# Datenschutzrechtliche Vereinbarung (nachfolgend auch Vertrag genannt) über die Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitung gemäß Art. 28 DS-GVO)

zwischen

Name des Auftraggebers

Straße und Hausnummer

PLZ Ort

**- „Auftraggeber“ -**

und

[ thefi.com ] GmbH & Co KG

Ebinger Hauptstraße 22

96179 Ebing

**- „Auftragsverarbeiter“ -**

# 1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

Administrative Wartung und Betreuung der beim Auftraggeber installierten IT-Infrastruktur

Administrative Wartung und Betreuung der beim Auftraggeber genutzten Endgeräte

Wartung oder Support eines Datenverarbeitungsverfahrens mit der Möglichkeit des Zugriffs auf personenbezogene Daten

Operative Verarbeitung personenbezogener Daten im Rahmen der Leistungserbringung

Sonstiges: Gegenstand / Beschreibung der Dienstleistungen

Der Auftragsverarbeiter 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).

Dauer des Auftrags:

Der Vertrag wird auf unbestimmte Zeit geschlossen. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragsverarbeiter eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragsverarbeiter Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

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

Die Verarbeitung personenbezogener Daten im Auftrag erfolgt ausschließlich zweckgebunden.

Der Zweck, der Umfang und die Art sind wie folgt (gemäß der Definition von Art. 4 Nr. 2 DS-GVO):

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

Beschäftigtendaten

Interessenten- / Kundendaten

Dienstleister- / Lieferantendaten

ggf. weitere personenbezogene Daten eintragen

ggf. weitere personenbezogene Daten eintragen

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

Name, Vorname,

Adresse

Telefonnummer

Email-Adresse

Gesundheitsdaten

Kontodaten

Steuerdaten

Sozialversicherungsdaten

Konfessionsdaten

Kommunikationsdaten (z.B. zu Email, Internet, Telefon)

Vertragsstammdaten

Vertragsbewegungsdaten (z.B. Abrechnungsdaten und Zahlungsdaten

ggf. weitere Kategorien von personenbezogenen Daten eintragen

ggf. weitere Kategorien von personenbezogenen Daten eintragen

# 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 Auftragsverarbeiter 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 Auftragsverarbeiter 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 sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragsverarbeiter 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 Auftragsverarbeiters vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

# 4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragsverarbeiters

Weisungsberechtigte Funktionen des Auftraggebers sind:

weisungsberechtigte Funktion des Auftraggebers mit Kontaktdaten

Weisungsempfänger beim Auftragsverarbeiter sind:

Otto Schobert, Ebinger Hauptstraße 22, 96179 Ebing, Tel. 09547-94360

Für Weisung zu nutzende Kommunikationskanäle:

postalisch

per Email (info@thefi.com)

per Telefon (09547-94360)

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 Auftragsverarbeiters

Der Auftragsverarbeiter 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/Auftraggeber 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 Auftragsverarbeiter 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 Auftragsverarbeiter 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.

Der Auftragsverarbeiter hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

Verfügbarkeitskontrolle der Daten durch mindestens tägliche Datensicherung

Plausibilitätskontrolle der Verarbeitungsergebnisse

ggf. weitere Kontrollmaßnahmen eintragen

Das Ergebnis der Kontrollen ist zu dokumentieren.

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 Auftragsverarbeiter 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:

Die in Ziffer 4 genannte weisungsberechtigte Funktion

Der Auftragsverarbeiter 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 Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragsverarbeiter 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 Auftragsverarbeiters dem nicht entgegenstehen.

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

Der Auftragsverarbeiter 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 Auftragsverarbeiter sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Der Auftragsverarbeiter bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

Bankgeheimnis

Fernmeldegeheimnis nach dem TKG und TMG

Sozialgeheimnis

Berufsgeheimnis nach § 203 StGB

Sonstiges: weitere Regelungen, die der Auftragnehmer einhalten muss

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

Der Auftragsverarbeiter 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 Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragsverarbeiter ist als Beauftragte(r) für den Datenschutz bestellt:

Dr. Sebastian Kraska, Marienplatz 2, 80331 München

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

Der Auftragsverarbeiter teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragsverarbeiters 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 Auftragsverarbeiter 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 Auftragsverarbeiter nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

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

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragsverarbeiter ohne gesonderte Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 Satz 2 DS-GVO. Der Auftragsverarbeiter muss dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen 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. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen zudem immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter.

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 Auftragsverarbeiter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragsverarbeiter auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragsverarbeiters 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 Auftragsverarbeiter hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:

Regelmäßige Prüfung der beim Subunternehmer eingerichteten technischen und organisatorischen Maßnahmen (mindestens alle 2 Jahre)

Regelmäßige Prüfung der beim Subunternehmer eingerichteten Datenschutzkonzeptes (mindestens alle 2 Jahre)

Regelmäßige Prüfung der beim Subunternehmer eingerichteten technischen und organisatorischen Maßnahmen (mindestens alle 2 Jahre) durch eine Begehung vor Ort.

Regelmäßige Einholung von Zertifikaten über eine gültige Zertifizierung nach der DS-GVO.

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

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

# 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 2 beschriebene Datenschutzkonzept stellt die Mindestanforderungen 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 Auftragsverarbeiter dar. Hierbei ist auch das Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung beschrieben.

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

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

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

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

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

Wichtig ist außerdem die in Anlage 1 aufgeführte Vereinbarung zur Fernwartung, ohne deren Klärung und entsprechender Zustimmung keine Fernwartung / Anlagen-Monitoring durchgeführt werden kann.

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

Nach Abschluss der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen,

wie nachfolgend beschrieben datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen:

Löschung unter Zuhilfenahme eines für die sichere Datenlöschung zugelassenen Softwareprogramms

Löschung durch mehrmaliges (mind. dreifaches) Überschreiben des Datenträgers mit Ziffern und Zeichen

Vernichtung durch ein auf die Vernichtung von Datenträger spezialisiertes Unternehmen

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

# 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. Als Gerichtsstand wird das für den Auftraggeber örtlich zuständige Gericht vereinbart.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter 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.

Diese Vereinbarung und deren Unterzeichnung durch Auftraggeber und Auftragsverarbeiter bezieht sich ausdrücklich auf die Hauptvereinbarung inklusive Anlage 1 und 2.

Ort, den Datum

Für den Auftraggeber:

Name: Name des Unterzeichners

Position: Position im Unternehmen

Unterschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Für den Auftragsverarbeiter:

Name: Otto Schobert

Position: Geschäftsführer

Unterschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Anlage 1 – Vereinbarung zur Fernwartung**

Um IT-Probleme aus der Ferne schnell lösen zu können, bietet der Auftragsverarbeiter die Installation einer Fernwartungslösung an.

Die Lösung zeichnet sich dadurch aus, dass sie neben der reinen Zugriffsmöglichkeit auch Zustandsinformationen über Hard- und Software sowie einen Änderungsbericht des Problemgeräts mitübermitteln kann und dadurch die Fehleranalyse erleichtert.

Zusätzlich erhalten alle Benutzer auf Wunsch ein Symbol im Info-Bereich der Windows-Taskleiste, mit dem sie Hilfe aus der Ferne anfordern können.

Für den Betrieb der Lösung wird ein kleines Programm, ein sogenannter Agent, auf allen Systemen ausgerollt, die Benutzersupport erhalten möchten. Dieser Agent übermittelt täglich Zustandsinformationen von Hard- und Software über eine gesicherte SSL Verbindung über das Internet an den Auftragsverarbeiter und vermittelt die Verbindung für eine Fernwartungsanfrage.

Fernzugriff bedeutet, dass ein Techniker über eine Internetverbindung Zugriff auf die Geräte des Auftraggebers nimmt. Dazu wird eine Fernzugriffssoftware verwendet, mit welcher eine Maus- und Tastatursteuerung der aktuell angemeldeten Benutzersitzung erfolgt. Dabei wird der Bildschirminhalt an das Technikergerät übertragen. Weiterhin ist ein Zugriff auf Systemebene wie bspw. Systemregistrierung, Dateisystem, Dienste und Kommandozeile im Hintergrund möglich, ohne den Benutzer zu stören.

Alternativ kann der Zugriff auch über TeamViewer, RDP, VPN oder technisch vergleichbaren Lösungen stattfinden.

Der Fernzugriff ist in jedem Falle kostenpflichtig und wird nach der aktuellen Service-Preisliste abgerechnet bzw. gegen bestehende Vereinbarungen wie bspw. Projektverträge, Serviceverträge oder Managed Service Pakete verrechnet.

Der Fernzugriff darf auf den Servern (ein Management-PC gilt ebenfalls als Server) des Auftraggebers installiert und genutzt werden

Jeder Fernzugriff auf Server erfolgt nur nach Bestätigung des Auftraggebers

Vom Auftraggeber wird unbeaufsichtigter Fernzugriff auf Server erlaubt

Der Fernzugriff darf auf den Clients des Auftraggebers installiert und genutzt werden

Jeder Fernzugriff auf Clients erfolgt nur nach Bestätigung des Auftraggebers

Vom Auftraggeber wird unbeaufsichtigter Fernzugriff auf Clients erlaubt

Der Auftragsverarbeiter darf keine Fernwartungssoftware installieren / nutzen. Der Auftraggeber wünscht grundsätzlich Vor-Ort-Einsätze zur Problemlösung auf Servern und Clients.

Sonstiges: weitere Regelungen, die der Auftragnehmer einhalten muss

**Anlage 2 – Technische und organisatorische Maßnahmen**

Der Auftragsverarbeiter sichert zu, dass er die nachfolgend beschriebenen Mindestanforderun-gen im Rahmen seines Datenschutzkonzeptes einhält. Es beschreibt die im Rahmen der Auf-tragsverarbeitung erforderlichen Maßnahmen beim Auftragsverarbeiter zum sicheren Umgang mit personenbezogenen Daten. Die Grundlage für dieses Datenschutz-Konzept bilden die EU-Datenschutzgrundverordnung DS-GVO und ggf. weitere von den interessierten Parteien gefor-derten Maßnahmen. Hierbei orientiert sich der Auftragsverarbeiter im Wesentlichen an den Vor-gaben der Artikel 24, 25 und 32 DS-GVO. Auf Anforderung weist der Auftragsverarbeiter die Einhaltung entsprechend nach.

1. **Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO**
   1. Zutrittskontrolle

Die Räume, in denen die Verarbeitung personenbezogener Daten erfolgt oder Datenverarbei-tungsanlagen installiert sind, dürfen nicht frei zugänglich sein. Sie müssen bei Abwesenheit der Mitarbeiter verschlossen sein. Die Zutrittsberechtigungen müssen in einem geregelten Verfahren nach dem „need to know Prinzip“ vergeben und regelmäßig hinsichtlich ihrer Erforderlichkeit überwacht werden. Räume, in denen Datenverarbeitungsanlagen (Rechenzentrum, Server, Netz-werkverteiler usw.) untergebracht sind, müssen besonders zutrittsgeschützt sein und dürfen nur für Beschäftigte der IT-Administration (ggfs. der Geschäftsleitung) zugänglich sein. Alternativ müssen die Geräte in geeigneten und verschlossenen Schränken untergebracht sein. Besucher und unternehmensfremde Personen müssen in einem dokumentierten Verfahren registriert und innerhalb der Geschäftsräume beaufsichtigt werden.

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Alarmanlage | Schlüsselregelung / Liste |
| Automatisches Zugangskontrollsystem | Empfang / Rezeption / Pförtner |
| Biometrische Zugangssperren | Besucherbuch / Protokoll der Besucher |
| Chipkarten / Transpondersysteme | Mitarbeiter- / Besucherausweise |
| Manuelles Schließsystem | Besucher in Begleitung durch Mitarbeiter |
| Sicherheitsschlösser | Sorgfalt bei Auswahl des Wachpersonals |
| Schließsystem mit Codesperre | Sorgfalt bei Auswahl Reinigungsdienste |
| Absicherung der Gebäudeschächte |  |
| Türen mit Knauf Außenseite |  |
| Klingelanlage mit Kamera |  |
| Videoüberwachung der Eingänge |  |
|  |  |
|  |  |
|  |  |

Weitere Maßnahmen bitte hier beschreiben:

* 1. Zugangskontrolle

Für jeden Netzwerkbenutzer muss ein persönlich zugeordneter Benutzer mit einem komplexen Passwort mit Groß- und Kleinbuchstaben, Ziffer und Sonderzeichen eingerichtet sein. Die Nutzer sind systemseitig zu verpflichten, die Passwörter regelmäßig zu verändern. Die Netzwerkbenutzer sind auf die Einhaltung der Benutzerzugangsrichtlinie zu verpflichten. Eingerichtete Zugangsberechtigungen müssen regelmäßig hinsichtlich ihrer Erforderlichkeit überprüft werden. Die Netzwerkzugriffe müssen überwacht und protokolliert werden, dies beinhaltet auch nicht erfolgreiche Anmeldeversuche. Ein Netzwerkzugang muss automatisiert nach spätestens 10 Fehlversuchen systemseitig gesperrt werden.

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Login mit Benutzername + Passwort | Verwalten von Benutzerberechtigungen |
| Login mit biometrischen Daten | Erstellen von Benutzerprofilen |
| Anti-Viren-Software Server | Zentrale Passwortvergabe |
| Anti-Virus-Software Clients | Richtlinie „Sicheres Passwort“ |
| Anti-Virus-Software mobile Geräte | Richtlinie „Löschen / Vernichten“ |
| Firewall | Richtlinie „Clean desk“ |
| Intrusion Detection Systeme | Allg. Richtlinie Datenschutz und / oder  Sicherheit |
| Mobile Device Management | Mobile Device Policy |
| Einsatz VPN bei Remote-Zugriffen | Anleitung „Manuelle Desktopsperre“ |
| Verschlüsselung von Datenträgern |  |
| Verschlüsselung Smartphones |  |
| Gehäuseverriegelung |  |
| BIOS Schutz (separates Passwort) |  |
| Sperre externer Schnittstellen (USB) |  |
| Automatische Desktopsperre |  |
| Verschlüsselung von Notebooks / Tablet |  |
|  |  |
|  |  |

Weitere Maßnahmen:

* 1. Zugriffskontrolle

Für die Zugriffe auf personenbezogene Daten muss ein dokumentiertes, rollenbasiertes Berech-tigungskonzept vorhanden sein, welches die Zugriffe in der Form einschränkt, dass nur berech-tigte Personen auf die für ihre Aufgabe notwendigen personenbezogenen Daten zugreifen kön-nen (Minimumprinzip). Die Passwort-Regelungen aus der Zugangskontrolle müssen auch im Rahmen der Zugriffskontrolle umgesetzt werden. Die administrativen Tätigkeiten müssen auf einen kleinen Kreis von Administratoren eingeschränkt sein. Die Tätigkeiten der Administratoren müssen im Rahmen technisch vertretbaren Aufwandes überwacht und protokolliert werden.

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Aktenschredder (mind. Stufe 3, cross cut) | Einsatz Berechtigungskonzepte |
| Externer Aktenvernichter (DIN 32757) | Minimale Anzahl an Administratoren |
| Physische Löschung von Datenträgern | Datenschutztresor |
| Protokollierung von Zugriffen auf  Anwendungen, konkret bei der Eingabe,  Änderung und Löschung von Daten | Verwaltung Benutzerrechte durch  Administratoren |
|  |  |
|  |  |

Weitere Maßnahmen:

* 1. Trennungskontrolle

Die Trennung von personenbezogenen Daten muss durch unterschiedliche Speicherorte oder durch eine Mandantentrennung sichergestellt werden.

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Trennung von Produktiv- und Test-  umgebung | Steuerung über Berechtigungskonzept |
| Physikalische Trennung (Systeme /  Datenbanken / Datenträger) | Festlegung von Datenbankrechten |
| Mandantenfähigkeit relevanter  Anwendungen | Datensätze sind mit Zweckattributen ver-  sehen |
|  |  |
|  |  |

Weitere Maßnahmen:

* 1. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Auswertungen müssen pseudonymisiert werden, sofern der Personenbezug für das Ergebnis nicht zwingend erforderlich ist.

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Im Falle der Pseudonymisierung:  Trennung der Zuordnungsdaten und Auf-  bewahrung in getrenntem und abge-  sicherten System (mögl. verschlüsselt) | Interne Anweisung, personenbezogene  Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist  möglichst zu anonymisieren / pseudonymisieren |
|  |  |
|  |  |

Weitere Maßnahmen:

1. **Integrität (Art. 32 Abs. 1 lit. b DSGVO)**
   1. Weitergabekontrolle

Im Rahmen der Weitergabekontrolle muss sichergestellt werden, dass nur berechtigte Personen die personenbezogenen Daten zur Kenntnis nehmen können. Bei einer Übermittlung per E-Mail sind entsprechende Schutzmaßnahmen (z.B. Verschlüsselung der Kommunikation zwischen den Mail-Servern) zu ergreifen. Mobile Geräte oder mobile Speichermedien müssen verschlüsselt werden, wenn auf ihnen personenbezogene Daten gespeichert werden.

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Email-Verschlüsselung | Dokumentation der Datenempfänger  sowie der Dauer der geplanten Über-  lassung bzw. der Löschfristen |
| Einsatz von VPN | Übersicht regelmäßiger Abruf- und  Übermittlungsvorgängen |
| Protokollierung der Zugriffe und Abrufe | Weitergabe in anonymisierter oder  pseudonymisierter Form |
| Sichere Transportbehälter | Sorgfalt bei Auswahl von Transport-  Personal und Fahrzeugen |
| Bereitstellung über verschlüsselte  Verbindungen wie sftp, https | Persönliche Übergabe mit Protokoll |
| Nutzung von Signaturverfahren |  |
|  |  |
|  |  |

Weitere Maßnahmen:

* 1. Eingabekontrolle

Die Eingabe, Änderung und Löschung personenbezogener Daten muss dem durchführenden Beschäftigten zugeordnet werden können. Die Änderung und Löschungen von Datensätzen muss systemseitig eingeschränkt sein, damit ein versehentliches Ändern oder Löschen wirksam verhindert wird. Diese Möglichkeit wird von den eingesetzten Systemen unterschiedlich umgesetzt und wird hier nicht generell beantwortet. Verweis auf das interne Verzeichnis von Verarbeitungstätigkeiten.

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Technische Protokollierung der Eingabe,  Änderung und Löschung von Daten | Übersicht, mit welchen Programmen  welche Daten eingegeben, geändert oder  gelöscht werden können |
| Manuelle oder automatisierte Kontrolle der Protokolle | Nachvollziehbarkeit von Eingabe,  Änderung und Löschung von Daten durch  Individuelle Benutzernamen (nicht  Benutzergruppen) |
|  | Vergabe von Rechten zur Eingabe,  Änderung und Löschung von Daten auf  Basis eines Berechtigungskonzepts |
|  | Aufbewahrung von Formularen, von  denen Daten in automatisierte Verar-  beitungen übernommen wurden |
|  | Klare Zuständigkeiten für Löschungen |

Weitere Maßnahmen:

1. **Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**
   1. Verfügbarkeitskontrolle

Die Verarbeitung von personenbezogenen Daten muss auf Datenverarbeitungssystemen erfol-gen, die einem regelmäßigen und dokumentierten Patch-Management unterliegen. Es dürfen im Netz keine Systeme verbunden sein, die außerhalb der Wartungszyklen der Hersteller sind (insb. kein Windows XP, Windows Server 2003 etc.). Sicherheitsrelevante Patches sollten innerhalb von 72 Stunden nach Bekanntgabe eingespielt werden. Die durchgängige Verfügbarkeit von personenbezogenen Daten muss mittels redundanten Speichermedien und Datensicherungen gemäß dem Stand der Technik gewährleistet werden. Rechenzentren und Serverräume müssen dem Stand der Technik (Temperaturregelung, Brandschutz, Wassereinbruch etc.) entsprechen. Die Server müssen über eine unterbrechungsfreie Stromversorgung (USV) verfügen, die ein geregeltes Herunterfahren ohne Datenverlust sicherstellt.

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Feuer- und Rauchmeldeanlagen | Backup & Recovery-Konzept (ausformuliert) |
| Feuerlöscher Serverraum | Kontrolle des Sicherungsvorgangs |
| Serverraumüberwachung Temperatur  und Feuchtigkeit | Regelmäßige Tests zur Datenwiederher-  Herstellung und Protokollierung der  Ergebnisse |
| Serverraum klimatisiert | Aufbewahrung der Sicherungsmedien an  einem sicheren Ort außerhalb des  Serverraums |
| USV | Keine sanitären Anschlüsse im oder  oberhalb des Serverraums |
| Schutzsteckdosenleisten Serverraum | Existenz eines Notfallplans (z.B. BSI IT-Grund-  schutz 100-4) |
| Datenschutztresor (S60DIS, S120DIS,  andere geeignete Normen mit Quell-  dichtung etc.) | Getrennte Partitionen für Betriebs-  systeme und Daten |
| RAID System / Festplattenspiegelung |  |
| Videoüberwachung Serverraum |  |
| Alarmmeldung bei unberechtigtem Zutritt  zu Serverraum |  |
|  |  |
|  |  |
|  |  |

Weitere Maßnahmen:

1. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)**
   1. Datenschutz-Management

Es muss ein Verfahren zur Überwachung des Datenschutzes im Unternehmen implementiert sein. Dieses muss die Verpflichtung der Beschäftigten auf das Datengeheimnis, die Schulung und Sensibilisierung der Beschäftigten und die regemäßige Auditierung der Datenverarbeitungsverfahren beinhaltet. Ebenso muss die Dokumentation des für den Auftraggeber durchgeführten Verarbeitungsverfahrens vor Aufnahme der Datenverarbeitung erfolgen.

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Software-Lösungen für Datenschutz-  Management im Einsatz | externer Datenschutzbeauftragter (siehe oben) |
| Zentrale Dokumentation aller Verfahrens-  weisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …) | Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet |
| Sicherheitszertifizierung nach ISO 27001,  BSI IT-Grundschutz oder ISIS12 | Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich |
| Sicherheitskonzept in Anlehnung an VdS3473 | Interner / externer Informationssicherheitsbeauftragter Name / Firma Kontakt |
| Eine Überprüfung der Wirksamkeit der  Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt | Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt |
|  | Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach |
|  | Formalisierter Prozeß zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden |
|  |  |
|  |  |

Weitere Maßnahmen:

* 1. Incident-Response-Management

Für Datenschutzverletzungen und die Wahrung der Betroffenenrechte muss ein durchgängiger Meldeprozess und Bearbeitungsprozess eingeführt sein. Dieser muss auch die Information des Auftraggebers beinhalten.

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Einsatz von Firewall und regelmäßige  Aktualisierung | Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht  gegenüber Aufsichtsbehörde) |
| Einsatz von Spamfilter und regelmäßige  Aktualisierung | Dokumentierte Vorgehensweise zum  Umgang mit Sicherheitsvorfällen |
| Einsatz von Virenscanner und regelmäßige Aktualisierung | Einbindung von  DSB und  ISB in Sicherheitsvorfälle und Datenpannen |
| Intrusion Detection System (IDS) | Dokumentation von Sicherheitsvorfällen  und Datenpannen z.B. via Ticketsystem |
| Intrusion Prevention System (IPS) | Formaler Prozeß und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvor-  fällen und Datenpannen |
|  |  |
|  |  |
|  |  |

Weitere Maßnahmen:

* 1. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Privacy by design / Privacy by default

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Es werden nicht mehr personenbezogene  Daten erhoben, als für den jeweiligen Zweck erforderlich sind |  |
| Einfache Ausübung des Widerrufrechts  des Betroffenen durch technische Maß-  nahmen |  |
|  |  |
|  |  |

Weitere Maßnahmen:

* 1. Auftragskontrolle (Outsourcing an Dritte)

|  |  |
| --- | --- |
| **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
|  | Vorherige Prüfung der vom Auftrag-  nehmer getroffenen Sicherheitsmaß-  nahmen und deren Dokumentation |
|  | Auswahl des Auftragnehmers unter  Sorgfaltsgesichtspunkten (gerade in  Bezug auf Datenschutz und Datensicher-  heit |
|  | Abschluss der notwendigen Vereinbarung  zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln |
|  | Schriftliche Weisungen an den Auftrag-  nehmer |
|  | Verpflichtung der Mitarbeiter des Auftrag-  nehmers auf Datengeheimnis |
|  | Verpflichtung zur Bestellung eines Daten-  schutzbeauftragten durch den Auftrag-  nehmer bei Vorliegen Bestellpflicht |
|  | Vereinbarung wirksamer Kontrollrechte  gegenüber dem Auftragnehmer |
|  | Regelung zum Einsatz weiterer Sub-  unternehmer |
|  | Sicherstellung der Vernichtung von Daten  nach Beendigung des Auftrags |
|  | Bei längerer Zusammenarbeit: Laufende  Überprüfung des Auftragnehmers und  seines Schutzniveaus |

Weitere Maßnahmen:

**ENDE DES DOKUMENTS**