Vertrag zur Auftragsverarbeitung

zwischen

_____

_____

_____

als Verantwortlicher (hier bezeichnet als „Auftraggeber“)

und

der **SD Software-Design GmbH**, Schwarzwaldstr. 21, 79189 Bad Krozingen, vertreten durch den Geschäftsführer Herrn Daniel Kemen,

als Auftragsverarbeiter (hier bezeichnet als „Auftragnehmer“)

Präambel

Der Auftraggeber beauftragt den Auftragnehmer mit den in § 3 genannten Leistungen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

SD Software-Design GmbH
Schwarzwaldstr. 21
79189 Bad Krozingen

Tel: +49 7633 80 69 311
Web: www.software-design.de
E-Mail: info@software-design.de

Registergericht Freiburg
HR-Nr: HRB 713955
Geschäftsführer: Daniel Kemen

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DSGVO 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DSGVO, biometrischen Daten gem. Art. 4 Abs. 14 DSGVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

§ 2 Angabe der zuständigen Datenschutz-Aufsichtsbehörde

(1) Zuständige Aufsichtsbehörde für den Auftraggeber ist:

_____

_____

(2) Zuständige Aufsichtsbehörde für den Auftragnehmer ist der Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Königstrasse 10 a, 70173 Stuttgart.

(3) Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

SD Software-Design GmbH
Schwarzwaldstr. 21
79189 Bad Krozingen

Tel: +49 7633 80 69 311
Web: www.software-design.de
E-Mail: info@software-design.de

Registergericht Freiburg
HR-Nr: HRB 713955
Geschäftsführer: Daniel Kemen

§ 3 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der digitalen Vereinsverwaltung auf Grundlage des abgeschlossenen Nutzungsvertrags („Hauptvertrag“). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und der dazugehörigen Leistungsbeschreibung). 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.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 4 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher oder in einem dokumentierten elektronischen Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus den in der Software als „Administratoren“ hinterlegten Benutzern.

SD Software-Design GmbH
Schwarzwaldstr. 21
79189 Bad Krozingen

Tel: +49 7633 80 69 311
Web: www.software-design.de
E-Mail: info@software-design.de

Registergericht Freiburg
HR-Nr: HRB 713955
Geschäftsführer: Daniel Kemen

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten. Im Rahmen des Standard-funktionsumfangs werden grundsätzlich keine besonderen Kategorien personenbezogener Daten verarbeitet.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in Anlage 2 dargestellt.

§ 6 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere mindestens die in Anlage 3 aufgeführten Maßnahmen der

a) Zutrittskontrolle
b) Zugangskontrolle
c) Zugriffskontrolle
d) Weitergabekontrolle
e) Eingabekontrolle
f) Auftragskontrolle
g) Verfügbarkeitskontrolle
h) Trennungskontrolle

SD Software-Design GmbH
Schwarzwaldstr. 21
79189 Bad Krozingen
Tel: +49 7633 80 69 311
Web: www.software-design.de
E-Mail: info@software-design.de
Registergericht Freiburg
HR-Nr: HRB 713955
Geschäftsführer: Daniel Kemen

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter bestellt: Frau Mareike Forcher. Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

SD Software-Design GmbH
Schwarzwaldstr. 21
79189 Bad Krozingen

Tel: +49 7633 80 69 311
Web: www.software-design.de
E-Mail: info@software-design.de

Registergericht Freiburg
HR-Nr: HRB 713955
Geschäftsführer: Daniel Kemen

(4) 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, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegen.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

(7) 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 Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO).

(8) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig (mindestens jährlich) von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen Anforderung innerhalb einer angemessenen Frist alle ergorderlichen Auskünfte und Nachweise (Art. 32 Abs. 1 lit. d DS-GVO) zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von

SD Software-Design GmbH
Schwarzwaldstr. 21
79189 Bad Krozingen
Tel: +49 7633 80 69 311
Web: www.software-design.de
E-Mail: info@software-design.de
Registergericht Freiburg
HR-Nr: HRB 713955
Geschäftsführer: Daniel Kemen

Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

§ 9 Anfragen und Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DSGVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 10 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

§ 11 Außerordentliches Kündigungsrecht

(1) Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung im Sinne dieses Vertrages des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

SD Software-Design GmbH
Schwarzwaldstr. 21
79189 Bad Krozingen

Tel: +49 7633 80 69 311
Web: www.software-design.de
E-Mail: info@software-design.de

Registergericht Freiburg
HR-Nr: HRB 713955
Geschäftsführer: Daniel Kemen

§ 12 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 13 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Freiburg im Breisgau.

SD Software-Design GmbH
Schwarzwaldstr. 21
79189 Bad Krozingen

Tel: +49 7633 80 69 311
Web: www.software-design.de
E-Mail: info@software-design.de

Registergericht Freiburg
HR-Nr: HRB 713955
Geschäftsführer: Daniel Kemen

Anlagen

Anlage 1 – Beschreibung der besonders schutzbedürftigen Daten/Datenkategorien

Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers

Datum und Unterschriften

SD Software-Design GmbH
Schwarzwaldstr. 21
79189 Bad Krozingen

Tel: +49 7633 80 69 311
Web: www.software-design.de
E-Mail: info@software-design.de

Registergericht Freiburg
HR-Nr: HRB 713955
Geschäftsführer: Daniel Kemen

Anlage 1

Beschreibung der Datenkategorien

- Name, Anrede, Titel, Geburtsdatum
- Kontaktdaten (wie E-Mail, Telefon, Anschrift)
- Zahlungsinformationen (wie Kontodaten, Zahlungsart, Beiträge)
- Familien- und Firmenzugehörigkeiten
- Individuelle Angaben die vom Auftraggeber frei gewählt und gefüllt werden können.

Anlage 2

Beschreibung der Betroffenen/Betroffenengruppen

- Mitglieder
- Mitarbeiter
- Lieferanten
- Kunden
- Kontakte und Interessenten des Auftraggebers,
  die vom Auftraggeber in der Software erfasst und verwaltet werden.

SD Software-Design GmbH
Schwarzwaldstr. 21
79189 Bad Krozingen

Tel: +49 7633 80 69 311
Web: www.software-design.de
E-Mail: info@software-design.de

Registergericht Freiburg
HR-Nr: HRB 713955
Geschäftsführer: Daniel Kemen

Anlage 3

Technische und organisatorische Maßnahmen des Auftragnehmers nach §64 Abs. 3 BDSG

1. Zugangskontrolle

Die Zutrittskontrolle zu den Büroräumen erfolgt über ein proprietäres Türsicherheitssystem, welches den Zutritt zu den Büroräumen personen- und zeitbasiert regelt und protokolliert, sodass sich Unbefugte zu keiner Zeit Zutritt verschaffen können. Fehlgeschlagene Zutrittsversuche über ungültige Schlüssel, oder Zugriffsversuche außerhalb der freigeschalteten Zeiten werden ebenfalls protokolliert. Ausnahmen werden ebenfalls protokolliert. Gehen Schlüssel verloren oder treten Mitarbeiter aus dem Unternehmen aus, werden die Schlüssel unverzüglich gesperrt.

Das Gelände sowie die Eingänge werden über mehrere unabhängige Systeme videoüberwacht und sind vollständig umzäunt. Die Räume sind nicht öffentlich zugänglich und Besucher können sich nicht unbeaufsichtigt in den Räumlichkeiten bewegen. Die Gebäudeeingänge sind mit modernen widerstandsfähigen Türen gesichert und vor ebenerdig erreichbaren Fenster sind zusätzlich Gitter oder widerstandsfähige Rollläden mit Sicherheitssperren angebracht. Im Gebäude gibt es zusätzlich eine Alarmsicherung.

Für Reinigungspersonal oder sonstige externe Personen gilt eine sehr präzise zeitliche Beschränkung. Die betroffenen Personen unterliegen strenger Geheimhaltungs- und Verhaltensrichtlinien, die regelmäßig von Mitarbeitern überwacht und kontrolliert werden. Besucher werden zu jederzeit beaufsichtigt, wenn diese sich in Verarbeitungsräumen aufhalten. Durch einen eigenen Besucher- und Besprechungsraum wird der Aufenthalt von Besuchern in Verarbeitungsräumen üblicherweise nicht erforderlich.

Die Server auf denen die eigenen Webseiten und Softwarelösungen bereitgestellt werden, werden in externen Rechenzentren betrieben, welche durch einen per Video überwachten Hochsicherheitszaun geschützt werden. Die Zufahrt zum Gelände wird durch Zutrittskontrollterminals gesichert und alle Räume und Eingänge werden rund um die Uhr videoüberwacht. Die Rechenzentren sind nach DIN ISO /IEC 27001 zertifiziert.

Zugänge zu Schränken, Geräten und Applikationen, die den Zugriff auf personenbezogenen Daten ermöglichen, sind limitiert und den Mitarbeitenden vorbehalten, die den Zugriff zur Erfüllung Ihrer Aufgaben benötigen. Die Zugänge zu IT-Systemen sind, wann immer technisch möglich, personengebunden und beinhalten wiederum unterschiedliche Zugriffsberechtigungen, die sich nach der Notwendigkeit der Zugriffsmöglichkeiten richtet. Wenn erforderlich, wird hier eine erneute Authentifizierung verlangt. Nach längerer Inaktivität wird anwendungsspezifisch eine erneute Eingabe gefordert. Für die Vergabe und Erneuerung von Passwörtern gibt es zudem eigene Richtlinien im Unternehmen, die von allen Mitarbeitern unterzeichnet werden

SD Software-Design GmbH
Schwarzwaldstr. 21
79189 Bad Krozingen

Tel: +49 7633 80 69 311
Web: www.software-design.de
E-Mail: info@software-design.de

Registergericht Freiburg
HR-Nr: HRB 713955
Geschäftsführer: Daniel Kemen

müssen und Teil des Vertrages sind. Häufige fehlerhafte Eingaben von Passwörtern führen wenn technisch möglich zur temporären Sperrung des Zugangs.

2. Datenträgerkontrolle

Als Datenträger kommen ausschließlich Festplatten und portable Geräte zum Einsatz, die sich im Firmenbesitz befinden. Die Mitarbeiter sind angewiesen keine eigenen oder fremden Geräte zur Übertragung von Daten zu verwenden und Datenträger auch nicht zusammen mit privaten oder fremden Geräten zu verwenden. Ferner wird durch die Mitarbeiter sichergestellt, dass sich Datenträger und Verarbeitungsgeräte zu keiner Zeit unbeaufsichtigt und ungeschützt in öffentlich zugänglichen Räumen befinden. Werden Daten auf Datenträgern nicht mehr benötigt, werden diese nach Gebrauch vom Datenträger entfernt. Portable Datenträger (USB Sticks / CDs) werden nach Möglichkeit nicht für den Transport von Daten verwendet. Sollte ein Transport von Nöten sein, werden die zu transportierenden Daten gesondert gesichert (s.Transportkontrolle).

Die Datenträger werden so gekennzeichnet, dass kein Rückschluss auf deren Inhalt möglich ist.

Wird ein Datenträger nicht länger oder für andere Zwecke eingesetzt, wird dieser entweder softwareseitig durch eine fachkundige Person vollständig bereinigt, oder vor seiner Entsorgung durch physikalische Krafteinwirkung zerstört.

3. Speicherkontrolle

Auf Servern und Verarbeitungsgeräten im Unternehmen werden Logins und auch fehlerhafte Login-Versuche wo anwendbar protokolliert. Ferner werden wenn technisch sinnvoll für Eingaben und Veränderungen an den Dateisystemen selbst Protokolle erstellt. In relevanten Fällen wird zusätzlich auf Applikationsebene jede relevante Datenveränderung / Aktivität protokolliert.

4. Benutzerkontrolle

Benutzerzugriffe werden nach dem Need-to-Know-Prinzip vergeben und kontrolliert (s. Zugriffskontrolle). Der Zugriff auf das interne Netzwerk ist zusätzlich gesichert - für Besucher und Externe stehen eigene Geräte und ein eigenes getrenntes Gästenetzwerk zur Verfügung, damit es nicht zu Überschneidungen oder ungewollten Freigaben kommen kann.

SD Software-Design GmbH
Schwarzwaldstr. 21
79189 Bad Krozingen

Tel: +49 7633 80 69 311
Web: www.software-design.de
E-Mail: info@software-design.de

Registergericht Freiburg
HR-Nr: HRB 713955
Geschäftsführer: Daniel Kemen

5. Zugriffskontrolle

Berechtigungsgruppen und individuelle personen-, gruppen- oder gerätebezogene Zugänge regeln den Zugriff auf personenbezogene Daten im internen Netzwerk. Bei der Einstellung neuer Mitarbeiter und bei unregelmäßigen Prüfungen wird zudem überprüft, ob die Notwendigkeit für die Gewährung spezieller Zugriffe nach wie vor besteht, oder ob eine Anpassung möglich beziehungsweise erforderlich ist. Beim Ausstieg eines Mitarbeiters werden alle Zugänge zu unseren Systemen unmittelbar gesperrt.

Daten, die ausgedruckt vorgehalten werden (müssen), werden in verschließbaren Schränken aufbewahrt, deren Schlüssel oder Zugangscodes ausschließlich den Mitarbeitern zugänglich sind, die den Zugriff auf die Daten zur Erfüllung Ihres Vertrages benötigen.

Wird die Löschung von Daten von Betroffenen beantragt und ist die Löschung wegen geltender Aufbewahrungsfristen nicht möglich, wird der Zugriff auf die Daten auf den engsten Bearbeiterkreis eingeschränkt, damit eine weitere Verarbeitung, die nicht im Sinne der bestehenden Pflichten anfällt, ausgeschlossen wird.

Im Unternehmen und an den Servern sind Firewalls konfiguriert, die den Netzwerkverkehr filtern. Ferner wird auf vielen Verarbeitungsgeräten im Unternehmen, welche zum Verarbeiten personenbezogener Daten genutzt werden, Software eingesetzt, die alle eingehenden und ausgehenden Verbindungen gegen ein individuelles Regelset prüft und Genehmigungen für jede neuartige oder unbekannte Verbindungsart abfragt. So werden unbemerkte Hintergrund-Abfragen oder -Datenübertragungen blockiert. Hierzu regeln die internen IT-Richtlinien, wie Mitarbeiter sich hinsichtlich der Kontrolle von Zugriffen zu verhalten haben.

Von den Verarbeitungsgeräten auf denen wichtige Daten abgespeichert werden, werden regelmäßig Backups durchgeführt, die selbst wiederum nicht durch andere Mitarbeiter abgegriffen werden können, da diese über Passwörter / Verschlüsselungen gesichert werden.

Eine Fernwartung durch externe Dienstleister erfolgt ausschließlich in Ausnahmefällen und unter beständiger Aufsicht eines fachkundigen Mitarbeiters, um möglicherweise unbefugten Zugriff zu verhindern.

6. Übertragungskontrolle

Die Zugriffe auf Server und zentrale Systeme, die vom Unternehmen eingesetzt werden, werden wann immer technisch möglich über verschlüsselte Verbindungen vorgenommen. Für Systeme über die Dritten die Eingabe von Daten ermöglicht wird, wird ebenfalls stets eine Möglichkeit für einen verschlüsselten Zugriff bereitgestellt. Damit wir die Datenintegrität, die Authentizität und die Sicherheit vor fremden Zugriffen gewährleistet. Dazu kommen unter anderem SSH-Tunnel bzw. SSL gesicherte Verbindungen zum Einsatz.

SD Software-Design GmbH
Schwarzwaldstr. 21
79189 Bad Krozingen

Tel: +49 7633 80 69 311
Web: www.software-design.de
E-Mail: info@software-design.de

Registergericht Freiburg
HR-Nr: HRB 713955
Geschäftsführer: Daniel Kemen

7. Eingabekontrolle

Die eingesetzten Datenverarbeitungssysteme verfügen über umfangreiche Protokollfunktionen, die Änderungen an Daten revisionssicher protokollieren. Ferner kann über systemabhängig festgelegte und regelmäßige Archivierungen und Backups die Authentizität und Veränderung von Daten nachvollzogen werden.

8. Transportkontrolle

Werden Daten auf Datenträgern gespeichert und diese physikalisch transportiert sind diese stets passwortgeschützt bzw. verschlüsselt gespeichert. Eine interne Richtlinie regelt darüber hinaus den Umgang mit diesen Speichermedien mit den Mitarbeitern (s. Datenträgerkontrolle). Der Transport mittels USB Sticks oder andere portable Speicher mit personenbezogenen Daten sind im Unternehmen untersagt.

9. Wiederherstellbarkeit

Daten werden regelmäßig mittels Backups auf physikalisch getrennten Systemen an unterschiedlichen Standorten, die selbst wiederum gemäß der oben stehenden Richtlinien geschützt sind, gesichert, um einen Datenverlust zu verhindern. Je nach System und schwere des Ausfalls können so Teile des Systems oder komplette Systemabbilder wiederhergestellt werden. Auch der Einsatz des unter "Datenintegrität" genannten RAID Systems dient der Möglichkeit beim Ausfall einer einzelnen Festplatte weitere vollfunktionsfähige Festplatten zur Verfügung zu haben, die den letzten gültigen Datenbestand halten und direkt eingesetzt werden können.

10. Zuverlässigkeit

Die eingesetzten Systeme werden regelmäßig getestet, überprüft und aktualisiert. Beim Einsatz externer Systeme wird auf geeignete Garantien für eine regelmäßige Prüfung und Aktualisierung durch den Betreiber geachtet. Fehlermeldungen von Mitarbeitern oder Kunden werden schnellst möglich geprüft, kontrolliert und bei Notwendigkeit korrigiert. Vor der Einführung neuer Systeme, Tools oder Funktionen erfolgen ausgiebige Tests durch mehrere fachkundigen Mitarbeiter.

Die Backupprozesse werden dokumentiert und die Wiederherstellung einzelner Backups stichprobenartig getestet, um im Falle einer notwendigen Wiederherstellung gewohnte und funktionierende Abläufe zur Hand zu haben. Bei Fehlern im Backup-Prozess werden die zuständigen Mitarbeiter automatisch informiert.

SD Software-Design GmbH
Schwarzwaldstr. 21
79189 Bad Krozingen

Tel: +49 7633 80 69 311
Web: www.software-design.de
E-Mail: info@software-design.de

Registergericht Freiburg
HR-Nr: HRB 713955
Geschäftsführer: Daniel Kemen

11. Datenintegrität

Während die Übertragungskontrolle die Datenintegrität bei der Übertragung sicherstellt und die Speicher- bzw. Datenträgerkontrolle die Integrität der Daten auf den Speichermedien sicherstellt, wird die Integrität von Daten zusätzlich über redundante Backupsysteme sichergestellt, die unabhängig voneinander physikalisch getrennt laufen. Ferner werden auf Servern und zentralen Datenspeichern sofern sinnvoll anwendbar RAID Systeme eingesetzt, die das Spiegeln von Festplatten in Echtzeit ermöglichen. Dadurch wird jeder Datensatz zu jeder Zeit mehrfach erzeugt und vorgehalten um die Integrität des Speicherprozesses zu gewährleisten und bei Fehlfunktionen einer Festplatte korrekte Daten zu behalten.

12. Auftragskontrolle

Der Vertrag zur Auftragsverarbeitung sowie die AGB regeln explizit, in welchen Fällen und in welchem Umfang Daten verarbeitet werden dürfen. Die Mitarbeiter sind vertraglich daran gebunden manuelle Datenverarbeitung nur im Auftrag auszuführen. Wenn Aufträge telefonisch erteilt oder Auskünfte telefonisch angefordert werden, erfolgt eine Prüfung der Legitimität des Anrufers (z.B. über eine personenbezogene Support-PIN), bevor Aufträge angenommen oder Daten herausgegeben werden.

13. Verfügbarkeitskontrolle

Zentrale Datenspeicher und Softwarelösungen werden in Rechenzentren betrieben, die besondere Maßnahmen zur Gewährleistung von Verfügbarkeiten ergreifen. In den Rechenzentren sind eigene Notstromaggregate und Feuerlöschanlagen eingebaut, die vor einem Ausfall schützen. Auch verfügen die Rechenzentren über redundante Anbindungen, die im Falle des Ausfalls einzelner Verbindungen die Verfügbarkeit von Daten zusätzlich gewährleisten. Im Unternehmen selbst laufen ebenfalls physikalisch getrennte Systeme für Backups, die eine Verfügbarkeit im Falle eines Hardwareausfalls gewährleisten.

14. Trennbarkeit

Informationen, die für Verarbeitungsprozesse durch den Auftragnehmer verwendet werden (z.B. Anschrift für Rechnungserstellung, Ansprechpartner, etc.) werden getrennt abgespeichert, sofern die Zwecke keine Überschneidung oder sinnvolle bzw. notwendige gemeinsame Verfügbarkeitsanforderung ergeben. In allen anderen Fällen werden jeweils die Zwecke der erfassten Daten kenntlich gemacht. Die Daten können jederzeit getrennt von einander verwendet werden. Zusätzliche Informationen, die Benutzer freiwillig hinterlegen, um diese selbst zu verarbeiten oder verarbeiten zu lassen, werden für interne Zwecke nicht herangezogen.

SD Software-Design GmbH
Schwarzwaldstr. 21
79189 Bad Krozingen

Tel: +49 7633 80 69 311
Web: www.software-design.de
E-Mail: info@software-design.de

Registergericht Freiburg
HR-Nr: HRB 713955
Geschäftsführer: Daniel Kemen