse ist vorhanden.

Störungsfallmanagement

Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT-Bereichen sowie hierzu vorbereitende Maßnahmen und Prozesse.

- Erstellung eines Plans zum Umgang mit Störfällen
- Sicherheitsteam ist benannt

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

- Beachtung privacy by Design/Datenschutz durch Technikgestaltung
- Beachtung privacy by Default/Datenschutz durch datenschutzfreundliche Voreinstellungen

- Auswahl datenschutzfreundlicher Technologie bei der Beschaffung

Auftragskontrolle/Einbindung von Unter-Auftragsverarbeitern

Keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Auftraggebers, z.B. Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

- Auswahl der (Unter-)Auftragsverarbeiter unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Vorherige Prüfung und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
- Schriftlich dokumentierte Weisungen an den Auftragsverarbeiter (z. B. durch Auftragsdatenverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf Vertraulichkeit
- Auftragsverarbeiter hat Datenschutzbeauftragten bestellt (wenn erforderlich)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart
- Laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten