AV-Vertrag, Art. 28 DSGVO

SeeYourData, dasRecht.de UG (haftungsbeschränkt)
Sillemstr. 68, 20257 Hamburg

VERTRAGSGEGENSTAND

Im Rahmen der Leistungserbringung nach dem Vertrag zur Nutzung des Webdienstes zur Führung des Verzeichnisses von Verarbeitungstätigkeiten (Hauptverstrag) ist es erforderlich, dass der Auftragnehmer als Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DSGVO mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO fungiert (nachfolgend Auftraggeber-Daten genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

ART UND ZWECK, DAUER DER AUFTRAGSVERARBEITUNG

1. Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nur nach Weisung des Auftraggebers. Der Auftraggeber bleibt gemäß Art. 5 Abs. 2 DSGVO im datenschutzrechtlichen Sinn Verantwortlicher (Herr der Daten).

2. Die Verarbeitung der Auftraggeber-Daten im Rahmen der Auftragsverarbeitung erfolgt entsprechend den in **Anlage 2** zu diesem Vertrag enthaltenen Festlegungen zu Art und Zweck der Verarbeitung. Sie bezieht sich auf die in **Anlage 2** festgelegte Art der Auftraggeber-Daten und auf die dort bestimmten Kategorien betroffener Personen.

   Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union (EU) statt. Jede Verlagerung in ein Land außerhalb der EU (Drittland) darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

3. Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

WEISUNGSRECHTE DES AUFTRAGGEBERS

1. Der Auftragnehmer verwendet die Auftraggeber-Daten ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers, wie sie abschließend in den Bestimmungen dieses Vertrags Ausdruck finden. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des im Hauptvertrag festgelegten Änderungsverfahrens.

2. Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt, wird er den

Auftraggeber möglichst zeitnah darauf hinweisen. Außerdem ist der Auftragnehmer berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen.

3. Soweit der Auftragnehmer durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist, die personenbezogenen Daten auch ohne Weisung des Auftraggebers zu verarbeiten, teilt der Auftragnehmer dem Auftraggeber die entsprechenden rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4. Weisungen des Auftraggebers sind mindestens in Textform (z. B. E-Mail) zu erteilen. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich mindestens in Textform (z. B. E-Mail).

5. Sofern gegen den Auftragnehmer wegen eines Verstoßes gegen die DSGVO Ansprüche auf Zahlung von Schadenersatz gemäß Art. 82 DSGVO geltend gemacht werden, ohne dass der Auftragnehmer gegen eine vom Auftraggeber erlassene Weisung verstoßen hat, stellt der Auftraggeber den Auftragnehmer auf erstes Anfordern von allen Ansprüchen frei. Der Auftraggeber übernimmt hierbei auch die Kosten der notwendigen Rechtsverteidigung des Auftragnehmers einschließlich sämtlicher Gerichts- und Anwaltskosten. Die Freistellungspflicht gilt nicht, soweit eine Weisung rechtswidrig und dies für den Auftragnehmer offensichtlich war oder der Schadenersatzanspruch auf die Verletzung einer speziell den Auftragsverarbeitern auferlegten Pflicht aus der DSGVO gestützt wird.

PFLICHTEN DES AUFTRAGGEBERS

1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

2. Der Auftraggeber ist Eigentümer der Auftraggeber-Daten und Inhaber aller etwaigen Rechte, die die Auftraggeber-Daten betreffen.

3. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4. Soweit sich der Auftragnehmer gegen einen Anspruch auf Schadenersatz nach Art. 82 DSGVO, gegen ein drohendes oder bereits verhängtes Bußgeld nach Art. 83 DSGVO oder sonstige Sanktionen im Sinne des Art. 84 DSGVO mit rechtlichen Mitteln verteidigen will, erlaubt der Auftraggeber dem Auftragnehmer Details der Auftragsverarbeitung inklusive erlassener Weisungen zum Zweck der Verteidigung offenzulegen.

5. Der Auftraggeber unterstützt den Auftragnehmer bei Kontrollen durch eine Aufsichtsbehörde, bei Ordnungswidrigkeits- oder Strafverfahren, bei der Geltendmachung eines Haftungsanspruchs einer betroffenen Person oder eines Dritten oder bei der Geltendmachung eines anderen Anspruchs im Rahmen des Zumutbaren und Erforderlichen, soweit ein Zusammenhang mit dieser Auftragsverarbeitung besteht.

PFLICHTEN DES AUFTRAGNEHMERS

1. Der Auftragnehmer darf ohne vorherige Zustimmung durch den Auftraggeber im Rahmen der Auftragsverarbeitung keine Kopien oder Duplikate der Auftraggeber-Daten anfertigen.

   Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem Hauptvertrag (einschließlich der Datensicherung) erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

2. Der Auftragnehmer unterstützt den Auftraggeber bei Kontrollen durch die Aufsichtsbehörde, bei Ordnungswidrigkeits- oder Strafverfahren, bei der Geltendmachung eines Haftungsanspruchs einer betroffenen Person oder eines Dritten oder bei der Geltendmachung eines anderen Anspruchs im Rahmen des Zumutbaren und Erforderlichen, soweit ein Zusammenhang mit dieser Auftragsverarbeitung besteht.
3. Der Auftragnehmer hat die bei der Verarbeitung von Auftraggeber-Daten beschäftigten Personen gemäß Art. 28 Abs. Satz 2 lit. b) DSGVO schriftlich auf die Vertraulichkeit zu verpflichten und sie zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut zu machen. Dies ist nicht erforderlich, wenn die bei der Verarbeitung von Auftraggeber-Daten beschäftigten Personen bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
4. Sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind, ist der Auftragnehmer verpflichtet, einen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis fachkundigen, für die Aufgaben nach Art. 39 DSGVO fähigen und zuverlässigen betrieblichen Datenschutzbeauftragten schriftlich zu bestellen, der seine Tätigkeit gemäß Art. 38, 39 DSGVO und § 38 Abs. 2 BDSG ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mindestens in Textform (z. B. E-Mail) mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt. Sollte keine Bestellpflicht für einen betrieblichen Datenschutzbeauftragten bestehen, benennt der Auftragnehmer gegenüber dem Auftraggeber mindestens in Textform (z. B. E-Mail) einen Ansprechpartner für datenschutzrechtliche Belange und teilt dem Auftraggeber dessen Kontaktdaten mit. Sollte der Auftragnehmer seinen Sitz außerhalb der EU haben, benennt er gegenüber dem Auftraggeber einen Vertreter nach Art. 27 Abs. 1 DSGVO in der EU und teilt dem Auftraggeber dessen Kontaktdaten
5. Der Auftragnehmer unterliegt der behördlichen Aufsicht nach § 40 BDSG sowie den Bußgeld- und Strafvorschriften in § 42, 43 BDSG sowie in Art. 83 Abs. 4-6 DSGVO nach Maßgabe von § 41 BDSG.
6. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der nach **Anlage 1** zu treffenden technischen und organisatorischen Maßnahmen im Rahmen der Kontrollrechte nach Ziffer 8 dieses Vertrages nachzuweisen.

TOM

1. Der Auftragnehmer hat vor Beginn der Verarbeitung der Auftraggeber-Daten die in **Anlage 1** dieses Vertrags aufgelisteten technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 Satz 2 lit. c), Art. 32 DSGVO zu implementieren und während des Vertrags aufrechtzuerhalten.

Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, 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 unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

2. Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der technologischen Weiterentwicklung unterliegen, ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der in **Anlage 1** festgelegten Maßnahmen nicht unterschritten wird.

   Der Auftragnehmer wird solche Änderungen dokumentieren. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers und sind vom Auftragnehmer zu dokumentieren und dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

UNTERSTÜTZUNG

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen. Hierzu gehören

1. 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,
2. die Unterstützung des Auftraggebers im Falle einer Verletzung des Schutzes personenbezogener Daten nach Art. 33 DSGVO,
3. die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht nach Art. 34 DSGVO gegenüber einem Betroffenen zu unterstützen,
4. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzungen i. S. d. Art. 35 DSGVO,
5. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde nach Art. 36 DSGVO.

Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des Hauptvertrages enthalten oder auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

KONTROLLRECHTE DES AUFTRAGGEBERS

1. Der Auftraggeber ist berechtigt, im Rahmen der üblichen Geschäftszeiten auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers, in denen Auftraggeber-Daten verarbeitet werden, zu betreten, um sich von der Einhaltung

der aus dieser Vereinbarung ergebenden Pflichten, insbesondere der technischen und organisatorischen Maßnahmen gemäß **Anlage 1** zu diesem Vertrag, zu überzeugen. Der Auftragnehmer weist dem Auftraggeber auf Anforderung die Umsetzung der technischen und organisatorischen Maßnahmen nach.

2. Der Auftragnehmer gewährt dem Auftraggeber die zur Durchführung der Kontrollen nach Ziffer 8.1 erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.

3. Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Auftraggebers, weitere Kontrollen im Fall von besonderen Vorkommnissen durchzuführen.

4. Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 8 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen.

5. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 1** anstatt einer Vor-Ort-Kontrolle auch durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren nach Art. 42 DSGVO, die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit z. B. nach BSI-Grundschutz (Prüfungsberichts) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 1** zu diesem Vertrag zu überzeugen.

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

UNTERAUFTRAGSVERHÄLTNISSE

1. Der Auftragnehmer darf Unterauftragsverhältnisse (Unterauftragnehmer) hinsichtlich der Verarbeitung oder Nutzung von Auftraggeber-Daten begründen.

   Zurzeit sind für den Auftragnehmer die in **Anlage 3** mit Namen, Anschrift und Auftragsinhalt bezeichneten Unterauftragnehmer beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragnehmers.

   Sofern der Auftraggeber keine Einwände gegen neue Unterauftragnehmer innerhalb von 2 Wochen ab Zugang der Mitteilung über den neuen Unterauftragnehmer erhebt, gilt dessen Einschaltung als durch den Auftraggeber genehmigt.

2. Nicht als Unterauftragsverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der

Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

3. Die Verpflichtung des Unterauftragnehmers muss schriftlich erfolgen, was auch in einem elektronischen Format erfolgen kann (z. B. E-Mail). Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer stellt bei jeder Unterbeauftragung sicher, dass die in Art. 28 Abs. 2 und Abs. 4 DSGVO genannten Bedingungen eingehalten werden.

4. Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Der Auftragnehmer stellt bei jeder Unterbeauftragung sicher, dass die in Art. 28 Abs. 2 und Abs. 4 DSGVO genannten Bedingungen eingehalten werden.

   Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, von dem Auftragnehmer Auskunft über den datenschutzwesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

5. Die Regelungen zu Unterauftragsverhältnissen gelten auch, wenn ein Unterauftragnehmer in einem Drittstaat eingeschaltet wird. Der Auftragnehmer stellt in einem solchen Fall die datenschutzrechtliche Zulässigkeit durch geeignete Rechtsinstrumente, beispielsweise EU-Standardvertragsklauseln, sicher.

6. Die Weitergabe von Auftraggeber-Daten an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

RECHTE DER BETROFFENEN

1. Die Rechte der durch die Datenverarbeitung betroffenen Personen nach Kapitel 3 DSGVO (Art. 12-23 DSGVO) unter Berücksichtigung von Teil 2, Kapitel 2 BDSG (§§ 32-37 BDSG), insbesondere auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch der gespeicherten Auftraggeber-Daten, sind gegenüber dem Auftraggeber geltend zu machen.

2. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks der unter Unterziffer 1 dieses Absatzes aufgeführten Rechte wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

3. Für den Fall, dass eine betroffene Person ihre Rechte im Sinne von Ziffer 1 dieses Absatzes geltend macht, hat der Auftragnehmer den Auftraggeber bei der Erfüllung dieser Ansprüche angesichts der Art der Verarbeitung in angemessenem und für den Auftraggeber erforderlichen Umfang mit geeigneten technischen und organisatorischen Maßnahmen zu unterstützen.

4. Der Auftragnehmer wird es dem Auftraggeber ermöglichen, Auftraggeber-Daten zu berichtigen, zu löschen oder zu sperren oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Löschung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

RÜCKGABE UND LÖSCHUNG ÜBERLASSENER DATEN UND DATENTRÄGER

1. Der Auftragnehmer hat sämtliche Auftraggeber-Daten nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des Hauptvertrags) oder früher nach Aufforderung durch den Auftraggeber datenschutzgerecht zu löschen und von dem Auftraggeber erhaltene Datenträger, die zu diesem Zeitpunkt noch Auftraggeber-Daten enthalten, an den Auftraggeber zurückzugeben. Gleiches gilt für Test- und Ausschussmaterial. Dies gilt nicht, sofern nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.
2. Über eine Löschung bzw. Vernichtung von Auftraggeber-Daten hat der Auftragnehmer ein Protokoll zu erstellen, das dem Auftraggeber auf Anforderung unverzüglich vorzulegen ist.
3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

VERHÄLTNIS ZUM HAUPTVERTRAG

Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

RA Fritz Mehler, dasRecht.de UG (Auftragnehmer)

Auftraggeber

Anlage 1: Technische und organisatorische Maßnahmen

ZUTRITTSKONTROLLE

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

- Besucher/Externe werden begleitet bzw. abgeholt und stets beaufsichtigt.
- Schlüssel

ZUGANGSKONTROLLE

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

- Zugang ist besonders gesichert (Verschlüsselung, VPN)
- Abschottung des Netzwerkes gegen ungewollte Zugriffe von außen (Firewall)
- Zugang zu EDV-Systemen nur mit Benutzerkennung und individuellem Passwort möglich.
- Zugangsberechtigungen werden dokumentiert
- Bildschirmsperre an Arbeitsstationen, automatische Sperrung bei längerer Abwesenheit
- Zwei-Faktor-Identifizierung

ZUGRIFFSKONTROLLE

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

- Individuelle Zugriffsrechte für jeden einzelnen Benutzer (in einem schriftlichen Berechtigungskonzept dokumentiert), zentrale Verwaltung und Steuerung
- Zugriffsberechtigungen werden aufgabenbezogen und nach dem Need-to-know-Prinzip erteilt
- Regelmäßige Überprüfung der Zugriffsberechtigungen. Nicht mehr erforderliche Berechtigungen werden unverzüglich entzogen
- Aufzeichnung von Zugriffen auf das IT-System

WEITERGABEKONTROLLE

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist,

- Übermittlungen personenbezogener Daten sind in Verfahrensübersicht dokumentiert
- Datenspeicherung und -verarbeitung erfolgt auf IT-Systemen im Rechenzentrum. Verbindung zwischen Clients und Server ist besonders gesichert (Verschlüsselung, VPN)
- Mitbringen und verwenden privater Datenträger ist untersagt. Es dürfen nur verschlüsselte betriebliche Datenträger genutzt werden
- Bei Hardwaretausch werden Festplatten vorher ausgebaut

EINGABEKONTROLLE

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

- automatisierte Protokollierung der Dateneingabe, Änderung oder Löschung

AUFTRAGSKONTROLLE

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden können:

- Auftragnehmer werden sorgfältig ausgesucht
- Klare und unzweifelhafte vertragliche Regelungen zur Datenverarbeitung

VERFÜGBARKEITSKONTROLLE

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (die Angaben beziehen sich auf eigene IT-Systeme des Auftragnehmers):

- Versionierte Daten- und Systembackups nach Backup-Plan (täglich/wöchentlich)
- Schadsoftwareschutz. Sicherheitsrelevante Updates und Patches werden regelmäßig und zeitnah eingespielt

TRENNUNGSKONTROLLE / ZWECKBINDUNGSKONTROLLE

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Trennung der Zugriffsregelungen über Datenbankprinzip

Anlage 2 Art und Zweck der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen

Zweck der Datenverarbeitung,
Erfüllung gesetzlicher Pflichten

Art der personenbezogenen Daten,
Namen, Emailadressen, Rechnungsinformationen

Kategorien betroffener Personen,
Beschäftigte

Anlage 3 - Unterauftragnehmer

netcup GmbH
Daimlerstraße 25
D-76185 Karlsruhe