Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung zwischen

Firmenname, Straße, Hausnummer, PLZ, Ort

- Verantwortlicher - nachstehend Auftraggeber genannt

und der

ITM design GmbH

Hauptstraße 43

48712 Gescher

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Inhalt

Präambel 3
1. Definitionen 3
2. Gegenstand und Dauer des Auftrags 3
3. Konkretisierung des Auftragsinhalts 4
4. Leistungsort 5
5. Verantwortlichkeit 6
6. Technisch-organisatorische Maßnahmen 6
7. Berichtigung, Einschränkung und Löschung von Daten 6
8. Qualitätssicherung und sonstige Pflichten des Auftragnehmers 7
9. Pflichten des Auftraggebers 8
10. Vereinbarung zur Wahrung des Berufsgeheimnisses nach § 203 StGB 8
11. Unterauftragsverhältnisse 9
12. Kontrollrechte des Auftraggebers 10
13. Mitteilung bei Verstößen des Auftragnehmers 11
14. Weisungsbefugnis des Auftraggebers 11
15. Löschung und Rückgabe von personenbezogenen Daten 12
16. Haftung und Schadensersatz 12
17. Informationspflichten, Schriftformklausel, Rechtswahl 13
18. Salvatorische Klausel 13
19. Unterschriften 14
20. Anlagen 14
Anlage 1 – Unterauftragnehmer 15
Anlage 2 – Technisch-Organisatorische Maßnahmen 16

Präambel

Soweit der Auftraggeber den Regelungen des Datenschutzgesetzes der Evangelischen Kirche in Deutschland (DSG-EKD n.F.) oder des kirchlichen Datenschutzgesetzes (KDG) unterliegt, wird in Ergänzung zu den nachfolgenden Regelungen auf der Grundlage der DSGVO und dem BDSG n.F. festgehalten, dass für die Vertragsparteien auch die Bestimmung des DSG-EKD n.F. und des KDG gelten. Das bedeutet u.a., dass sich der Auftragnehmer ggf. auch der Kontroller kirchlicher Datenschutzbeauftragter unterwirft.

1. Definitionen

Es gelten die Begriffsbestimmungen entsprechend Art. 4 DS-GVO, § 2 UWG. Sollten in den Artikeln bzw. Paragraphen sich widersprechende Darstellungen zu finden sein, gelten die Definitionen in der Rangfolge DS-GVO, Landesrecht, UWG. Weiterhin gelten folgende Begriffsbestimmungen:

(1) Anonymisierung: Prozess, bei dem personenbezogene Daten entweder vom für die Verarbeitung der Daten Verantwortlichen allein oder in Zusammenarbeit mit einer anderen Partei unumkehrbar so verändert werden, dass sich die betroffene Person danach weder direkt noch indirekt identifizieren lässt. (Quelle: DIN EN ISO 25237)

(2) Drittland: Ein Land, welches sich außerhalb der EU/EWR befindet.

(3) Unterauftragnehmer: Vom Auftragnehmer beauftragter Leistungserbringer, dessen Dienstleistung und/oder Werk der Auftragnehmer zur Erbringung der in diesem Vertrag beschriebenen Leistungen gegenüber dem Auftraggeber benötigt.

(4) Verarbeitung im Auftrag: Verarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch einen Auftragnehmer im Auftrag des Auftraggebers.

(5) Weisung: Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch einen Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

2. Gegenstand und Dauer des Auftrags

(1) Gegenstand der Vereinbarung ist die Verarbeitung personenbezogener Daten (nachstehend „Daten“ genannt) durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung im Zusammenhang mit einem Dienstleistungsvertrag oder entsprechend jeweiliger Einzelaufträge (im Folgenden Leistungsvereinbarung).

(2) Die Vereinbarung gilt entsprechend für die Administration, für die (Fern-) Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(3) Eine detaillierte Beschreibung des Gegenstandes ergibt sich aus der Leistungsvereinbarung.

(4) Die Laufzeit dieses Vertrages richtet sich nach dem erteilten Auftrag der Datenverarbeitung, sofern sich aus den Bestimmungen dieses Vertrages nicht darüberhinausgehende Verpflichtungen ergeben.

(5) Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen AV-Vertrages z. B. bei Beendigung des vorliegenden Vertragsverhältnisses, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.

3. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten: Der Auftragnehmer führt für den Auftraggeber je nach Vereinbarung folgende Leistungen durch.

- Webprogrammierung
  - Er übernimmt nach Vereinbarung die Wartung der Website / des Webshops / des Portals.
  - Als Administrator legt er im CMS nach Bedarf neue Benutzer an oder nimmt Löschungen vor.
  - Er leistet IT-Support bei Anwendungsproblemen und technischen Störungen.
  - Er meldet die Website des Kunden bei einem Hosting-Anbieter an.
  - Er pflegt Texte des Auftraggebers ein, die ggf. personenbezogene Daten enthalten.
  - Er bindet einen Cookie-Banner ein, um Einwilligungen der Nutzer zu verwalten.
  - Er generiert Rechtstexte (Datenschutzerklärung / Impressum) mit einem Online-Tool.

- Bereitstellung eines Analyse-Tools
  - Er richtet ein Analyse-Tool auf der Website ein.
  - Er erstellt nach Anweisung Analyse-Reports und erhält hierbei Einsicht in die Daten.

- E-Mail-Adressen
  - Für den Kunden werden E-Mail-Adressen und entsprechende Postfächer erstellt und nach Bedarf angepasst.
  - Auf einem E-Mail-Server werden die E-Mail-Postfächer des Kunden gehostet.

- Visitenkartenerstellung / Druckerzeugnisse mit personenbezogenen Daten
  - Er entwirft Visitenkarten oder andere Druckerzeugnisse mit entsprechenden personenbezogenen Daten und leitet die Druckdaten an eine Druckerei weiter.

- E-Mail-Newsletter inkl. Versand
  - Er entwirft und programmiert E-Mail-Newsletter.
  - Er versendet E-Mail-Newsletter an einen vom Kunden bereitgestellten E-Mail-Verteiler.

- Erstellung und Administration eines Social-Media-Kanals
  - Er legt den gewünschten Social-Media-Kanal an.
  - Er administriert den Kanal und postet im Auftrag Beiträge und Fotos.

- Lettering-Service
  - Er versendet Druckerzeugnisse direkt an Kontakte, die in Listenform bereitgestellt werden.

(2) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Mitarbeiterdaten (Webprogrammierung) – Benutzernamen, E-Mail-Adressen, ggf. Fotos
- Interessentendaten (Webhosting / Analyse-Tool / Cookie-Banner) – Nutzerdaten / Serverlogfiles
- Mitarbeiterdaten (Hosting E-Mail-Postfächer) – E-Mail-Adressen
- Mitarbeiterdaten (Visitenkartenerstellung) – E-Mail-Adresse, Durchwahl, Position

- Kundendaten (Newsletterversand) – E-Mail-Adressen von Kunden
- Bestelldaten (Webshop) – Kontaktdaten, Bestellungen, ggf. Bankdaten
- Bewerberdaten (Bewerberportal) – Kontaktdaten, Bewerbungsunterlagen
- Mitarbeiterdaten / Interessentendaten (Social-Media-Kanäle) – E-Mail-Adressen (für die Rollenzuweisung), ggf. Fotos, Insights-Daten, Inhaltsdaten von Beiträgen

(3) Eine Verarbeitung und Nutzung der personenbezogenen Daten außerhalb der Zweckbestimmung des jeweiligen Vertrages ist dem Leistungsgeber nicht gestattet. Der Leistungsgeber darf jedoch nach Rücksprache Arbeiten durchführen, die zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind (z. B. die Erstellung von Sicherheitskopien und die Durchführung von Migrationen im Rahmen technischer Weiterentwicklungen) sowie so mit den Daten umgehen, wie es im Hinblick auf die Einhaltung gesetzlicher Pflichten der Vertragspartner erforderlich ist.

(4) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen hauptsächlich Beschäftigte. Aufgrund der Dienstleistungsart kann ein Zugriff auf personenbezogene Daten weiterer Betroffener (Kunden, Lieferanten, Interessenten) nicht ausgeschlossen werden.

(5) Hinweise zur Fernwartung: Sofern der Auftragnehmer die Wartung und/oder Pflege der IT-Systeme im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.

Der Auftragnehmer ist verpflichtet, Technologien einzusetzen, die nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglicht, sondern dem Auftraggeber auch eine Möglichkeit gibt, die Fernwartungsarbeiten jederzeit zu unterbinden.

Wenn der Auftraggeber bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.

Falls im Rahmen der Wartung Daten beim Auftragnehmer gespeichert wurden, sind diese nach Abschluss der Arbeiten sorgfältig wieder zu löschen.

4. Leistungsort

(1) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

(2) Sofern der Auftraggeber ein Produkt über den Auftragnehmer bestellt oder einsetzt, dessen Anbieter seinen Sitz in einem Drittland hat und dieser Anbieter durch die Leistungen des Auftragnehmers als dessen Subunternehmer fungiert, findet zwangsläufig eine Datenverarbeitung in diesem Drittland statt. Der Einsatz dieses Anbieters (Subunternehmens) findet somit mit Zustimmung des Auftraggebers statt.

(3) Darüberhinausgehende Datenübermittlung in ein Drittland erfolgen ebenfalls nur mit der vorherigen Zustimmung des Auftraggebers und wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

5. Verantwortlichkeit

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortlicher" im Sinne des Art. 4 Ziff. 7 DS-GVO).

(2) Auftraggeber sowie Auftragnehmer müssen gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Dazu müssen alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf das Datengeheimnis verpflichtet und über ihre Datenschutzpflichten belehrt werden. Dabei ist jede Partei für die Verpflichtung des eigenen Personals zuständig. Ferner müssen die eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht.

(3) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

6. 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 2**].

(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 unterstützt angesichts der Art der Verarbeitung den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen.

7. 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.

8. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Sie erreichen unseren Datenschutzbeauftragten unser folgenden Kontaktdaten:

ITM systems GmbH & Co. KG, Abteilung Datenschutz, Hauptstraße 43, 48712 Gescher
Tel.: 02542 917 918 0 | E-Mail: datenschutz@itm-gruppe.com

(2) 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. Die Verpflichtung zur Einhaltung des Datengeheimnisses und der Vertraulichkeit bestehen auch nach Beendigung dieser Vereinbarung fort.

(3) 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 2**].

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

(5) 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.

(6) 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.

(7) 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.

(8) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 12 dieses Vertrages.

9. Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z. B. durch Einholung von Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Der Auftraggeber ist hinsichtlich der vom Auftragnehmer eingesetzten und vom Auftraggeber genehmigten Verfahren zur automatisierten Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich und hat – neben der eigenen Verpflichtung des Auftragnehmers – ebenfalls die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.

(4) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

(5) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

(6) Der Auftraggeber stellt sicher, dass die aus Art. 32 DS-GVO resultierenden Anforderungen bzgl. der Sicherheit der Verarbeitung seinerseits eingehalten werden. Insbesondere gilt dies für Fernzugriffe des Auftragnehmers auf die Datenbestände des Auftraggebers.

10. Vereinbarung zur Wahrung des Berufsgeheimnisses nach § 203 StGB

Sofern der Auftraggeber der Schweigepflicht gem. § 203 StGB unterliegt, gilt Folgendes:

(1) Im Rahmen dieses Auftrages werden auch Daten verarbeitet, die unter ein Berufsgeheimnis (im Sinne von § 203 StGB) fallen.

Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist.

Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen nach § 203 Abs. 4 S. 1.

Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

(2) Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z. B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203

Abs. 4 StGB belehrt wurden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.

(3) Der Auftragnehmer ist berechtigt, Unterauftragnehmer zur Vertragserfüllung heranzuziehen. Im Ausland dürfen Unterauftragnehmer zur Vertragserfüllung nur dann herangezogen werden, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist.

Der Auftragnehmer wird etwaige Unterauftragnehmer sorgfältig auswählen und diese, soweit sie im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Vereinbarung erlangen könnten, zur Geheimhaltung verpflichten. Der Auftragnehmer wird ferner etwaige Unterauftragnehmer dazu verpflichten, sämtliche von diesen eingesetzten Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen dies nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren.

(4) Diese Verpflichtung gilt für sämtliche weitere Unterbeauftragungen.

(5) Der Auftragnehmer wird darauf hingewiesen, dass Daten, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u. U. dem Zeugnisverweigerungsrecht von sogenannten mitwirkenden Personen unterliegen (§ 53a Strafprozessordnung (StPO)). Entsprechend § 53a StPO entscheidet jedoch der Berufsgeheimnisträger über die Ausübung des Schweigerechts. Im Falle einer Befragung wird der Auftragnehmer unter Hinweis auf § 53a StPO dieser widersprechen und unverzüglich den Auftraggeber informieren, der daraufhin bzgl. der Wahrnehmung des Schweigerechts entscheidet.

(6) Der Auftragnehmer wird darauf hingewiesen, dass die in seinem Gewahrsam befindlichen Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Die Daten dürfen nicht ohne das Einverständnis des Auftraggebers (Berufsgeheimnisträger) herausgegeben werden. Im Falle einer Beschlagnahme wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren.

11. 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.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Hierfür wird eine 2-wöchige Frist vereinbart. Mit Ablauf der Frist gelten die Änderungen als genehmigt.

(3) Verweigert der Auftraggeber durch seinen Einspruch die Zustimmung aus anderen als aus wichtigen Gründen, kann der Auftragnehmer den Vertrag zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen.
(4) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht.

(5) Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der **Anlage 1** aufgeführten Unternehmen als Unterauftragnehmer für Teilleistungen für den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Unterauftragnehmer gilt die Einwilligung für das Tätigwerden als erteilt.

(6) Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind 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.

(7) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(8) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(9) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

12. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Dieser darf jedoch nicht in einem Konkurrenzverhältnis zum Auftragnehmer stehen. Der Auftraggeber 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.

(2) 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.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI Grundschutz).

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

13. 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-Folgenabschätzung
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.

14. Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet soweit ihm möglich in derartigen Situationen den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.

(2) Der Auftraggeber kann weisungsberechtigte Personen benennen. Diese sind dem Auftragnehmer zu Beginn des Auftrages mitzuteilen.

(3) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(4) 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.

(5) Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer schriftlich oder in Textform mitteilen.

(6) Ansprechpartner bei Auftragnehmer ist: Marco Steinbauer (Bereich Webprogrammierung) / Heike Steinbauer (Bereich Marketing, Design) sowie im Tagesbetrieb das Techniker-Team, das per E-Mail an info@itm-design.com oder über die Zentrale unter der Tel.-Nr. 02542 917 918 0 erreichbar ist.

15. 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.

16. Haftung und Schadensersatz

(1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wird gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.

(2) Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der

a) er den aus der DS-GVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
b) er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
c) er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

(3) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.

(4) Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er

a) seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder
b) unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

(5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

17. Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung den Regelungen des Haupt-Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

(5) Gerichtsstand ist der Sitz des Auftragnehmers.

18. Salvatorische Klausel

(1) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

(2) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(3) Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.

(4) Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unter 18 Abs. 1 genannte unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Daten im Sinne dieses Vertrages am besten gewährleistet.

19. Unterschriften

Ort, Datum

Unterschrift Auftragnehmer (Marco Steinbauer, ITM design GmbH)

Unterschrift Auftraggeber

20. Anlagen

Anlage 1: Unterauftragnehmer

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 1 – Unterauftragnehmer

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

Unterauftragnehmer	**Anschrift/Land**	**Leistung**
ALL-INKL.COM - Neue Medien Münnich	Hauptstraße 68 D-02742 Friedersdorf	Webhosting
TeamViewer GmbH	Jahnstr. 30 D-73037 Göppingen	Fernwartung
eRecht24 GmbH & Co. KG	Lietzenburger Str. 94 D-10719 Berlin	Online-Generator für Impressum und Datenschutzerklärung
Usercentrics GmbH	Rosental 4 D-80331 München	Anbieter Cookie-Banner

Sofern Druckaufträge in Auftrag gegeben werden, die Datenverarbeitungsvorgänge wie Lettershop-Services umfassen, unterstützen uns die folgenden Druckereien. Welche Druckerei wir einsetzen, richtet sich nach dem individuellen Druckauftrag.

Unterauftragnehmer	**Anschrift/Land**	**Leistung**
FLYERALARM GmbH	Alfred-Nobel-Str. 18 D-97080 Würzburg	Druckerei / ggf. Lettershop-Service
Oing-Druck GmbH Co. KG	Ramsdorfer Straße 14 D-46354 Südlohn	Druckerei / ggf. Lettershop-Service
WIRmachenDRUCK GmbH	Mühlbachstr. 7 D-71522 Backnang	Druckerei / ggf. Lettershop-Service
Brinkmann DruckService	Von-Ardenne-Straße 14 D-48703 Stadtlohn	Druckerei / ggf. Lettershop-Service

Sofern wir innerhalb unserer ITM Firmengruppe für die Durchführung der Leistung IT-Support in Anspruch nehmen, werden folgende Unterauftragnehmer eingesetzt:

Unterauftragnehmer	**Anschrift/Land**	**Leistung**
ITM systems GmbH & Co. KG	Hauptstraße 43 D-48712 Gescher	IT-Administration, IT-Support
ViSaaS GmbH & Co. KG	Hauptstraße 43 D-48712 Gescher	IT-Administration (Rechenzentrum)
ITM solutions GmbH	Hauptstraße 43 D-48712 Gescher	IT-Administration, IT-Support

Anlage 2 – Technisch-Organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren.

Der generelle Zutritt zu den Geschäftsräumen der ITM design GmbH wird – während der Geschäftszeiten – dadurch gewährleistet, dass die hintere Eingangstür zum Bürogebäude stets verschlossen ist. Der Haupteingang wird durch einen stetig besetzten Empfang kontrolliert.

Der Besucher wird hier durch einen Mitarbeiter empfangen, der den gewünschten Ansprechpartner informiert und ggf. ins Besprechungszimmer begleitet.

Da die Mitarbeiterzahl überschaubar ist, ist eine gesonderte Kennzeichnung der Besucher nicht notwendig. Eine fremde Person fällt direkt als Besucher auf.

Es ist dokumentiert, welche Mitarbeiter Schlüssel zu den Bürogebäuden und einzelnen Büros erhalten haben. Ein Verlust muss direkt gemeldet werden.

Der Zutritt zum Serverschrank ist nur berechtigten Personen gestattet. Wartungsarbeiten werden durch internes Fachpersonal durchgeführt.

Um die Zutrittskontrolle auch außerhalb der Geschäftszeiten zu gewährleisten, werden alle Gebäudetüren mit einem Sicherheitsschloss verschlossen. Zusätzlich werden Durchgangstüren zu den verschiedenen Büroräumen verschlossen sowie die einzelnen Büros selbst.

Im Rahmen des für die tägliche Arbeit genutzten Rechenzentrums wird darauf geachtet, dass:

- der Zutritt zum Rechenzentrum nur autorisierten Personen gestattet ist
- der Zutritt durch ein materielles (RFID-Chip) und ein geistigen (PIN) Identifikationsmerkmal gesichert ist
- der Zutritt zu den einzelnen Kundenschränken oder -flächen ausschließlich durch den Kunden und durch das zuständige Personal möglich ist
- die Zutrittskontrollsysteme sowie die Raumüberwachung über USV und Netzersatzanlage gegen Stromausfall gesichert sind
- das Rechenzentrum, insbesondere der Zutritt zu Sicherheitsbereichen mit Raumüberwachung und Einbruchmeldeanlage ausgestattet ist
- es nach ISO/IEC 27001, EN 1047-2 und ECB-S zertifiziert ist

Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Der Zugang zu Anwendungen und Dokumenten ist grundlegend durch ein Berechtigungskonzept gewährleistet. Mit individuellen Benutzernamen und Kennwörtern erfolgt sowohl die Anmeldung am PC-Arbeitsplatz als auch der Login zu einzelnen Anwendungen. Es existiert eine Kennwortrichtlinie, nach

der sich die Mitarbeiter richten müssen. Diese entspricht den Standards nach der DIN-Norm für Informationssicherheit – ISO 27001.

Zudem ist eine „Clean Desktop Policy“ etabliert, die regelt, dass alle Mitarbeiter bei Abwesenheit ihren Bildschirm durch einen Passwortschutz sperren und keine personenbezogenen oder vertraulichen Daten durch Unbefugte eingesehen werden können.

Das interne Netzwerk ist durch eine Firewall vor externen Zugriffen geschützt. Die regelmäßige Wartung übernimmt der interne IT-Verantwortliche.

Um den externen Zugriff auf das Netzwerk für Mitarbeiter zu gewährleisten, wird eine verschlüsselte VPN-Verbindung genutzt.

Die Arbeit mit Notebooks erfolgt unter der Anweisung, sämtliche personenbezogenen Daten nicht lokal, sondern auf dem Firmenserver zu speichern. Falls auf externen Datenträgern personenbezogene Daten transportiert werden, sind diese zu verschlüsseln.

Für den zuverlässigen Schutz vor Viren oder Trojanern ist ein Virenschutzkonzept umgesetzt, das sowohl für die Arbeitsplätze der Mitarbeiter als auch für die Notebooks der Mitarbeiter anwendbar ist.

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Im Zuge eines Berechtigungskonzeptes ist gewährleistet, dass die Mitarbeiter nur die Daten verarbeiten, die sie für ihre Arbeit benötigen. In diesem Konzept sind auch verschiedene Profile festgelegt, um den Benutzern entsprechende Rechte zum Lesen, Schreiben oder Löschen zuweisen zu können. Administrative Rechte besitzen lediglich die mit der Wartung vertrauten internen Mitarbeiter.

Im Falle der Verwendung von USB-Sticks werden nur solche genutzt, die durch den IT-Verantwortlichen ausgegeben wurden. Die Mitarbeiter wurden durch eine Richtlinie auf die datenschutzfreundliche Verwendung dieses Mediums hingewiesen. Falls der Einsatz von externen Festplatten nötig ist, werden diese ebenfalls kontrolliert durch den IT-Verantwortlichen ausgegeben. Für die Wiederverwendung wird für eine fachgerechte Löschung der nicht mehr benötigten Daten gesorgt. Ebenso ist eine fachgerechte Entsorgung der Hardware geregelt, wenn sie nicht mehr verwendet werden soll.

Papierdokumente werden ebenfalls fachgerecht entsorgt, wenn sie personenbezogene Daten enthalten. Dies erfolgt mit einem Aktenvernichter unter Einhaltung der Sicherheitsstufen nach DIN 66399.

Die für die Datenverarbeitung genutzten Anwendungen sind mit einer Historienfunktion ausgestattet, die eine Protokollierung von Eingabe, Änderung und Löschung von Daten gewährleistet.

Trennungskontrolle

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

Datenerhebungen erfolgen stets zu einem bestimmten Zweck. Zu unterschiedlichen Zwecken erhobene Daten werden getrennt voneinander gespeichert.

Test- und Produktivdaten werden unterschieden. Produktivdaten werden in keiner Weise zu Testzwecken genutzt.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

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.

Bei der Weitergabe von personenbezogenen Daten werden Verfahren genutzt, die eine verschlüsselte Übertragung gewährleisten. Dies umfasst die Nutzung von verschlüsselten VPN-Verbindungen sowie den Einsatz von Fernwartungstools, die eine Sitzungsverschlüsselung gewährleisten (derzeit werden Datenkanäle mit einem 2048 Bit RSA Public-/Private Key Exchange aufgebaut und mit 256 Bit AES verschlüsselt).

Wenn einzelne Dokumente mit personenbezogenen Daten per E-Mail übermittelt werden, sind die Mitarbeiter auf Grundlage einer Richtlinie dazu verpflichtet, diese mit Hilfe eines Passwortes zu verschlüsseln. Zusätzlich ist ein Outlook-Plugin installiert, das eine komplette Verschlüsselung des E-Mail-Inhalts inkl. Anhänge gewährleistet, sofern diese durch den Nutzer aktiviert wird. Standardmäßig werden E-Mails mittels einer TLS-Verschlüsselung verschlüsselt. Die Mitarbeiterrichtlinie enthält auch Regelungen, welche Übertragungswege genutzt werden dürfen und welche aus Datenschutzgründen nicht erlaubt sind.

Zur gesamtheitlichen Übersicht wird ein Verfahrensverzeichnis geführt, in dem jegliche Weitergabe von Daten dokumentiert ist.

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Durch eine systemseitige Protokollierung, welcher Benutzer wann eine bestimmte Änderung von Daten vorgenommen hat, wird die Eingabekontrolle sichergestellt.

Bei der Nutzung von Fernwartungstools wird darauf geachtet, dass die Mitarbeiter sich nicht ohne Absprache des Kunden auf die Systeme schalten. Es existiert eine Richtlinie zur Fernwartung, nach der die Supporttechniker die datenschutzkonforme Wartung durchführen.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Im Falle eines Notfalls, der die gewohnte Arbeitsweise beeinträchtigt, greift ein Notfallkonzept, das die Wiederherstellung des IT-Betriebs sicherstellt.

Es ist außerdem ein umfangreiches Datensicherungskonzept eingeführt, das ein zuverlässiges Backup und die schnelle Wiederherstellbarkeit von Daten gewährleistet. Die Datensicherungen werden an einem sicheren, ausgelagerten Ort aufbewahrt. Durch regelmäßige Tests wird geprüft, ob die Datenrücksicherung einwandfrei funktioniert. Außerdem erfolgt eine automatische Überprüfung, ob die Sicherung erfolgreich durchgeführt worden ist. Bei Fehlern werden die Administratoren automatisch benachrichtigt.

In den Serverräumen sind eine USV sowie eine redundante Klimaanlage installiert, die an die Größe des Serverraumes angepasst sind. Für die zuverlässige Brandvorbeugung und -bekämpfung sind Rauchwarnmelder installiert und Feuerlöscher stehen bereit.

Um die Belastbarkeit der Systeme sicherzustellen, werden Betriebssysteme auf Client-Arbeitsplätzen sowie Servern regemäßig aktualisiert. Auch Hilfsprogramme wie der PDF-Reader oder zip-Programme werden regelmäßig aktualisiert. Ebenso werden Firmwareupdates von Firewall- und Routersystemen durchgeführt, wenn sie die Sicherheit des Netzwerkes erhöhen bzw. aufrechterhalten.

Dieses Vorgehen ist in der Richtlinie zur Betriebssicherheit festgehalten. Diese orientiert sich an Standards gemäß ISO 27001.

Im Rahmen des Rechenzentrumsbetriebes wird insbesondere darauf geachtet, dass:

- die Stromversorgung durch Redundanzen sichergestellt wird (Notstromaggregate sowie USV-Anlagen mit n+1 Redundanz; Überbrückungszeit mindestens 15 min. bis die Notstromaggregate die Stromversorgung wieder sicherstellen - Anlaufzeit inkl. Lastübernahme 1-2 min.)
- eine redundante Internetanbindung mit direktem Draht zu den wichtigsten Internetknoten eingerichtet ist
- das Rechenzentrum mit einer Raumklimatisierung ausgestattet ist (mittlere Temperatur 22° C +/- 4°, redundant ausgelegt (n+1), die installierten Luftfilter entsprechen DIN EN 779 G4)
- an den Kältebedarf anpassbare, redundante Klimaanlagen mit Warmgangeinhausung eingerichtet sind
- das Rechenzentrum über baulich getrennte Brandabschnitte verfügt und in den Räumlichkeiten eine Brandmeldeanlage installiert ist
- die Hochwasser- und Erdbebenkritikalität DIN-gerecht geprüft wurde
- die Messbarkeit der Prozesse durch permanente Systemüberwachung gegeben ist
- es insgesamt nach ISO/IEC 27001, EN 1047-2 und ECB-S zertifiziert ist

Auftragskontrolle

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

Dienstleister, die die ITM design GmbH in ihrer Tätigkeit unterstützen, werden sorgfältig ausgewählt. Besonders der Bereich Datenschutz und Informationssicherheit ist ein wichtiges Kriterium bei der Auswahl. Im Zuge der Verwendung ausländischer Dienste ist sichergestellt, dass ein vergleichbar hoher Datenschutzstandard eingehalten wird.

Es wird stets ein Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO geschlossen, wenn die Datenverarbeitung oder Dateneinsicht durch einen externen Dienstleister erfolgt.

Daten, die im Zuge einer Auftragsverarbeitung an die ITM design GmbH übermittelt werden, werden nach Auftragsende gelöscht, sofern dies nicht gegen gesetzliche Aufbewahrungspflichten verstößt. Außerdem ist vertraglich festgehalten, dass Daten, die die ITM design GmbH ihrerseits an Auftragsverarbeiter übermittelt, von diesen nach Auftragsende zuverlässig gelöscht werden. In diesem Zusammenhang sind auch Kontrollrechte auf Seiten der ITM design GmbH festgelegt. Von diesen wird in regelmäßigen Abständen Gebrauch gemacht, indem aktuelle Auditberichte eingeholt werden.

Sämtliche Dienstleister werden zur Verschwiegenheit verpflichtet, sollten sie mit personenbezogenen Daten in Kontakt kommen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management

Für den Aufbau eines Datenschutzmanagementsystems wurde ein interner Mitarbeiter als Datenschutzbeauftragter bestellt. Dieser ist beratend tätig wirkt auf die Einhaltung der Datenschutzgesetze hin.

Mit Einführung eines Datenschutzmanagementsystems wurde auch eine Leitlinie zum Datenschutz veröffentlicht, die für das gesamte Unternehmen anwendbar ist. Gleichzeitig wurden mehrere Richtlinien und Vereinbarungen eingeführt, nach denen die Datenverarbeitung durch die Mitarbeiter erfolgt. Darunter fällt auch die Vertraulichkeitserklärung, die jeder Mitarbeiter im Zuge seiner Einstellung unterschreibt.

In diesem Zusammenhang werden neue Mitarbeiter über die Einhaltung der Datenschutzvorschriften unterrichtet und sensibilisiert. Außerdem finden 1 Mal pro Jahr Mitarbeiterschulungen statt, um die Sensibilisierung aufrechtzuerhalten bzw. weiter zu erhöhen.

Um jederzeit den Überblick zu haben, an welcher Stelle welche Daten verarbeitet werden, wird ein Verfahrensverzeichnis geführt und gepflegt, das alle Verarbeitungstätigkeiten dokumentiert. Hier sind ebenfalls Verarbeitungen aufgeführt, die im Auftrag erfolgen. Entsprechende Sicherheitsmaßnahmen sind dokumentiert und werden regelmäßig auf ihre Angemessenheit überprüft. Die Prüfung inkl. Berichterstellung erfolgt jedes Jahr durch den Datenschutzbeauftragten.

Umgesetzt wird das Datenschutzmanagement mit Hilfe einer Software. Berichte können jederzeit erstellt und exportiert werden.