Vereinbarung über die Auftragsverarbeitung

zwischen

- nachstehend Verantwortlicher genannt -
und der
3H Solutions AG
- nachstehend Auftragsverarbeiter genannt -

Auftraggeber / Verantwortlicher

Name des Verantwortlichen	
Straße/Nr.	
PLZ/Ort	
Name des fachlichen Ansprechpartners	
Telefon:	
Email:	
Name des Datenschutzbeauftragten/-koordinators	
Telefon:	
Email:	
Name des Informationssicherheitsbeauftragten	
Telefon:	
Email:	

Auftragnehmer / Auftragsverarbeiter

3H Solutions AG
Hohenlindener Str. 1
81677 München

Name des fachlichen Ansprechpartners:	Tamer Hosgör
Telefon:	089 – 209 263 30
Email:	tamer.hosgoer@tamtech.org
Name des Datenschutzbeauftragten:	ER Secure GmbH
Telefon:	089 – 552 94 870
Email:	datenschutz@3h.solutions

Teil 1: Vertrag zu Datenschutz und zur Informationssicherheit

§1 Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten im Rahmen der Leistung des/der Hauptvertrag/Leistungsvereinbarung durch den Auftragsverarbeiter für den Verantwortlichen in dessen Auftrag und nach dessen Weisung. Sie ist im Teil2 unter Punkt 1 benannt.
(2) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des/der Hauptvertrag/Leistungsvereinbarung. Sie ist im Teil2 unter Punkt 2 benannt.

§2 Umfang und Zweck der Datenverarbeitung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten für den Verantwortlichen. Der Umfang der Verarbeitung sowie der Zweck der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten durch den Auftragsverarbeiter für den Verantwortlichen sind konkret beschrieben im Teil2 unter Punkt 5.

(2) Die Daten dürfen nur zweckgebunden verarbeitet werden. Ausgeschlossen ist es, die Daten für andere Zwecke, insbesondere eigene Zwecke zu verwenden oder außerhalb des vereinbarten Zweckes an Dritte weiterzugeben.

(3) Die Verarbeitung umfasst nicht die Erteilung von Auskünften an Dritte oder den Betroffenen. Dies bedarf im Einzelfall einer gesonderten Beauftragung.

(4) Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Ausgenommen sind Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(5) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und in Übereinstimmung mit §11(1) dieser Vereinbarung nach Einigung der Parteien in Schriftform zu dokumentieren.

§3 Art der verwendeten Daten

(1) Die Art der verwendeten personenbezogenen Daten ist konkret beschrieben im Teil2 unter Punkt 3.

§4 Informationssicherheit

(1) Der Auftragsverarbeiter verpflichtet sich, alle Informationen und Daten des Verantwortlichen nach dem Stand der Technik sofort wirksam gegen unberechtigten Zugriff, Veränderung, Zerstörung oder Verlust, unerlaubte Übermittlung, anderweitige unerlaubte Verarbeitung und sonstigen Missbrauch im Rahmen eines Sicherheitskonzeptes zu sichern. Das Sicherheitskonzept ist konkret beschrieben im Teil3.

Der Auftragsverarbeiter stimmt sein Sicherheitskonzept mit dem zuständigen Informationssicherheitsbeauftragten des Verantwortlichen ab. Teil3 kann durch ein genehmigtes Zertifizierungsverfahren abgebildet werden, um hinreichende technische und organisatorische Maßnahmen nachzuweisen. Der Nachweis ersetzt aber nicht die Prüfung im Einzelfall. Wird ein solcher Nachweis als Faktor herangezogen, ist dieser den Vertragsunterlagen beizufügen.
(2) Der Auftragsverarbeiter darf Zugriffsberechtigungen auf die Daten des Verantwortlichen nur an eigene Mitarbeiter gemäß Berechtigungskonzept in dem für die jeweilige Aufgabe im Zusammenhang mit der Vertragserfüllung erforderlichen Umfang vergeben. Ist die Vergabe von Zugriffsberechtigungen an Mitarbeiter von Subunternehmen oder an freie Mitarbeiter zur Vertragserfüllung erforderlich, so darf dies erst nach der vorherigen Zustimmung des Verantwortlichen in Textform im für die jeweilige Aufgabe zur Vertragserfüllung erforderlichen Umfang erfolgen. Die zugriffsberechtigten Personen oder Personengruppen sind dem Verantwortlichen auf Anfrage zu benennen. Der Auftragsverarbeiter verpflichtet sich, keinem Unbefugten die ihm zur Nutzung des Systems zugeteilten Zugriffsberechtigungen bekannt zu geben. Wird dem Auftragsverarbeiter die Möglichkeit eingeräumt auf die IT-Systeme des Verantwortlichen oder dessen Auftragsverarbeiter zuzugreifen, so verpflichtet er sich, nur auf die für die Vertragserfüllung notwendigen Daten und Informationen zuzugreifen.

(3) Der Auftragsverarbeiter versichert die Umsetzung der in Teil3 beschriebenen technischen und organisatorischen Maßnahmen vor Beginn der Datenverarbeitung und ist zur regelmäßigen Überprüfung und Anpassung dieser Maßnahmen verpflichtet.

(4) Der Auftragsverarbeiter hat den zuständigen Informationssicherheitsbeauftragten des Verantwortlichen über wesentliche Änderungen der in Teil3 beschriebenen technischen und organisatorischen Maßnahmen in Textform zu informieren. Bei einer absehbaren Minderung der Schutzwirkung ist vor der Änderung die Zustimmung des Verantwortlichen in Textform einzuholen.

§5 Pflichten des Auftragnehmers

(1) Der Auftragsverarbeiter wird den Verantwortlichen bei der Umsetzung der Rechte der Betroffenen auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Widerspruch, Löschung, Recht auf Datenübertragbarkeit der über sie gespeicherten Daten unterstützen. Soweit ein Betroffener sich unmittelbar an den Auftragsverarbeiter zwecks Auskunft, Berichtigung, Löschung oder Sperrung seiner Daten wenden sollte, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(2) Der Auftragsverarbeiter verpflichtet sich, seine mit der Verarbeitung von Daten des Verantwortlichen

befassten Mitarbeiter im Datenschutz zu schulen und auf das Datengeheimnis (Einhaltung der Vertraulichkeit

personenbezogener Daten) zu verpflichten.
(3) Der Auftragsverarbeiter teilt dem Verantwortlichen die Kontaktdaten des/der Ansprechpartner für Datenschutz und Informationssicherheit mit. Soweit der Auftragsverarbeiter gesetzlich zur Bestellung eines Datenschutzbeauftragten verpflichtet ist, bestellt er diesen

schriftlich und teilt dem Verantwortlichenden den / die Namen mit.

(4) Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage die für die Erfüllung von Meldepflichten, die Führung einer Verfahrensübersicht oder die Durchführung einer Datenschutzfolgenabschätzung notwendigen Informationen zur Verfügung.

(5) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen für Verstöße gegen die Regelungen dieser Vereinbarung und für Verstöße gegen anwendbare Datenschutzvorschriften, die auf das Verschulden des Auftragsverarbeiters zurückzuführen sind.

(6) Der Verantwortliche kann jederzeit die Löschung der vertragsgegenständlichen Daten anweisen. Unabhängig hiervon ist der Auftragsverarbeiter verpflichtet, jederzeit auf Verlangen des Verantwortlichen die Daten in einem allgemein lesbaren Format herauszugeben. Im Fall der Löschung muss die Rekonstruktion der Daten ausgeschlossen sein. Der Auftragsverarbeiter wird die vollständige Rückgabe und Löschung der Daten, Vervielfältigungen, Speichermedien nachweisen und in Textform bestätigen. Sofern der Auftragsverarbeiter aufgrund zwingender gesetzlicher Vorschriften die Löschung bestimmter vertragsgegenständlicher Daten, bzw. Datenkategorien, nicht vornehmen darf, muss er dies dem Verantwortlichen mitteilen.

(7) Für den Auftragsverarbeiter besteht die Verpflichtung, Daten des Verantwortlichen auch nach Beendigung der entsprechenden Servicevereinbarung für die Dauer von sechs Monaten aufzubewahren. Innerhalb der sechs Monate sind die Daten in einem allgemein lesbaren Format zurückzugeben oder auf Weisung zu löschen.

(8) Im Falle, dass der Auftragsverarbeiter oder wesentliche Unternehmensteile des Auftragsverarbeiters von einem Dritten erworben werden, oder erwirbt ein Dritter die Aktienmehrheit oder die Mehrheit der Stimmrechte am Auftragsverarbeiter, ist der Verantwortliche berechtigt, diesen Vertrag außerordentlich zu kündigen.

§6 Unterauftragsverhältnisse

(1) Schaltet der Auftragsverarbeiter Subunternehmer oder freie Mitarbeiter ein, so bedarf dies der vorherigen Zustimmung des Verantwortlichen in Textform. Die vertraglichen Vereinbarungen zwischen dem Auftragsverarbeiter und dem Subunternehmer oder freien Mitarbeiter sind durch den Auftragsverarbeiter so zu gestalten, dass sie den Vereinbarungen im Vertragsverhältnis zwischen Verantwortlichen und Auftragsverarbeiter entsprechen. Insbesondere ist durch den Auftragsverarbeiter sicherzustellen, dass der Verantwortliche Kontrollen auch bei Subunternehmern oder freien Mitarbeitern durchführen kann. Der Verantwortliche ist berechtigt, vom Auftragsverarbeiter Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der Verpflichtungen dieses Vertrages – erforderlichenfalls auch durch Einsicht in die relevanten Vertragsdokumente - zu erhalten.

(2) Für die unter Teil4 aufgeführten Subunternehmer und die dort genannten Aufgabenbereiche gilt die Zustimmung des Verantwortlichen mit Vertragsschluss als erteilt. Der Auftragsverarbeiter stellt sicher, dass diese Subunternehmer die technischen und organisatorischen Anforderungen gemäß Teil3 ebenso einhalten wie der Auftragsverarbeiter selbst. Werden im Laufe der Vertragsbeziehungen Subunternehmer ausgetauscht oder hinzugefügt, so bedarf dies der Zustimmung des Verantwortlichen in Textform.

§7 Datenverarbeitung in einem Drittstaat

(1) Erfolgt die Verarbeitung von personenbezogenen Daten aus der EU durch den Auftragsverarbeiter oder dessen Subunternehmer außerhalb des Europäischen Wirtschaftsraumes (EU-Staaten zzgl. Island, Liechtenstein, Norwegen) oder eines Staates, für den die EU-Kommission ein angemessenes Datenschutzniveau festgestellt hat, oder greift der Auftragsverarbeiter oder dessen Subunternehmer von außerhalb der genannten Staaten auf personenbezogene Daten aus der EU zu, so muss zusätzlich zu dieser Vereinbarung entweder

- mit dem Auftragsverarbeiter oder dessen Subunternehmern die Einbeziehung der EU-Standardvertragsklauseln zur Auftragsverarbeitung in Drittstaaten schriftlich vereinbart werden, oder
- die Datenverarbeitung den verbindlichen Unternehmensregelungen des Auftragsverarbeiters unterliegen, welche von einer zuständigen Aufsichtsbehörde als ausreichend zur Schaffung eines adäquaten Datenschutzniveaus im Sinne des EU-Rechts angesehen werden.

(2) Für personenbezogene Daten aus anderen als den unter §7(1) genannten Ländern, die ebenfalls datenschutzrechtliche Anforderungen an die Datenverarbeitung im Ausland stellen, sind entsprechende Maßnahmen nach Vorgabe des nationalen Rechts umzusetzen.

§8 Pflichten des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Verantwortliche verantwortlich.

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

(3) Der Verantwortliche ist verpflichtet, alle im Rahmen des Auftragsverhältnisses erlangten Kenntnisse über IT-Sicherungsmaßnahmen des Auftragsverarbeiters streng vertraulich als Betriebs- und Geschäftsgeheimnisse zu behandeln. Diese Pflicht gilt auch nach Beendigung des Auftragsverhältnisses weiter.

§9 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche oder dessen Beauftragter ist berechtigt, die Einhaltung der Anforderungen dieses Vertrages zu kontrollieren. Der Auftragsverarbeiter wird die gewünschten Auskünfte erteilen und auf Wunsch des Verantwortlichen einen Nachweis über die Umsetzung seiner Verpflichtungen innerhalb angemessener Zeit erbringen.

(2) Dem Verantwortlichen oder dessen Beauftragten ist nach vorheriger Anmeldung zur Überprüfung der Umsetzung der vertraglichen Vereinbarungen sowie der Angemessenheit der technischen und organisatorischen Datensicherheitsmaßnahmen Zutritt zu den Räumen und Zugriff auf IT-Systeme, in denen Daten des Verantwortlichen verarbeitet werden, zu gewähren.

(3) Um dem Verantwortlichen die Meldung des Vorfalls binnen 72 Stunden an die zuständige Aufsichtsbehörde zu ermöglichen, hat der Auftragsverarbeiter den Verantwortlichen bei Verdacht auf Verletzungen des Schutzes personenbezogener Daten unverzüglich zu informieren. In Abstimmung mit dem Verantwortlichen sind unverzüglich alle erforderlichen Schritte zur Aufklärung des Sachverhalts einzuleiten und weitere Verletzungen des Schutzes personenbezogener Daten zu verhindern.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollhandlungen von Aufsichtsbehörden, die in seinem Unternehmen oder der von ihm genutzten IT-Infrastruktur stattfinden und in deren Rahmen eine Verarbeitung von personenbezogenen Daten des Verantwortlichen stattfindet.

(5) Im Falle eines bevorstehenden Zugriffs auf Daten des Verantwortlichen im Rahmen einer Pfändung, einer Beschlagnahme, eines Ermittlungsverfahren oder einer sonstigen behördlichen Maßnahme, die beim Auftragsverarbeiter durchgeführt wird, oder im Rahmen eines Insolvenzverfahrens oder anderer Maßnahmen Dritter, informiert der Auftragsverarbeiter den Verantwortlichen darüber unverzüglich.

(6) Der Auftragsverarbeiter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Verfügungsgewalt über die vertragsgegenständlichen Daten beim Verantwortlichen liegt und wird ohne die Zustimmung des Verantwortlichen keine Daten an Dritte übermitteln oder diesen Zugriff ermöglichen.

(7) Wird der Auftragsverarbeiter im Falle einer Kontrolle, eines Zugriffs oder anderer ergriffener Maßnahmen in Bezug auf die Daten des Verantwortlichen durch die zugriffsberechtigte Stelle zur Verschwiegenheit verpflichtet, so hat er die Sorgfaltspflicht im Namen des Verantwortlichen jede Möglichkeit zu ergreifen gegen die Maßnahmen und die Verschwiegenheitsverpflichtung vorzugehen.

§10 Weisungsbefugnis des Verantwortlichen

(1) Bei der Verarbeitung personenbezogener Daten ist der Auftragsverarbeiter verpflichtet, ausschließlich den Weisungen des Verantwortlichen zu folgen. Die Weisung bedarf der Textform. Außerhalb von Weisungen darf der Auftragsverarbeiter die ihm zur Verarbeitung überlassenen Daten weder für seine eigenen Zwecke noch für Zwecke Dritter verwenden. Der Auftragsverarbeiter hat nach Weisung des Verantwortlichen die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Sofern der Auftragsverarbeiter der Meinung ist, dass Weisungen des Verantwortlichen gegen geltende Datenschutzbestimmungen verstoßen, hat er den Verantwortlichen unverzüglich darüber zu informieren.

(2) Weisungen wird der Auftraggeber schriftlich oder per E-Mail (in Textform) bestätigen.

§11 Schriftformerfordernis, Salvatorische Klausel

(1) Änderungen oder Ergänzungen zu dieser Vereinbarung bedürfen der Schriftform. Auf dieses Schriftformerfordernis kann nur schriftlich verzichtet werden.

(2) Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, so wird dadurch die Gültigkeit dieser Vereinbarung im Übrigen nicht berührt. Die Vertragsparteien werden in einem solchen Fall die unwirksame Bestimmung durch eine gesetzeskonforme Regelung ersetzen.

Teil 2: Anlage zur Auftragsvereinbarung

1. Gegenstand des Auftrages

- Bereitstellung, Betrieb und Betreuung eines CRM-Systems zur Verwaltung von Kunden- und Interessentendaten, Aufgaben und Vertragsbeziehungen
- Bereitstellung, Betrieb und Betreuung einer Online-Plattform zur Analyse von Kunden- und Interessentendaten und Automatisierung von Interaktionsaufgaben
- Bereitstellung und Betreuung einer Schnittstelle zwischen dem CRM und anderen Systemen des Auftraggebers und der Online-Plattform inklusive E-Post-Verfahren

2. Dauer des Auftrages

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des/der Hauptvertrag/Leistungsvereinbarung.

3. Art der Daten

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

- Personenstammdaten (Name, Vorname, Geburtsdatum, Geschlecht, Anschrift)
- Kommunikationsdaten (z.B. Telefon, Email)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Einkommens- und Steuerdaten
- Kundenhistorie
- Vertragsbeziehungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- Adressdaten
- Bilddateien
- Zugangsdaten
- Audiodateien
- Hobbys
- Gesundheitsdaten
- Pflichtauskunftsangaben von Dritten (z.B. Vorversicherer, Bonität)

4. Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Versicherungsnehmer
- Mitversicherte Personen
- Kontoinhaber
- Vermittlerdaten
- Vermittler-Mitarbeiterdaten
- Mitarbeiter
- Interessenten
- Abonnenten
- Beschäftigte
- Lieferanten, Dienstleister
- Handelsvertreter
- Ansprechpartner

5. Standort der Verarbeitung

- Standorte, an denen die personenbezogenen Daten gespeichert werden:

  Straßburg, Frankreich

  München, Deutschland
- Standorte von denen ein (Fern-) Zugriff auf die personenbezogenen Daten vorgesehen ist:

  München, Deutschland

6. Umfang, Art und Zweck der Datenerhebung und -verarbeitung

- Die Datenerhebung und Verarbeitung erfolgt zum Zweck des Vertragsabschlusses zwischen Auftraggeber und Endkunde
- Der Auftragnehmer übernimmt die Kundenverwaltung der über die MLP zur Verfügung gestellten Plattform generierten Verträge auf Servern und Systemen des Aufraggebers
- Übermittlung der Versicherungsanträge an Produktgeber
- Weiterleitung der Versicherungsverträge vom Produktgeber an den Endkunden und den Auftraggeber
- Erstellung einer Beratungsdokumentation und Versand an den Endkunden und den Auftraggeber
- Datensicherung inkl. Wiederherstellung bei Bedarf

Teil 3: Datenschutzkonzept und Informationssicherheitskonzept

Im Folgenden sind die technischen und organisatorischen Maßnahmen zu dokumentieren, die für die Gewährleistung der Sicherheit der Datenverarbeitung umgesetzt werden.

1. Zutrittskontrolle

Definition: Maßnahmen um einen unbefugten physischen Zutritt zu Datenverarbeitungssystemen zu verhindern, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

a. Es existiert ein Zutrittsberechtigungssystem für Mitarbeiter des Auftragnehmers bzw. dritter Personen (z.B. Reinigungsfirmen; Wartungsfirmen, etc.)

b. Die Ausgabe von Schlüsseln sind über Richtlinien geregelt

c. Unterteilung in verschiedene Sicherheitszonen

d. Die Zutrittsberechtigung zu den Sicherheitszonen (Rechenzentrum etc.) ist gesondert geregelt

e. Das Rechenzentrum ist gegen andere Zutrittsmöglichkeiten gesichert

f. Es werden technisch-organisatorische Maßnahmen zur Zutrittskontrolle und zur Legitimation der Zugriffsberechtigten eingesetzt

g. Es sind erweiterte physische Schutzmaßnahmen implementiert (z.B. Schließanlagensystem, Ausweisleser, Überwachungseinrichtung)

h. Personenkontrolle durch Pförtner bzw. Werkschutz bzw. Empfang

2. Zugangskontrolle

Definition: Maßnahmen um die Nutzung der Datenverarbeitungssysteme durch Unbefugte zu verhindern.

a. Es existiert ein verbindliches Berechtigungskonzept für Endgeräte und Systeme (z.B. Rechner, etc.)

b. Es erfolgt eine Mandantentrennung auf Systemen oder Datenträgern für verschiedene Auftraggeber

c. Es existieren verbindliche Richtlinien zu einem angemessenen Passwortschutz

d. Es erfolgt eine sichere Aufbewahrung der Administrator-Passwörter

e. Durch technische oder organisatorische Maßnahmen wird sichergestellt, dass nicht mehr benötigte Berechtigungen zeitnah entzogen werden

f. Automatische Bildschirmsperrung ist aktiviert und kennwortgeschützt

g. Ereignisse werden protokolliert, zentral gesammelt und archiviert

3. Zugriffskontrolle

Definition: Maßnahmen um Tätigkeiten in den Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen zu verhindern. Personenbezogene Daten dürfen bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

a. Es existiert ein Berechtigungs- und Rollenkonzept zu den Zugriffsrechten

b. Zugriffsbeschränkungen werden gemäß „Need-to-Know“ und „Least Privilege“ umgesetzt

c. Protokollierung der lesenden und schreibenden Zugriffe sowie von unberechtigten Zugriffsversuchen

d. Anlassbezogene Auswertung der Protokolle

e. Umsetzung von Löschfristen für Daten

f. Trennung von Test- und Produktivumgebungen

4. Weitergabekontrolle

Definition: Maßnahmen zur Gewährleistung, dass personenbezogene Daten bei der elektronischen Übertragung und ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es muss festgestellt werden können, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist.

a. Vollständige Dokumentation der Formen der Weitergabe von Daten

b. Dokumentationen der Schnittstellen und der Abruf- und Übermittlungsprogramme

c. Verschlüsselung der Datenübermittlung bei elektronische Weitergaben

d. Beschränkung der Befugnisse zur Datenübertragung

e. Kontrolle der zulässigen Empfänger

f. Technische Beschränkung auf zulässige Empfänger

g. Für die Verwaltung der Datenträger existiert ein ordnungsgemäßes Verfahren (Kennzeichnung, Laufwerksnutzung und -zuordnung)

h. Datenträger sind unter Verschluss bzw. in abgeschlossenen Räumen

i. Richtlinien zur datenschutzgerechten Vernichtung von Daten bzw. Datenträgern sind implementiert

5. Eingabekontrolle

Definition: Maßnahmen zur (nachträglichen) Überprüfung und Feststellung ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

a. Protokollierung der Erfassung, Änderung und Verarbeitung von personenbezogene Daten (wer, wann)

b. Protokollierung der Administratorentätigkeiten im Hinblick auf das Anlegen von Benutzern und das Ändern von Benutzerrechten

c. Organisatorisch festgelegt Zuständigkeiten für die Berechtigungsvergaben auf schützenswerte Ressourcen

6. Auftragskontrolle

Definition: Maßnahmen zur Gewährleistung, da8 die im Auftrag verarbeitete personenbezogene Daten ausschließlich der Weisung nach verarbeitet werden.

a. Vorlage der Verträge mit Unterauftragnehmern

b. Auftragsverarbeiter führt Kontrollen bei Subunternehmern durch

7. Verfügbarkeitskontrolle

Definition: Maßnahmen zum Schutz der personenbezogenen Daten gegen zufällige Zerstörung oder Verlust

a. Backup- und Wiederanlaufkonzept sind implementiert

b. Datenarchivierungskonzept ist implementiert

c. Regelmäßige Tests des Notfallkonzepts werden durchgeführt

d. Funktionsfähige physische Schutzeinrichtungen (Brandschutz, Energie, Klima) sind vorhanden

e. Sicherheitssoftware wird eingesetzt (Virenschutz /Malware-Protection, Firewalls, SPAM-Filter, Verschlüsselungsprogramme)

8. Trennungsgebot

Definition: Maßnahmen zur Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

a. Vorhandensein von Richtlinien und Arbeitsanweisungen

b. Es ist eine „interne Mandantenfähigkeit" beim Auftragnehmer implementiert

c. Es ist eine Funktionstrennung von Produktion und Test vorhanden

d. Regelmäßige Prüfung der bestimmungsgemäßen Nutzung der Informationen und IT-Systeme

9. Organisatorische Grundelemente

Definition: Regelungen und Prozesse um personenbezogene Daten zu schützen.

a. Regelungen zu Prozessen und Verantwortlichkeiten für Datenschutz

b. Regelungen zu Prozessen und Verantwortlichkeiten für Informationssicherheit

c. Bestehen eines Informationssicherheitsmanagements

d. Bestehen eines Incident Managements

e. Regelmäßige Aufklärung und Sensibilisierung der Mitarbeiter und Führungskräfte

Teil 4: Genehmigte Subunternehmer

Name:	TamTech GmbH
Straße/Nr.	Hohenlindener Str. 1
PLZ/Ort	81677 München
Land	Deutschland

Name des Datenschutzbeauftragten/-koordinators: ER Secure GmbH / Tamer Hosgör

Kurzbeschreibung der Aufgabe des Subunternehmers:
Erstellung und Wartung der Software sowie der Server-Umgebung, Umsetzung des SaaS-Angebots, Erbringung von Customer-Support-Leistungen

Teil 5: Unterschriften

.....
Ort, Datum

.....
Unterschrift(en) Auftraggeber

.....
Ort, Datum

.....
Unterschrift(en) 3H Solutions AG