soft-nrg Development GmbH
Karl-Hammerschmidt-Str. 40
85609 Dornach

Wir möchten Sie bitten,

- diese Seite mit Ihren Angaben zu vervollständigen,
- die Anlage 4 auszufüllen und
- auf Seite 1 bis 6 die Punkte zu prüfen und mit Unterzeichnung zu versehen.

Bitte senden Sie uns das gesamte Formular in zweifacher Ausfertigung per Post oder in einfacher Ausfertigung per E-Mail an vertrieb@soft-nrg.de.

Hiernach erhalten Sie ein von uns unterschriebenes Exemplar für Ihre Unterlagen.

Vielen Dank!

Ihre Angaben	
	Firma
	Straße und Hausnummer
	PLZ und Ort
	Vertreten durch (Vorname, Nachname)

Ich bestätige hiermit, dass ich den beigefügten Vertrag über die Auftragsverarbeitung personenbezogener Daten und dessen Anlagen, wie von der soft-nrg Development GmbH bereitgestellt, ohne Änderungen unterschrieben habe.

Ort, Datum

Unterschrift Auftraggeber

Vertrag über die Auftragsverarbeitung personenbezogener Daten

1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Auftragnehmer übernimmt die in Anlage 1 benannten Verarbeitungen, welche auf dem zwischen den Parteien bestehenden Vertrag und dessen Ergänzungen (im Folgenden „Hauptvertrag“) beruhen.

2.2 Dauer

Die Laufzeit dieses Vertrages richtet sich nach dem zwischen den Parteien bestehenden Hauptvertrag, sofern sich aus den Bestimmungen dieses Vertrages nicht darüberhinausgehende Verpflichtungen ergeben.

3 Art und Zweck der Verarbeitung

Art und Zweck der Verarbeitung und Kategorien der betroffenen Personen werden in Anlage 1 im jeweiligen Absatz benannt.

4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet.
Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, wurden schriftlich zur Vertraulichkeit verpflichtet.

(4) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden.

(5) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen.

(6) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer, den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(7) Auskünfte an Dritte oder den Betroffenen wird der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen leitet er unverzüglich an den Auftraggeber weiter.

(8) Der Auftragnehmer bestellt eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz, welche in Anlage 5 benannt wird.

(9) Die Auftragsverarbeitung erfolgt ausschließlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

5 Technische und organisatorische Maßnahmen

(1) Die in Anlage 2 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber mitzuteilen.

(3) Soweit beim Auftraggeber besondere Anforderungen an Sicherheitsmaßnahmen bestehen, hat er diese dem Auftragnehmer mitzuteilen. Soweit die getroffenen Maßnahmen mitgeteilten besonderen Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

(4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen getrennt werden.

(5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(6) Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung.

6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

(2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7 Unterauftragsverhältnisse

(1) Zurzeit sind die in Anlage 3 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

(2) Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung des Subunternehmers informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber hat das Recht, einer Subbeauftragung innerhalb von 2 Wochen mit Begründung schriftlich zu widersprechen. Erfolgt kein begründeter Widerspruch, gilt der Einsatz des Subunternehmers als genehmigt.

(3) Subunternehmern werden vertraglich mindestens Datenschutzpflichten auferlegt, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.

(4) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

(5) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

(6) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

(7) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.

(8) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8 Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort, zu kontrollieren.

(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung von mindestens 72 Stunden und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 18 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber festgestellte Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Die Mitteilung hat mindestens die Angaben nach Art. 33 Abs. 3 Datenschutz-Grundverordnung zu enthalten. Die korrekte Bewertung und Behandlung des Vorfalls obliegt allein dem Auftraggeber.

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur beauftragten Verarbeitung aufweisen.

(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10 Weisungen

(1) Dem Auftraggeber ist hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vorbehalten. Weisungen sind klar und eindeutig zu erteilen.

(2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 4. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

(3) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(4) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11 Beendigung des Auftrags

(1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben und sodann zu vernichten. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

(2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

(3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

(4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12 Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

13 Sonderkündigungsrecht

(1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

(2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen, in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

(3) Bei unerheblichen Verstößen gegen die Bestimmungen dieses Vertrages setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung berechtigt.

(4) Der Auftragnehmer ist zur außerordentlichen Kündigung von Hauptvertrag und dieser Vereinbarung berechtigt, sofern der Auftraggeber der Beauftragung eines Subunternehmers gem. 7 (1) dieses Vertrages widerspricht und keine Einigung erreicht werden kann.

(5) Die außerordentliche Kündigung ist innerhalb einer Ausschlussfrist von 2 Wochen zu erklären. Die Frist beginnt mit Kenntnis der zugrundeliegenden Tatsachen durch die zur Kündigung berechtigten Partei.

14 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

(2) Soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist, stellt der Auftraggeber den Auftragnehmer auf erste Anforderung von sämtlichen Ansprüchen Dritter frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftragnehmer erhoben werden.

(3) Eine zwischen den Parteien im Hauptvertrag zur Leistungserbringung vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas Anderes vereinbart.

15 Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

	soft-nrg Development GmbH
Firma	Firma
Unterschrift Auftraggeber	Unterschrift Auftragnehmer
	Dornach,
Ort, Datum	Ort, Datum

Anlage 1 – Angaben zur Verarbeitung

Onlinedienste

soft-net

Gegenstand	soft-net Online-Terminvereinbarung für Kunden des Auftraggebers
Aufgaben	Bereitstellung, Wartung und Betreuung von Onlinediensten
Zweck	Erfassung der Daten des Kunden, von deren Fahrzeugen, Abfragen und Abgleichen gewünschter Serviceleistungen und geplanter Termine, Erfassen und Speichern von Daten aus Benutzerverwaltung.
Art der personenbezogenen Daten	Es werden insbesondere folgende Datenkategorien und Daten verarbeitet: Kundendaten ▪ Anrede, Name, Vorname ▪ Adresse ▪ Telefonnummern ▪ E-Mail-Adresse ▪ KFZ-Kennzeichen ▪ Fahrzeugmodell ▪ Fahrgestellnummer (VIN) Mitarbeiterdaten ▪ Anrede, Name, Vorname Benutzerdaten ▪ Name, Vorname ▪ E-Mail-Adresse
Kategorien der betroffenen Personen	Kunden, Interessenten und Mitarbeiter des Auftraggebers

soft-agent

Gegenstand	soft-agent Webbasierte Online-Terminvereinbarung zur Unterstützung von Serviceabteilung und Callcenter
Aufgaben	Bereitstellung, Wartung und Betreuung von Onlinediensten
Zweck	Erfassung der Daten des Kunden, von deren Fahrzeugen, Abfragen und Abgleichen gewünschter Serviceleistungen und geplanter Termine, Erfassen und Speichern von Daten aus Benutzerverwaltung.
Art der personenbezogenen Daten	Es werden insbesondere folgende Datenkategorien und Daten verarbeitet: Kundendaten ▪ Anrede, Name, Vorname ▪ Adresse ▪ Telefonnummern ▪ E-Mail-Adresse ▪ KFZ-Kennzeichen ▪ Fahrzeugmodell ▪ Fahrgestellnummer (VIN) Mitarbeiterdaten ▪ Anrede, Name, Vorname Benutzerdaten ▪ Name, Vorname ▪ E-Mail-Adresse
Kategorien der betroffenen Personen	Kunden, Interessenten und Mitarbeiter des Auftraggebers

soft-messenger

Gegenstand	soft-messenger Versand von Benachrichtigungen per SMS und E-Mail
Aufgaben	Bereitstellung, Wartung und Betreuung von Onlinediensten
Zweck	Weiterleitung der Informationen und Kommunikation per SMS und E-Mail an Kunden des Auftraggebers
Art der personenbezogenen Daten	Es werden insbesondere folgende Datenkategorien und Daten verarbeitet: Kunden- und Kommunikationsdaten ▪ Mobiltelefonnummer ▪ Anrede, Name, Vorname ▪ E-Mail-Adresse ▪ Personenbezogene Inhalte der Korrespondenz Mitarbeiterdaten ▪ Anrede, Name, Vorname Benutzerdaten ▪ Name, Vorname ▪ E-Mail-Adresse
Kategorien der betroffenen Personen	Kunden, Interessenten und Mitarbeiter des Auftraggebers

soft-analytics

Gegenstand	soft-analytics Auswertungen anhand detaillierter Managementreports
Aufgaben	Bereitstellung, Wartung und Betreuung von Onlinediensten
Zweck	Erstellung von Auswertungen und Exporten von Kundendaten, deren Fahrzeugen, vereinbarten Terminen für Serviceleistungen und Rädereinlagerungen
Art der personenbezogenen Daten	Es werden insbesondere folgende Datenkategorien und Daten verarbeitet: Kundendaten ▪ Anrede, Name, Vorname ▪ Adresse ▪ Telefonnummern ▪ E-Mail-Adresse ▪ KFZ-Kennzeichen ▪ Fahrzeugmodell ▪ Fahrgestellnummer (VIN) Mitarbeiterdaten ▪ Anrede, Name, Vorname Benutzerdaten ▪ Name, Vorname ▪ E-Mail-Adresse
Kategorien der betroffenen Personen	Kunden, Interessenten und Mitarbeiter des Auftraggebers

Dienstleistungen

Gegenstand	Betreuung und Schulung
Zweck	Erbringung von Leistungen wie ▪ Wartung, Anwenderunterstützung via E-Mail, Telefon und Fernwartung, ▪ Schulung und Training von Anwendern, wobei der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.
Art der personenbezogenen Daten	Es werden insbesondere folgende Datenkategorien und Daten verarbeitet: Kundendaten ▪ Anrede, Name, Vorname ▪ Adresse ▪ Telefonnummern ▪ E-Mail-Adresse ▪ KFZ-Kennzeichen ▪ Fahrzeugmodell ▪ Fahrgestellnummer (VIN) Mitarbeiterdaten ▪ Anrede, Name, Vorname ▪ Personalnummer ▪ Eintritts- und Austrittsdatum Benutzerdaten ▪ Name, Vorname ▪ E-Mail-Adresse
Kategorien der betroffenen Personen	Kunden, Interessenten und Mitarbeiter des Auftraggebers

Anlage 2 – Technische und organisatorische Maßnahmen

Nachstehend wird beschrieben, welche technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt sind. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Unternehmen verarbeiteten Informationen.

Die Struktur orientiert sich nach der international anerkannten Norm DIN ISO/IEC 27002.

Organisation der Informationssicherheit

Die Führungskräfte der soft-nrg Development GmbH sind in ihrer Organisationseinheit für die vollständige Umsetzung der Grundsätze der IT-Sicherheit und für die Erfüllung der an sie gestellten IT-Sicherheitsaufgaben verantwortlich.

Informationssicherheitsrollen und -verantwortlichkeiten sind in dem Konzept IT-Sicherheitsorganisation definiert. Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche sind getrennt, um die Möglichkeiten zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch der Werte unseres Unternehmens zu reduzieren.

Wir verfügen über ein Verfahren, das festlegt, wann und durch wen relevante Behörden benachrichtigt und erkannte Datenschutz- und Informationssicherheitsvorfälle rechtzeitig gemeldet werden.

Auch pflegen wir laufenden Kontakt zu speziellen Interessensgruppen, um über Änderungen und Verbesserungen im Bereich Datenschutz und Informationssicherheit informiert zu sein.

In unseren Projekten ist Datenschutz und Datensicherheit Bestandteil aller Phasen unserer Projektmethodik.

Durch unsere jeweiligen Richtlinien und Prozesse zur Telearbeit und der Nutzung von Mobilgeräten, stellen wir den Datenschutz und die Datensicherheit auch in diesen Bereichen sicher.

Personalsicherheit

Wir haben unsere Mitarbeiter sorgsam ausgewählt und ihre Eignung für ihre Rolle im Unternehmen überprüft. Ihre Verantwortlichkeiten haben wir in Funktionsbeschreibungen festgelegt und gleichen regelmäßig ab, ob die Mitarbeiter diesen entsprechen. Vor Beginn ihrer Anstellung unterschreiben alle Mitarbeiter eine Vertraulichkeits- sowie Datenschutzvereinbarung, die über die Beendigung des Beschäftigungsverhältnisses hinaus gilt. Die Mitarbeiter werden im Bereich Datenschutz- und Datensicherheit nachweislich geschult.

In einem dokumentierten Prozess für die Zeit vor, während und nach Beendigung des Beschäftigungsverhältnisses stellen wir sicher, dass personenbezogene Daten geschützt und die Datensicherheit gewährleistet ist. Diese beinhaltet auch Maßregelungen für den Fall eines Datenschutzverstoßes.

Verwaltung der Werte

Sämtliche Werte (wie z.B. Betriebsmittel, Wechseldatenträger, Notebooks) und Informationen, die mit personenbezogenen Daten in Zusammenhang stehen, werden von uns inventarisiert und gepflegt.

Wir haben zum Schutz dieser Werte Verantwortliche festgelegt, die für den Lebenszyklus eines Wertes zuständig sind.

Es wurden dokumentierte Regeln für den zulässigen Gebrauch unserer Werte aufgestellt. Die Rückgabe erfolgt dokumentiert.

Unsere Informationen und Daten werden anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung klassifiziert und gekennzeichnet.

Diesem Klassifizierungsschema entsprechend, haben wir dokumentierte Verfahren für die Handhabung unserer Werte, insbesondere auch unserer Wechseldatenträger, entwickelt und umgesetzt. Wir verfügen über einen dokumentierten und geregelten Prozess zum Transport von Datenträgern, um diese vor unbefugtem Zugriff, Missbrauch oder Verfälschung zu schützen.

Nicht mehr benötigte Datenträger entsorgen wir sicher, unter Anwendung eines dokumentierten Verfahrens und verpflichteter zertifizierter Dienstleister.

Zugriffssteuerung

Wir verfügen über geregelte und dokumentierte Maßnahmen, die sicherstellen, dass berechtigte Personen nur auf solche personenbezogenen Daten Zugriff erhalten, für die sie die Befugnis zur Einsichtnahme und zur Verarbeitung besitzen.

Berechtigungen zum Zugriff auf IT-Systeme werden über ein geregeltes Verfahren auf der Grundlage eines dokumentierten und restriktiven Berechtigungskonzepts vergeben. Den Zugang zu Netzwerken und Netzwerkdiensten haben wir geregelt und umgesetzt.

Es ist sichergestellt, dass nur befugte Benutzer Zugang zu Systemen und Diensten haben und unbefugter Zugang unterbunden wird, insbesondere besteht ein formaler Prozess für die Registrierung und Deregistrierung von Benutzern, der die Zuordnung von Zugangsrechten zu ermöglicht.

Unsere administrativen Rechte erteilen wir eingeschränkt und gesteuert.

Wir verfügen über einen dokumentierten und geregelten Prozess über den Umgang mit Passwörtern. Ist- und Soll-Zustand von Benutzerzugangsrechten werden regelmäßig abgeglichen. Bei Bedarf werden diese entzogen oder angepasst.

Wir schränken den Zugriff auf unsere Daten bedarfsgerecht ein und steuern den Zugang auf unsere Systeme und Anwendungen durch ein sicheres Anmeldeverfahren. Wir verwenden ein System zur Nutzung sicherer und starker Kennwörter.

Der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, ist eingeschränkt und streng überwacht.

Kryptographie

Der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information ist sichergestellt. Zu diesem Zwecke haben wir eine Richtlinie über den Einsatz von Kryptographischen Maßnahmen im Unternehmen implementiert, die auch die Verwaltung von kryptographischen Schlüsseln umfasst und dem Schutzbedarf angemessen ist.

Physische und umgebungsbezogene Sicherheit der Verwaltungsräume

Wir haben dokumentierte und geregelte Maßnahmen getroffen, die verhindern sollen, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet oder genutzt werden. Diese umfassen unter anderem:

- Die Geschäftsräume liegen in einem Bürogebäude und werden exklusiv genutzt.
- Der zentrale Eingang wird überwacht.
- Türen zu Sicherheitsbereichen sind stets geschlossen. Diese können nur von berechtigten Personen betreten werden.
- Besucher oder externe Dienstleister werden individuell eingelassen.
- Der Brandschutz wird beachtet.
- Es sind Sicherheitsbereiche vorhanden, zu denen nur eigens hierzu Berechtigte Zutritt erhalten.
- IT-Räume sind separat verschlossen und nur durch Berechtigte zu öffnen.
- Versorgungseinrichtungen werden vor Stromausfällen und Störungen geschützt.
- Die Sicherheit der Verkabelung wird beachtet.
- Die Instandhaltung von Systemen wird geplant und umgesetzt.
- Das Entfernen und Änderungen von Systemen und Informationen erfolgt geregelt.
- Die Sicherheit von Systemen außerhalb der Geschäftsräume wird beachtet.
- Die Entsorgung oder Wiederverwendung von Betriebsmitteln erfolgt geregelt.
- Richtlinien für Clean Desk und Bildschirmsperren werden umgesetzt.

Betriebssicherheit

Wir verfügen über geregelte und dokumentierte Maßnahmen, um einen ordnungsgemäßen und sicheren Betrieb von informations- und datenverarbeitenden Einrichtungen sicherzustellen. Diese umfassen u.a. die Steuerung im Falle einer Änderung an den informationsverarbeitenden Einrichtungen, als auch eine Steuerung und regelmäßige Messung unserer Kapazitäten und Ressourcen, um die Verfügbarkeit der erforderlichen Systemleistung sicherzustellen. So werden z.B. unter anderem folgende Werte laufend aktuell überwacht:

- Festplattenstatus und verfügbarer Speicher
- Raid-Status
- Dienste und Status aller virtuellen Maschinen
- Fehlerhafte Anmeldeversuche

- Speicherbelegung der Storages und Hauptspeicher
- Auslastung Ethernet in Kbit/s und Mbit/s
- Anzahl der RDP-Sessions der einzelnen Terminal-Server
- Durchsatz und Auslastung der Firewall
- Erreichbarkeit aller Server von außen
- Erreichbarkeit und Durchsatz der Switche

Ein geschütztes Verfahren zur Datensicherung wurde von uns implementiert und ist dokumentiert.

Standardwartungsfenster sind definiert. Zusätzlich notwendige Fenster werden vorab angekündigt.

In unserem Unternehmen ist es essentiell, Entwicklungs-, Test- und Betriebsumgebungen voneinander zu trennen, sodass wir ein besonderes Augenmerk hierauf haben.

Maßnahmen zur Erkennung, Vorbeugung und Wiederherstellung zum Schutz von Schadsoftware wurden getroffen und werden regelmäßig aktualisiert.

Wir verfügen über eine zentral überwachte und geschützte Ereignisprotokollierung und haben für den Fall der Speicherung sensibler personenbezogener Daten Maßnahmen zum Schutz der Privatsphäre getroffen. Sämtliche Protokollierungseinrichtungen und Protokollinformationen, einschließlich Administratoren und Bedienerprotokolle sind vor Manipulation und unbefugtem Zugriff geschützt.

Die Synchronisation unserer Uhren erfolgt zentral mit einer einzigen Referenzzeitquelle.

Wir verfügen über ein zentrales Verfahren zur gesteuerten Installation von Software auf Systemen in unserem Unternehmen.

Es besteht eine Aufstellung unserer technischen Werte und eine geregelte, dokumentierte Handhabung für den Fall einer technischen Schwachstelle, die u.a. unser Patchmanagement mit definierten Verantwortlichkeiten umfasst.

Regelungen für die Einschränkungen von Softwareinstallationen sind von uns zentral implementiert.

Im Falle einer Auditprüfung unserer Informationssysteme haben wir Maßnahmen festgelegt, die Störungen der Geschäftsprozesse soweit wie möglich minimieren.

Kommunikationssicherheit

Die Sicherheit unserer in Netzwerken und Netzwerkdiensten gespeicherten personenbezogenen Daten und Informationen ist unumgänglich. Daher haben wir dokumentierte Maßnahmen eingesetzt, die unsere Netzwerke verwalten, steuern und sichern.

Informationsdienste, Benutzer und Informationssysteme werden bedarfsgerecht voneinander getrennt gehalten.

Wir verfügen über Richtlinien und Verfahren für die Informations- und Datenübertragung, sowie die Vereinbarungen zur Informationsübertragung an externe Stellen.

Unsere elektronische Nachrichtenübermittlung wird angemessen geschützt. So haben wir unter anderem Maßnahmen zum Schutz der Nachrichten vor unbefugtem Zugriff, vor Veränderung oder Denial of Service getroffen, die dem von der Organisation übernommenen Klassifizierungsschema entsprechen.

Um unsere Daten zu schützen, schließen wir bedarfsgerechte Vertraulichkeits- oder Geheimhaltungsvereinbarungen ab, die wir regelmäßig überprüfen.

Anschaffung, Entwicklung und Instandhaltung von Systemen

Es ist sichergestellt, dass Daten- und Informationssicherheit ein fester Bestandteil über den gesamten Lebenszyklus unserer Systeme sind. Dies beinhaltet auch die Anforderungen an und die Sicherung von Informationssystemen, die Dienste über öffentliche Netze bereitstellen. Der Schutz der Transaktionen bei Anwendungsdiensten erfolgt bedarfsgerecht. Zudem haben wir ein Verfahren zur Verwaltung von Systemänderungen eingerichtet, um die Integrität des Systems, der Anwendungen und der Produkte von den frühen Entwurfsphasen bis zu allen später anfallenden Wartungsarbeiten sicherzustellen. Bei Änderungen an Betriebsplattformen werden geschäftskritische Anwendungen überprüft und getestet, um sicherzustellen, dass es keine negativen Auswirkungen auf die Organisationssicherheit auch der Kundenanwendungen gibt. Wir verfügen über einen gesteuerten Prozess zur Analyse, der Entwicklung und der Pflege sicherer IT Systeme.

Für neue Informationssysteme, Aktualisierungen und neue Versionen sind Abnahmetestprogramme und dazugehörige Kriterien festgelegt. Unsere Testdaten werden sorgfältig ausgewählt, geschützt und gesteuert.

Lieferantenbeziehungen

Wir wählen unsere Lieferanten im Vorfeld sorgsam aus und überprüfen ihre Geeignetheit hinsichtlich der Wahrung des Daten- und Informationssicherheitsschutzes.

Dokumentierte Vereinbarungen sichern den Schutz und die Geheimhaltung unserer Werte und Daten. Die Lieferanten werden verpflichtet, technisch-organisatorische Maßnahmen zu treffen, um dies zu gewährleisten.

Es besteht eine reglementierte und benutzerdefinierte Zugriffsberechtigung auf die für den jeweiligen Lieferanten zwingend benötigten Werte und Daten.

Lieferanten dürfen weitere Lieferanten lediglich mit unserer Zustimmung beauftragen, um eine sichere Lieferkette zu gewährleisten.

Regelmäßig führen wir eine Überprüfung der Datenschutz- und Datensicherheitsmaßnahmen unserer Lieferanten durch, um das vereinbarte Niveau aufrecht zu erhalten. Auch die zugewiesenen Berechtigungen unterliegen einer ständigen dokumentierten Kontrolle.

Nach Beendigung des Lieferantenverhältnisses sind diese verpflichtet, die von uns erhaltenen Daten und Werte zu vernichten. Zudem gilt die Wahrung der Geheimhaltungspflicht unbegrenzt.

Handhabung von Informationssicherheits- und Datenschutzereignissen

Unser Unternehmen verfügt über einen geregelten dokumentierten Prozess für die Handhabung von Informationssicherheits- und Datenschutzvorfällen, um diesbezüglich eine konsistente und wirksame Herangehensweise zu gewährleisten. Die Mitarbeiter sind angehalten, sämtliche Datenschutz- und Sicherheitsereignisse unverzüglich zu melden und werden diesbezüglich regelmäßig geschult. Wir haben ein Meldesystem installiert, das Ereignisse an ein Interventionsteam weitergeleitet, um eine schnelle Reaktion zu gewährleisten. Sämtliche Ereignisse werden dokumentiert, klassifiziert und bewertet. Das implementierte Interventionsteam hat genaue Vorgaben, wie auf ein Ereignis zu reagieren ist.

Zusammen mit der Geschäftsführung werden regelmäßig Verbesserungsmaßnahmen besprochen und umgesetzt, die sich aus den Erkenntnissen und den gesammelten Beweisen eines Ereignisses ergeben.

Informationssicherheitsaspekte beim Business Continuity Management

Im Rahmen der Informationssicherheit wird die vorgesehene Verfügbarkeit von Systemen eigens bewertet und dokumentiert. Aus den Anforderungen leiten wir die technischen und organisatorischen Vorgaben, wie redundante Systeme/Anbindungen oder entsprechende Planungen ab und setzen diese konsequent und gesteuert um. Ein übergreifender Notfallplan bildet den Rahmen bezüglich der entsprechenden Handlungsanweisungen für ausgewählte dokumentierte Notfallszenarien. Laufende aktualisierte Übungspläne für die Erprobung der eingesetzten Maßnahmen und die Dokumentation der Durchführung entsprechender Tests runden das Notfallmanagement ab.

Compliance

Wir haben alle relevanten gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen sowie das Vorgehen unseres Unternehmens zur Einhaltung dieser Anforderungen bestimmt, dokumentiert und halten diese auf dem neuesten Stand.

Auch wurden angemessene Verfahren umgesetzt, mit denen die Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen mit Bezug auf geistige Eigentumsrechte und der Verwendung von urheberrechtlich geschützten Softwareprodukten sichergestellt ist.

Entsprechend der gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen schützen wir Aufzeichnungen und personenbezogene Daten bedarfsgerecht. Jährliche Tätigkeitsberichte des Datenschutzbeauftragten dokumentieren die ergriffenen Maßnahmen.

Wir beachten hierfür die Regelungen Kryptographischer Maßnahmen.

Um den Schutz unserer Informationen und Daten sicher zu stellen, erfolgt regelmäßig eine unabhängige Überprüfung unseres Informationssicherheit- und Datenschutzniveaus, unserer Sicherheits- und Datenschutzrichtlinien, sowie die Einhaltung von technischen Vorgaben.

Anlage 3 – Zugelassene Subunternehmer

Onlinedienste

Firma, Adresse	Leistungen/Zweck
softNRG srl str. Simion Barnutiu nr. 69 ap. 20-21 300303 Timişoara RUMÄNIEN	Wartung/3rd Level Support der Applikationen SOFT-SOLUTIONS und deren Datenbanken Wartung/Support der Onlinedienste

Online-Seminare

Firma, Adresse	Leistungen/Zweck
LogMeIn, Inc. 333 Summer Street Boston, MA 02210 USA https://www.logmeininc.com/de/gdpr/gdpr-compliance	Bereitstellung eines Onlinedienstes für die Organisation und Durchführung von Schulungen

Rechenzentrum – Colocation

Firma, Adresse	Leistungen
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Standort: Nürnberg ISO 27001 Zertifikat siehe https://www.hetzner.de/unternehmen/downloads	Colocation Webhosting

Anlage 4 – Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

Weisungs- und kontrollberechtigte Personen beim Auftraggeber

Zuständige Weisungsempfänger beim Auftragnehmer
Herr Dedes Lionis, Tel. +49 89 452280-456, dedes.lionis@soft-nrg.de Herr Markus Zipfer, Tel. +49 89 452280-540, markus.zipfer@soft-nrg.de

Anlage 5 – Kontaktdaten des Datenschutzbeauftragten

Als externer Datenschutzbeauftragter ist bestellt:

Herr Michael Weiß
activeMind AG
Potsdamer Str. 3
80802 München
dsb@soft-nrg.de

Er wird durch einen weiteren Mitarbeiter der activeMind AG vertreten.