

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen dem

Auftraggeber

und der

DPS Software GmbH

Esslinger Straße 7, 70771 Leinfelden-Echterdingen

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Präambel

Im Rahmen einer Leistungsvereinbarung kann es notwendig sein, dass der Auftragnehmer Zugriff auf das System des Auftraggebers erhält, um für den ordnungsgemäßen Betrieb Sorge zu tragen. Im Rahmen der Tätigkeiten des Auftragnehmers ist nicht ausgeschlossen, dass der Auftragnehmer dabei auch Zugriff auf personenbezogene Daten des Auftraggebers erhält. Zur Sicherung und ordnungsgemäßen Verwendung der personenbezogenen Daten werden in diesem Vertrag entsprechende Regelungen getroffen.

Der Vertrag ist in Anlehnung an die ab dem 25.05.2018 geltende Datenschutzgrundverordnung (DS-GVO) ausgestellt. Verweise die auf Normen der DS-GVO referenzieren sind bis zum 24.05.2018 als Verweise auf das Bundesdatenschutzgesetz (BDSG) auszulegen. Sofern Regelungen in diesem Vertrag sich auf die DS-GVO beziehen, die über die Vorschriften des BDSG hinausgehen oder den Vorschriften des BDSG widersprechen, findet die jeweilige Regelung bis zur Gültigkeit der DS-GVO keine Anwendung.

1. Gegenstand und Dauer des Auftrags

(1) Es handelt sich bei diesem Auftrag um einen Grundvertrag für alle zukünftigen Aufträge des Auftraggebers an den Auftragnehmer.

(2) die beiden Vertragsparteien sind sich einig, dass der Auftrag über die Auftragsdatenverarbeitung nur einmal und nicht für jeden einzelnen Auftrag abgeschlossen werden soll.

(3) Die Dauer des Auftrags (Laufzeit) entspricht der Zusammenarbeit des Auftraggebers und des Auftragnehmers.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten ist die Softwarewartung, Hotline-Dienstleistungen sowie projektbezogene Dienstleistungen durch den Auftragnehmer gemäß der mit dem Auftraggeber bestehenden Vereinbarungen.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Abonnenten
- Beschäftigte
- Lieferanten
- Handelsvertreter
- Ansprechpartner

3. 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 1**].

(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. 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.

5. 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:

- a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

Als Datenschutzbeauftragte sind bestellt:

Für die DPS Software GmbH:

Herr Thorsten Jordan, Firma ENSECUR GmbH, Josef-Wolf-Str. 31, 763556 Weingarten,
Telefon: +49 (0) 721 18035671, E-Mail: thorsten.jordan@ensecur.de.

Ein Wechsel des/der Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

- a) 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.
- b) 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 1].
- c) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- d) 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.
- e) 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.
- f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. 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 zur Erfüllung seiner unternehmerischen Aufgaben 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 Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

- a) Der Auftraggeber stimmt der Beauftragung der in **Anlage 2** aufgeführten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:
- b) Die Auslagerung auf 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 innerhalb 14 Tagen nach Anzeige des Auftragnehmers der Auslagerung auf Unterauftragnehmer oder Wechsel des bestehenden Unterauftragnehmers 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.

Die Zustimmung durch den Hauptauftraggeber kann nur bei Vorliegen eines wichtigen Grundes versagt werden. Sollte ein vom Auftragnehmer ausgewählter Unterauftragnehmer abgelehnt werden, steht dem Auftragnehmer innerhalb von 14 Tagen ein Sonderkündigungsrecht von 4 Wochen zum Quartalsende zu.

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

(4) 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.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. 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. Er 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-Grundschrift).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Aufwände des Auftragnehmers, welche im Zusammenhang mit der Überprüfung, Kontrolle und Dokumentation datenschutzrechtlicher Angelegenheiten stehen, werden dann gemäß aktueller Preisliste des Auftragnehmers abgerechnet.

8. 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 vorheriger 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.

9. Weisungsbefugnis des Auftraggebers

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

(2) 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.

10. 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.

11. Sonstiges

(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 wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.

(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) Es gilt deutsches Recht.

Leinfelden-Echterdingen, den 15.05.2018

Dr. Marcus Knieps
Geschäftsführer

Anlage 1 – Technisch-organisatorische Maßnahmen

1. Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- Der Zutritt zu den Geschäftsräumen der DPS Software GmbH ist durch ein Schlüssel-/Schließsystem geregelt. Die Schlüsselausgabe ist dokumentiert. Schlüsselverlust ist unverzüglich zu melden.
- Der Serverraum ist nur für autorisierte (d.h. benannte) Personen zugänglich.
- Außerhalb der Bürozeiten ist ein Wach- und Schließdienst im Einsatz.

2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Die Nutzeranmeldung an Betriebssystemen erfolgt durch Kennworteingabe. Es wird nur ein Zugang pro Benutzer verwendet.
- Das Kennwort muss mindestens acht Zeichen lang sein.
- Das Kennwort muss Zeichen aus drei der folgenden Kategorien enthalten: Großbuchstaben (A bis Z), Kleinbuchstaben (a bis z), Zahlen zur Basis 10 (0 bis 9), nicht alphabetische Zeichen (zum Beispiel !, \$, #, %)
- Kennwortalter beträgt 60 Tage
- Automatische Sperrung bei Fehl- oder Falscheingabe

3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

-
- Die Benutzer sind in mehrere Benutzergruppen gegliedert und verfügen zudem über differenzierte Berechtigungen beim Zugriff auf die Daten.
 - Single-Sign-On Regelung

4. Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle...

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- Der externe Zugriff auf das Firmennetzwerk ist nur über VPN möglich. Alle Zugriffe werden protokolliert.
- Verschlüsselung bei Datenweitergabe/Datenaustausch: Es wird auf Anforderung kundenindividuell Verschlüsselungssoftware zum Einsatz gebracht.
- Für den Remote Desktopzugriff für Remote Support und Fernwartung wird Deskshare, TeamViewer und GoToMeeting eingesetzt. Es wird durch den Nutzer auf Auftraggeberseite eine temporäre Erlaubnis für den Auftragnehmer erzeugt. Der Desktopzugriff ist nur zusammen mit dem Auftragnehmer möglich.

5. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- Protokollierung erfolgt über eine Log-Datei, die aufzeichnet, welche Login-Versuche unternommen wurden, Logouts, Passwortänderungen und schreibender Zugriff auf einen Datensatz, wo technisch möglich und spezifiziert.

6. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

- Bei einer weisungsgebundenen Auftragsdatenverarbeitung (als Auftraggeber) werden die Prozessschritte der Auftragnehmerauswahl, sowie die formalen Anforderungen an die Vertragsgestaltung des § 11 BDSG eingehalten und dokumentiert.
- Bei einer weisungsgebundenen Auftragsdatenverarbeitung (als Auftragnehmer) erfolgt die Verarbeitung der personenbezogenen Daten entsprechend der Weisungen des Auftraggebers.

-
- Im Fall von vereinbarten (Unter-) Auftragsverhältnissen: Die hier vereinbarten Bedingungen zwischen Auftraggeber und Auftragnehmer werden in jedem Vertrag an Subunternehmen weitergegeben. Der Auftraggeber wird in Unterauftragsverhältnisse eingebunden.

7. Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physikalisch / logisch):

- Mehrstufiges Datensicherungskonzept
- Die Systeme sind mit einem Hardware-RAID-Controller ausgestattet.
- Unterbrechungsfreie Stromversorgung
- Systeme sind von außen über eine Firewall geschützt
- Aufbewahrung von Datensicherungsmedien an einem sicheren, ausgelagerten Ort
- Disaster Recovery

8. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- Daten werden entsprechend ihrer Zweckbindung logisch getrennt
- Datenschutzrelevante Kundendaten werden an den möglichen Stellen anonymisiert
- Die Entwicklungssysteme sind mehrschichtig aufgebaut und in lokale Entwicklungsumgebung, Demo- sowie Testumgebung getrennt

Anlage 2 – Unterauftragnehmer

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Dassault Systèmes SE	10, rue Marcel Dassault CS 40501 78946 Velizy-Villacoublay Frankreich	Lieferant für Dassault Produkte, Hotline, Marketing
SOLIDWORKS Deutschland GmbH	Joseph-Wild-Str. 20 81929 München	Lieferant für SOLIDWORKS Produkte, Hotline, Marketing
SolidCAM GmbH	Gewerbepark H.A.U. 36 78713 Schramberg	Lieferant für SolidCAM Produkte, Hotline, Marketing
Ibermática, S.A.	Paseo Mikeletegi, 5. 20009 Donostia - San Sebastián, Spanien	Lieferant für RPS Produkte, Hotline, Marketing
Sage GmbH	Emil-von-Behring-Str. 8-14 60439 Frankfurt am Main	Lieferant für Sage Produkte, Hotline, Marketing
LOGOPRESS - ZA	Z.A. Les Salines 25115 Pouilley Les Vignes Frankreich	Lieferant für LogopressProdukte, Hotline, Marketing
EFICAD S.A.R.L.	55 Avenue de Melgueil 34180 La Grande Motte Frankreich	Lieferant für SWOOD Produkte, Hotline, Marketing
Cimco Integration A/S	Vermundsgade 38, 3 2100 Copenhagen Dänemark	Lieferant für CIMCO Produkte, Hotline, Marketing
Visual Components GmbH	Landsberger Strasse 302 80687 München	Lieferant für Visual Components Produkte, Hotline, Marketing
direct cnc-systeme GmbH	Brühlweg 26 73553 Alfdorf-Bonholz	Lieferant für NCHOPS Produkte, Hotline, Marketing
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen Deutschland	Rechenzentrums Leistungen
Ingenieurbüro Westphal	Dornsgasse 5 99510 Apolda	Geschäftsstelle Apolda, Schulungen