.artfiles

Der folgende ADV-Vertrag ist bereits digital unterzeichnet. Folgende Schritte sind notwendig, damit dieser Vertrag gültig wird:

1. **Vertrag ausdrucken und die Felder mit dem roten „X“ ausfüllen und die Checkboxen entsprechend markieren.**
2. **Unterschriebenen Vertrag im DCP unter „Ihr Account“ -> „ADV-Vertrag“ hochladen.**
3. **Auf Bestätigung von Artfiles warten. Sie erhalten eine Bestätigung an die bei uns hinterlegte E-Mail Adresse (erst dann gilt der Vertrag als gültig).**

Artfiles New Media GmbH
Zirkusweg 1
20359 Hamburg

Tel: +49 (0)40 3202729-0
E-Mail: datenschutz@artfiles.de
Web: https://www.artfiles.de

Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO[1]

Auftraggeber (Verantwortlicher): X

Auftragnehmer (Auftragsverarbeiter): Artfiles New Media GmbH

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

X

- ☐ Webhosting
- ☐ Virtual Server Hosting
- ☐ Videokonferenz-Lösung
- ☐ Domainservice
- ☐ Dedicated Server Hosting
- ☐ Colocation
- ☐ Internet Access

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu 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 (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

[1] diese Vorlage basiert auf der offiziellen Vorlagen des bayerischen Landesamtes für Datenschutz https://www.lda.bayern.de/media/muster_adv.pdf

Dauer des Auftrags

Die Dauer des Auftrags und die genauen Kündigungsmöglichkeiten richten sich nach den Vereinbarungen im Hauptvertrag.

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 das 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 Vestoß dar.

---

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO):

X

☐ Webhosting ☐ Domainservice ☐ Colocation
☐ Virtual Server Hosting ☐ Dedicated Server Hosting ☐ Internet Access
☐ Videokonferenz-Lösung

X

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO):

☐ Stammdaten ☐ Kommunikationsdaten ☐ Programmcode
☐ Zahlungsdaten ☐ Vertragsdaten ☐ Kundenhistorie
☐ Genetische Daten und Krankendaten
☐ Sonstiges Daten:

X

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

☐ Lieferanten ☐ Beschäftigte ☐ Nutzer Videokonferenz
☐ Interessenten ☐ Kunden des Auftraggebers
☐ Sonstiges betroffene Personen:

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

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.

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

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.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und so dann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind:

X

(Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger beim Auftragnehmer sind:

Harald,Oltmanns, Geschäftsführer, 040 / 320 272 90
Tim Evers, Geschäftsführer, 040 / 320 27 90

Für Weisung zu nutzende Kommunikationskanäle:

- per Ticket aus dem Domain Control Panel (DCP)

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. Pflichten des Auftragnehmers

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).

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.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

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). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten.

X

☐ Die in Ziffer 4 genannte weisungsberechtigte Funktion:

☐ An die folgende Person oder Funktion:

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch
Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS- GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb**.**

Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz

Dr. Bahr, Dr. Bahr Consulting GmbH,
Datenschutzbeauftragter, 040/ 555 98 300

---

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

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 gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.
Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Für die auftragsgemäße Verarbeitung personenbezogener Daten wird eine angemessene und nachvollziehbare Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten der von der Verarbeitung Betroffenen berücksichtigt.

Das in Anlage 1 „Technische und organisatorische Maßnahmen nach Art. 32, 24 DSGVO“ beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT- Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maß- nahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen,
datenschutzgerecht zu löschen bzw. vernichten/vernichten zu lassen.

10. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich. Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Datum:

X

Auftraggeber

Auftragnehmer

Anlage 1: Technische und organisatorische Maßnahmen nach Art. 32, 24 DSGVO

.artfiles

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO

der Organisation
Artfiles New Media GmbH
Stand
August 2020

1. Pseudonymisierung

- Autorisierung: Festlegung der Personen, die zur Verwaltung der Pseudonymisierungsverfahren, zur Durchführung der Pseudonymisierung und ggf.
  der Depseudonymisierung berechtigt sind
- Maßnahmen zur Pseudonymisierung bei gegebener Verhältnismäßigkeit und Umsetzbarkeit

2. Verschlüsselung

- Schutz der Schlüssel vor nicht autorisiertem Zugriff oder Nutzung
- zufällige Erzeugung der Schlüssel
- alle Arbeitsstationen sind über eine gesicherte VPN-Verbindung mit dem internen Netz verbunden)
- Übertragung der Daten ausschließlich verschlüsselt
- Verschlüsselung von Datenträgern / Verschlüsselung von Arbeitsplatzrechnern
- Festplatten komplett verschlüsselt
- E-Mail-Kommunikation mit TLS Verschlüsselung
- Verschlüsselung mobiler Geräte und gesonderte Arbeitsanweisung für Umgang mit Datenträgern am Arbeitsplatz (Mobile Device Policy)
- Bereitstellung über verschlüsselte Verbindungen wie SFTP, FTP oder HTTPS

3. Gewährleistung der Vertraulichkeit

3.1. Zutrittskontrolle

- getrennte Sicherheitsbereiche (Rechenzentren/Server getrennt von normalen Büroräumen, separate Räumlichkeiten und gesondert zutrittsgeschützt)
- Richtlinie zur Begleitung von Besuchern in Gebäuden (Besucherüberwachung durch Begleitung von Mitarbeitern, Führen eines Besucherbuchs)
- Alarmanlage in den Rechenzentren und im Büro
- Verwendung von Mitarbeiterausweisen mit Foto
- Verwendung von Sicherheitsschlössern
- Wachdienst außerhalb der Geschäftszeiten
- Klingelanlage mit Kamera
- Videoüberwachung der Eingänge
- Videoüberwachung im Rechenzentrum
- Sorgfalt bei Auswahl der Reinigungsdienste
- Dokumentierter Prozess bei Verlust eines Zugangsmittels
- Rechenzentren werden ausschließlich in Deutschland und mit deutschen Vertragspartnern betrieben
- Zugang zum Rechenzentren nur mit Chipkarte und PIN

3.2. Zugangskontrolle

- Login mit Benutzername + Passwort
- Anti-Viren-Software für Server, Clients und mobile Geräte
- Einsatz von Firewalls
- Intrusion Detection Systeme
- Mobile Device Management (Mobile Device Policy)
- Verschlüsselung von Datenträgern, Smartphones, Notebooks und Arbeitsplatzrechnern
- Einsatz von VPN bei Remote-Zugriffen
- Dokumentierte Richtlinie für Benutzerprofile und Passwörter
- allgemeine Richtlinie zu Datenschutz und Datensicherheit
- Dokumentierte Richtlinie zum „Löschen / Vernichten“ von Daten

3.3. Zugriffskontrolle

- regelmäßige Überprüfung/Aktualisierung der Berechtigungen
- Aktenschredder (mind. Stufe 3, cross cut)
- Physische Löschung von Datenträgern
- Schutz der Rechner durch Sperrbildschirm mit Kennwort
- Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten
- Netzseparierung

3.4. Trennungskontrolle

- Trennung von Produktiv- und Testumgebung
- Mandantenfähigkeit relevanter Anwendungen
- getrennte Speicherung von Firmendaten (Buchhaltung, Personverwaltung etc.)

4. Gewährleistung der Integrität

4.1. Weitergabekontrolle

- alle Mitarbeiter sind vertraglich auf das Datengeheimnis verpflichtet
- mobile Datenträger, sowie die Datenträger von Laptops / Notebooks werden verschlüsselt.
- bei externer Kommunikation werden Verschlüsselungen nach dem Stand der Technik eingesetzt, sofern der Kommunikationspartner dies unterstützt.
- Löschfristen entsprechen den gesetzlichen Vorgaben
- Zugang auf alle internen Dienste erfolgt über VPN
- verschlüsselte Übertragung (SFTP, FTPS, HTTPS)

4.2. Eingabekontrolle

- Protokollierung bei Eingabe, Änderung und Löschung von Daten
- es existieren klare Zuständigkeiten für Löschungen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Regelungen zum Zugriff und zur Löschung der Protokolle
- Protokollierung aller relevanten Nutzeraktivitäten

5. Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme

- Brandschutzeinrichtungen
- Wasserschutzeinrichtungen
- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage
- redundante Stromzuführung, Überspannungsschutz
- Löschanlage
- Ersatz- und Austauschkomponenten in den Rechenzentren vorhanden
- regelmäßige Durchführung von Wiederherstellungsübungen
- Verschlüsselung der Datensicherung
- Serverraumüberwachung (Temperatur, Feuchtigkeit etc.)
- Einsatz von Monitoring-Systemen (im Fehlerfall SMS, E-Mail und Push Service Benachrichtigungen)
- Vertretungsregelungen für abwesende Mitarbeiter
- Rufbereitschaft 24/7 (mit Stellvertreterregelung bei Nichterreichbarkeit)
- Verwendung von RAID Systemen in den Servern
- Intrusion Detection System (DoS/DDoS-Angriffe)
- dokumentierte Beschaffungsstrategie für Soft- und Hardware
- Backup & Recovery-Konzept (ausformuliert), Existenz eines Notfallplans

6. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

- Notfallhandbuch (inkl. Wiederanlaufpläne für Dienste, Netze, Server, RZ-Infrastruktur)
- täglich Backups an einen anderen Standort
- Dokumentierter Prozess für die Wiederherstellung der Daten nach einem Zwischenfall

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

7.1. Datenschutz-Management

- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Berechtigungen (Wiki)
- eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
- mindestens jährliche Sensibilisierung der Mitarbeiter bzgl. Informationssicherheit
- die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
- die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
- formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

7.2. Incident-Response-Management

- dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen (Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen)
- formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

7.3. Datenschutzfreundliche Voreinstellungen

- es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

7.4. Auftragskontrolle (Outsourcing an Dritte)

- Zwischen Auftragnehmer und evtl. Unterauftragnehmer wird bei Bedarf ein ADV-Vertrag geschlossen.
- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation

Es liegen schriftlich vor:

- interne Verhaltensregeln
- Risikoanalyse
- allgemeine Datensicherheitsbeschreibung
- umfassendes Datensicherheitskonzept
- Wiederanlaufkonzept