Vereinbarung
über die Verarbeitung personenbezogener Daten
(Auftragsverarbeitung)

zwischen

Name:
Straße:
PLZ Ort:

- nachstehend Auftraggeber genannt -

und

Name: PC-Tutor IT-Systemhaus GmbH
Straße: August-Borsig-Ring 1
PLZ Ort: 15566 Schöneiche bei Berlin

- nachstehend Auftragnehmer genannt -

- nachstehend einzeln oder gemeinsam auch Parteien genannt -

Diese Vereinbarung konkretisiert die gesetzlichen Rechte und Pflichten, die sich für die Vertragsparteien aus dem anwendbaren Datenschutzrecht und insbesondere aus dem Bundesdatenschutzgesetz, ab dem 25.05.2018 aus der Datenschutzgrundverordnung (VO (EU) 2016/679, nachfolgend auch „DS-GVO“) sowie der nationalen Datenschutzgesetze ergeben, sofern und soweit der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet (Anlage 1). Sie findet Anwendung auf alle Tätigkeiten, die mit dem/den Hauptvertrag/Haupt-verträgen in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.
Als solche Tätigkeiten kommen insbesondere ein Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtdaten enthaltenden Dump / Backup-Datei – vor allem im Zusammenhang mit Supportanfragen – in Betracht, soweit auf dem IT-System oder in den Echtdaten personenbezogene Daten enthalten sind. Weiterhin fallen hierunter Hosting von Software, ASP, SaaS oder Cloud basierende Angebote der Softwareüberlassung.
Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit der Hauptverträge. Sie endet, ohne dass es einer gesonderten Kündigung bedarf mit dem Laufzeitende des letzten verbleibenden Vertrages.

§ 1 Definitionen

(1) Personenbezogene Daten: Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

(2) Verarbeitung: Verarbeitung umfasst jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(3) Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete dokumentierte Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in dokumentierter Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten Format zu bestätigen.

§ 2 Anwendungsbereich

(1) Der Auftragnehmer prüft und wartet automatisierte Verfahren oder Datenverarbeitungsanlagen im Auftrag, insbesondere die von ihm im Rahmen eines getrennten Vertragsverhältnisses überlassene Standardsoftware und bietet im Rahmen seiner Supportangebote weitergehende Hilfestellungen im Umgang mit der Software an. Ferner bietet er Softwarelösungen auch im Rahmen von Hosting, ASP, SaaS oder Cloud basierender Angebote an. Im Rahmen dieser Tätigkeiten kann in besonderen Konstellationen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden. Die umfassten Tätigkeiten sind in der Leistungsbeschreibung des Hauptvertrages konkretisiert. Die Hauptverträge sind ferner in Anhang 1 zu dieser Vereinbarung, unter Nennung der jeweils betroffenen Datenkategorien, aufgeführt. Die Auflistung wird von den Parteien bei Wegfall oder Neuabschluss eines weiteren Hauptvertrages, der auch Auftragsverarbeitung zum Gegenstand hat, fortlaufend aktualisiert.

(2) Die nach diesem Vertrag den Parteien auferlegten Rechte und Pflichten gelten nur während der Laufzeit des Vertrages und innerhalb dieses Zeitraums nur in den Zeitabschnitten bei denen tatsächlich eine Auftragsverarbeitung durchgeführt wird oder eine vergleichbare Gefahrenlage für personenbezogene Daten, für die der Auftraggeber verantwortliche Stelle ist, gegeben ist. Alle Tätigkeiten und Aufträge, die keine personenbezogenen Daten erheben oder verarbeiten sind von den Regelungen dieses Vertrages explizit ausgeschlossen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Darüber hinaus kann sich im Einzelfall für den Auftragnehmer eine gesetzliche Verpflichtung zur Verarbeitung personen-bezogener Daten ergeben. In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, die betreffende rechtliche Verpflichtung verbietet eine solche Mitteilung wegen wichtigen öffentlichen Interesses.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des anwendbaren Datenschutzrechts gerecht wird. Er wird die geeigneten und gesetzlich erforderlichen technischen und organisatorischen Maßnahmen treffen, um ein, dem Risiko angemessenes, Schutzniveau zu gewährleisten. Das bedeutet insbesondere 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.

Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Dies beinhaltet insbesondere

- die Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Eine Darstellung dieser technischen und organisatorischen Maßnahmen wird als Anlage 2 diesem Vertrag beigefügt. 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 und dem Auftraggeber mitzuteilen.

(3) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen.

(4) Der Auftragnehmer bestellt den Datenschutzbeauftragten nach der aktuellen Gesetzeslage.

(5) Im Rahmen des Zumutbaren und Erforderlichen sowie unter Berücksichtigung der Art der Verarbeitung und der vorliegenden Informationen hat der Auftragnehmer den Auftraggeber bei der Einhaltung der in Artikeln 33 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten sowie bei Datenpannen (Art. 28 Abs. 3 S 2 lit. F DS-GVO) angemessen zu unterstützen.
Hierzu gehören u.a.

- die Verpflichtung, Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten unverzüglich mitzuteilen. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO,
- erforderlichenfalls die Unterstützung des Auftraggebers bei seinen Pflichten nach Art. 33 und 34 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. f. DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung durchführen,
- erforderlichenfalls die Unterstützung bei der Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)
- erforderlichenfalls die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde (Art. 36 DS-GVO)

Der Auftraggeber erstattet dem Auftragnehmer durch die Unterstützung entstehende Kosten und Aufwand. Können sich die Parteien nicht über den Umfang der Erstattung einigen, werden die Kosten, die der Auftragnehmer für erforderlich halten durfte, in vollem Umfang erstattet.

(6) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber, spätestens jedoch ein halbes Jahr nach Abschluss der zugrunde liegenden Beauftragung. In besonderen, vom Auftraggeber zu bestimmenden, Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

(7) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragsverarbeiters dem nicht entgegenstehen. Unabhängig davon hat der Auftragsverarbeiter personenbezogenen Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Weisung des Verantwortlichen ein berechtigter Anspruch des Betroffenen aus Art. 16, 17 und 18 DS-GVO zugrunde liegt. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig berichtigen, löschen oder deren Verarbeitung einschränken.

(8) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und auf Verlangen in geeigneter Weise nachzuweisen.

(9) Die Auftragsverarbeitung darf nur innerhalb des Gebiets eines Mitgliedstaats der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stattfinden. Eine Verlagerung in ein Drittland außerhalb dieses Gebietes 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).

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Sinne des anwendbaren Datenschutzrechts für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer verantwortlich (Verantwortlicher). Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt dem Auftraggeber.

(2) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen bezüglich Zweck, Art und Umfang der Verarbeitung von Daten an den Auftragnehmer zu erteilen (Einzelweisung). Der Auftraggeber trägt hierdurch anfallende Mehrkosten; der Auftragnehmer kann einen Vorschuss verlangen. Der Auftragnehmer darf die Ausführung zusätzlicher oder geänderter Datenverarbeitungen verweigern, wenn sie zu einer erheblichen Änderung des Arbeitsaufwands führen würden oder wenn der Auftraggeber die Erstattung der Mehrkosten oder den Vorschuss verweigert.

(3) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund von angeblich unrechtmäßigen Datenverarbeitungen Ansprüche geltend machen, wird der Auftraggeber, soweit diese angeblich unrechtmäßigen Verarbeitungen auf Vorsatz oder Fahrlässigkeit des Auftraggebers beruhen, den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen. Soweit der Auftragnehmer den Auftraggeber bei der Erfüllung der Ansprüche Betroffener unterstützt (insbesondere hinsichtlich Berichtigung, Löschung und Sperrung von Daten), erstattet der

Auftraggeber dem Auftragnehmer Kosten und Aufwand. Die Parteien verständigen sich über den erwarteten Umfang von Kosten und Aufwand.

(4) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftragsgeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftragsgeber beim Auftragsnehmer nach Überprüfung bestätigt oder geändert wird.

§ 5 Kontrollpflichten

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis. Die hierfür erforderlichen Informationen werden dem Auftraggeber gemäß nachfolgendem Absatz zur Verfügung gestellt.

(2) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag geregelten Pflichten zur Verfügung. Er ermöglicht und trägt bei zu Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden.

(3) Die Häufigkeit der Kontrollen soll, maximal einmal jährlich erfolgen. Hiervon unbenommen ist das Recht des Auftraggebers, anlassbezogen weitere Kontrollen im Fall von Verletzungen datenschutzrechtlicher Pflichten durch den Auftragnehmer durchzuführen.

(4) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt durch eine Vor-Ort Kontrolle durch die Vorlage eines geeigneten Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revisor, interner oder externer Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditor, Qualitätsauditor) oder einer geeigneten Datenschutz-Zertifizierung durch eine zugelassene Stelle erbracht werden ("Zertifizierungsurkunde"). Die Zertifizierungsurkunde muss es dem Auftraggeber in angemessener Weise ermöglichen, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß beiliegender Anlage 2 zu überzeugen.

§ 6 Subunternehmer

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen die in der Anlage 3 benannten weiteren Auftragsverarbeiter (Subunternehmer) einschaltet. Über eine Änderung der in der Anlage 3 genannten Subunternehmer wird der Auftragnehmer den Auftraggeber informieren und ihm die Möglichkeit geben, gegen derartige Änderungen einen Einspruch zu erheben.

(2) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung gelten 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.

(3) Im Übrigen ist die Beauftragung von Subunternehmern durch den Auftragnehmer nur mit vorheriger Zustimmung des Auftraggebers zulässig. Die Zustimmung darf nur aus wichtigem, dem Auftragnehmer nachzuweisendem Grund verweigert werden.

(4) Der Auftragnehmer wird weiteren Auftragsverarbeitern vertraglich dieselben Pflichten wie nach diesem Vertrag auferlegen, einschließlich hinreichender Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den gesetzlichen Anforderungen erfolgt. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten, datenschutzbezogenen Vertragsunterlagen.

§ 7 Informationspflichten

(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 Stelle“ im Sinne des Bundesdatenschutzgesetzes liegen.

§ 8 Vertragsdauer und -beendigung

(1) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des letztbestehenden Hauptvertrages.

(2) Nach Abschluss der Erbringung der Verarbeitungstätigkeiten bzw. nach Beendigung der Vereinbarung hat der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten zu löschen oder herauszugeben. Dies gilt nicht, soweit für den Auftragnehmer auf Grundlage des anwendbaren Datenschutzrechts eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (z.B. gesetzliche Aufbewahrungspflicht).

(3) 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. Dadurch resultierende zusätzliche Kosten durch die Herausgabe oder Löschung der Daten sind vom Auftraggeber zu tragen.

§ 9 Schlussbestimmungen

(1) Die Parteien sind sich einig, die vorliegende Vereinbarung einschließlich Anlagen im Fall von Änderungen, Anpassungen und/oder Ergänzungen datenschutzrechtlicher Bestimmungen – insbesondere der DS-GVO und/oder der jeweils nationalen Datenschutzgesetze – einvernehmlich anzupassen und zu ändern.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung 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) Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts sowie der Verweisungsnormen des internationalen Privatrechts. Ausschließlicher Gerichtsstand ist Schöneiche bei Berlin.

(4) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Ort, Datum: _____	Ort, Datum Schöneiche, 22.05.2018
_____	_____
Auftraggeber	PC-Tutor IT-Systemhaus GmbH

Anlage 1
Umfang, Art und Zweck der Datenverarbeitung

1. Art der Daten / Datenkategorien und Personen

Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenarten und –Kategorien:

- Kontaktdaten und –historie bzgl. natürlicher Personen d.h. Kunden, Lieferanten, Mitarbeiter, Leiharbeitskräfte, Ansprechpartner von Firmen, Interessenten und Vertretern
- Daten zur Geschäftshistorie von Kunden, Lieferanten und Vertretern
- Daten von Mitarbeitern, Leiharbeitskräften bzw. Anwendern des Systems
- Daten zu finanziellen Transaktionen von Kunden, Lieferanten, Mitarbeitern und Vertretern
- Daten zu Bankverbindungen und Zahlungsarten von Kunden, Lieferanten und Vertretern
- Daten zu Vermögens- und Ertragssituationen von Kunden und Lieferanten
- Daten zu Qualifikationen, Arbeitszeiten und Abläufen von Mitarbeitern und Leiharbeitskräften
- Sonstige (unstrukturierte) personenbezogenen Daten von Kunden, Lieferanten, Ansprechpartnern von Firmen, Interessenten, Vertretern, Mitarbeitern, Leiharbeitskräfte und Anwendern des Systems

2. Kreis der Betroffenen

Die übertragenen personenbezogenen Daten betreffen die folgenden Personengruppen:

- Kunden
- Lieferanten
- Ansprechpartner
- Mitarbeiter
- Leiharbeitskräfte (an den AG überlassenen, externe Arbeitskräfte)
- Anwender des Systems

3. Gegenstand und Zweck der Datenverarbeitung

- Projektierung (Prozessaufnahme und Optimierung) von Software- und Organisationsentwicklungsprojekten für den Auftraggeber
- Entwicklungsleistungen (Softwareentwicklung, Erstellung von Auswertungen aller Art, Prozessentwicklung, Change Management Prozesse)
- Schulungs- und Supportaufgaben für die vom Auftraggeber, bzw. dessen Auftraggeber genutzten Softwareprodukte

Anlage 2
Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO
betreffend Softwarepflegeleistungen der PC-Tutor IT-Systemhaus GmbH
(d.h. Zugriffe im Rahmen der Projektierung, Fehleranalyse, Entwicklung, Software und Remotesupport)
Stand 08.05.2018

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn Ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

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

1.1 Zutrittskontrolle

Der allgemeine Zutritt zum Gebäude erfolgt über eine Sicherheitsschließanlage.

Zutritt zum Serverraum für befugte Personen erfolgt über ein Schließsystem.

1.2 Zugangskontrolle

Für die Anmeldung an das Netzwerk ist ein Kennwort mit einer vorgegebenen Mindestlänge erforderlich. Dabei sind Zahlen und Sonderzeichen zu verwenden, sowie Groß- und Kleinschreibung zu beachten. In bestimmten Konstellationen wird eine 2-Faktor-Authentifizierung verlangt.

Eine automatische Sperrung des Benutzers erfolgt nach drei falschen Eingaben bei der Benutzeranmeldung. Das Kennwort ist spätestens nach 90 Tagen zu ändern. Die Aufforderung erfolgt dazu automatisch. Eine Aktivierung des Bildschirmschoners erfolgt automatisch nach 10 Minuten und kann nur wieder über Passwortfreigabe freigegeben werden.

Benutzerauthentifizierung wird mittels eines zentralen Verzeichnisdienstes abgebildet. Grundsätzlich und soweit nicht technisch notwendig, ist ein Zugang zu Auftragsdaten nur mittels personifizierten Accounts zugelassen.

Das System wird durch eine Firewall ständig überwacht. Es gibt eine Antivirus-Software auf Systemebene. Darüber hinaus ist für das Mail-System eine Antivirus-Software je Client sowie Server installiert. Es werden ausschließlich IT-Systeme eingesetzt, die vom Hersteller durch regelmäßige Sicherheitsupdates unterstützt werden.

1.3 Zugriffskontrolle

Die Zugriffskontrolle ist in differenzierten Berechtigungen auf Menü-Ebene eingerichtet. Ein elektronischer Datensafe überwacht den Zugang der Supportmitarbeiter zu Kundendaten. Zugriffe auf Anwendungen werden protokolliert.

1.4 Pseudonymisierung (Art. 32 Abs. 1 lit. A DSGVO; Art. 25 Abs. 1 DSGVO)

Kommt für Softwarepflegeleistungen nicht als Option in Betracht. Personenbezogene Daten aus dem Datensafe werden nicht weitergegeben. Diese Datenträger mit Kundendaten werden grundsätzlich verschlüsselt.

2. Integrität (Art. 32 Abs. 1.lit. b DSGVO)

2.1 Weitergabekontrolle

Der Transport außerhalb des jeweiligen Netzwerks erfolgt verschlüsselt. Hierzu werden starke Verschlüsselungsalgorithmen eingesetzt. Kundendaten können nur elektronisch direkt in den Datensafe oder per verschlüsselte Verbindung auf einen PC-Tutor FTP-

Server übermittelt werden. Innerhalb des FTP-Servers werden abgelegte Daten nach spätestens 30 Tagen gelöscht.

2.2 Eingabekontrolle

Alle Netzwerkan- und abmeldungen sowie sämtliche Transaktionen auf Dateiebene (z.B. Neuanlagen, Veränderungen, Löschungen) werden protokolliert. Die Protokolle werden hinsichtlich unberechtigter Zugriffe analysiert und nach 6 Monaten gelöscht.

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

3.1 Verfügbarkeitskontrolle

Es wird ein wöchentliches Backup (Vollsicherung) durchgeführt. Dazu wird zusätzlich täglich inkrementell gesichert. Die Sicherung erfolgt in zwei räumlich getrennten Bereichen auf entsprechenden Storage Systemen.

Es wird ein RAID-verfahren bei den Festplattensicherungen eingesetzt. Unterbrechungsfreie Stromversorgung (USV) samt Überspannungsschutz ist vorhanden. In bestimmten Konstellationen wird eine 2-Faktor-Authentifizierung verlangt.

Durch den Einsatz der Firewall und der Antivirus-Software für das Mail-System und alle Server, sowie Antivirus-Software je Client wird die Verfügbarkeit technisch bestmöglich sichergestellt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO,Art. 25 Abs. 1 DSGVO)

4.1 Datenschutzmanagement

Alle Mitarbeiter des Auftragnehmers sind auf das Datengeheimnis verpflichtet. Es erfolgt eine regelmäßige Unterweisung der Mitarbeiter im Datenschutz. Ein Datenschutzkonzept wurde erstellt.

Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach. Für die Bearbeitung von Auskunftsanfragen seitens Betroffener existiert ein formalisierter Prozess. Für die eingesetzten IT-Systeme und Prozesse existieren Verarbeitungsverzeichnisse. Die Wirksamkeit unserer technischen Schutzmaßnahmen wird regelmäßig überprüft.

4.2 Incident-Response-Management

Firewalls, Spamfilter und Virenscanner werden eingesetzt und regelmäßig aktualisiert. Daneben existieren Systeme zur Intrusion Detection und Prevention. Eine Policy regelt den Umgang mit Sicherheitsvorfällen. Es gibt Alarmpläne und eine Dokumentation von Sicherheitsvorfällen und Datenpannen. In Abstimmung mit dem Geschäftsführer erfolgt die Meldung gegenüber den Aufsichtsbehörden.

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Die Prozesse für Softwarepflegeleistungen, die im Zusammenhang mit personenbezogenen Daten stehen, sind klar definiert und die involvierten Mitarbeiter sind per bindender Arbeitsanweisung entsprechend verpflichtet. Dazu gehören, dass Kundendaten nur über den Datensafe entgegengenommen und verwaltet werden. Die Mitarbeiter sind angehalten nicht mehr personenbezogene Daten zu erheben, als für den jeweiligen Zweck erforderlich sind. Aufzeichnungen von Remote-Sitzungen werden nach 4 Wochen automatisch gelöscht.

4.4 Auftragskontrolle (Outsourcing an Dritte)

Unsere Mitarbeiter kennen den Datenverarbeitungszweck. Sie erhalten Weisungen zum Umgang mit personenbezogenen Daten. Spezielle Unterauftragsverhältnisse (Subunternehmer) werden schriftlich beauftragt und sind im Anhang aufgeführt.