Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO

zwischen

Südwestdeutsche Stromhandels GmbH
Eisenhutstraße 6
72072 Tübingen

- nachstehend Auftragnehmer genannt -

und

- nachstehend Auftraggeber genannt -

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes (bitte ankreuzen)

☐ Portfolio-Management einschließlich Handel und Bilanzkreismanagement – Erdgas

☐ Portfolio-Management einschließlich Handel und Bilanzkreismanagement – Strom

☐ Energiedatenmanagement einschließlich Metering, Kommunikation und/oder Abrechnung - Netz Erdgas

☐ Energiedatenmanagement einschließlich Metering, Kommunikation und/oder Abrechnung - Netz Strom

☐ Energiedatenmanagement - Vertrieb Erdgas

☐ Energiedatenmanagement - Vertrieb Strom

☐ Energiewirtschaftliche Beratung

☐ Kaufm. Betriebsführung für Windparks

☐ Einsatz der „Datenweiche“ (B2B by Practice zur Weiterleitung von MSCONS/UTILMD-E06)

☐ Einsatz der Software SWS-Connect

Die ausführliche Beschreibung des Auftragsumfangs ist Bestandteil der Leistungsvereinbarung.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags

Die Laufzeit ist in der Leistungsvereinbarung festgelegt.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Umfang, Art und Zweck der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus der jeweiligen Leistungsvereinbarung.

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

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. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

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

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind:

.....
(Vorname, Name, Organisationseinheit, Telefon, eMail)

Weisungsempfänger beim Auftragnehmer sind:

Die Kontaktdaten können auf der Internetseite

https://www.suedweststrom.de/unternehmen/kontakt.html

abhängig vom jeweiligen Auftragsumfang entnommen werden.

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

Die Überprüfung der technischen und organisatorischen Maßnahmen erfolgt jährlich durch die Datenschutzbeauftragte.

Das Ergebnis der Kontrollen ist zu dokumentieren.

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).

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.
Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Der Auftragnehmer gewährleistet die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeiten - 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.

Wenn und soweit der Auftragnehmer im Zusammenhang mit der Verarbeitung von Daten eine Anfrage einer Aufsichtsbehörde oder sonstigen zuständigen Stelle erhält, hat er den Auftraggeber unverzüglich zu informieren und die Anfrage unverzüglich an den Auftraggeber weiterzuleiten.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO und des BDSG bekannt sind.

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO).

Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragnehmer ist als Beauftragte für den Datenschutz bestellt:

Frau Sonja Holzherr,
shQ Consulting, Pfeiferstrasse 32, 72108 Rottenburg
Tel: +49 (0)7472 2059782 Mobil: +49 (0) 1738127473
eMail: sonja.holzherr@shq-consulting.de

Der Auftragnehmer unterhält eine Datenschutzorganisation, die den Nachweispflichten aus Art. 5 Abs. 2 DSGVO genügt und insbesondere die Anforderungen an eine datenschutzkonforme Gestaltung der Datenverarbeitung gem. Art. 25 DSGVO erfüllt. Auf Anfrage des Auftraggebers weist der Auftragnehmer das Vorhandensein der Datenschutzorganisation in geeigneter Weise nach.
Insbesondere hat der Auftragnehmer ein internes Meldesystem vorzuhalten, das dem Auftraggeber die Einhaltung der Meldefrist aus Art. 33 DSGVO ermöglicht.

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen: Der Auftragnehmer überprüft die Subunternehmer auf die Einhaltung der Pflichten und die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen zur Datensicherung regelmäßig (alle 1 bis 3 Jahre schriftlich, ggf. per E-Mail), entsprechend der Sensibilität der personenbezogenen Daten.

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer die in Anlage 1 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt: Die Risikobewertung erfolgt jährlich durch die Datenschutzbeauftragte.

Das im Anhang 2 beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

Folgendes Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt:
Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. *oder* datenschutzgerecht zu löschen bzw. zu vernichten oder vernichten zu lassen.

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Vergütung

Die Vergütung ist in der Leistungsvereinbarung geregelt.

11. Haftung

Auf Art. 82 DS-GVO wird verwiesen.

12. Garantien

Der Auftragnehmer garantiert, dass

- er eine angemessene Datenschutzorganisation unterhält.
- die Umsetzung der technisch-organisatorischen Maßnahmen den Anforderungen der DSGVO entspricht.
- eine ordnungsgemäße Beauftragung von Subunternehmern durchgeführt wurde.

Der Auftragnehmer wird geeignete Nachweise für die Einhaltung dieser Vorgaben erbringen. Als Nachweis können Zertifikate und Prüfnachweise Dritter dienen.

13. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten 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.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

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

_____	_____
Ort, Datum Auftraggeber	Ort, Datum Auftragnehmer

Anlage 1 Liste der eingesetzten Subunternehmer

Anlage 2: Beschreibung der technischen und organisatorischen Maßnahmen

Anlage 3: Art. 82 DS-GVO

Anlage 1:
Liste der eingesetzten Subunternehmer

Name des Subunternehmers	Anschrift	Auftragsinhalt
Internett GmbH	Richard-Wagner-Strasse 14-16 66111 Saarbrücken	Umfängliches Hosting der Server und Managed-Services der Infrastruktur (Email, Serverführung, Sicherungen, Sicherheit, Monitoring, Support)
DiCentral GmbH	Fraunhoferstrasse 9 85737 Ismaning	Software-Hersteller elektronischer Datenaustausch (EDI)
Bunte Büffel GmbH	Fiduciastraße 6 76227 Karlsruhe	Support Homepage
Klafka & Hinz Energie-Informations-Systeme GmbH	Weststraße 54 D-52074 Aachen	Software-Hersteller EDM-System, Support der Software
Medialine enterprise IT solutions GmbH	Zehntenhofstrasse 5b 65201 Wiesbaden	Support CRM-System und DMS
Znuny GmbH	Marienstrasse 11 10117 Berlin	Software-Hersteller Ticket-System, Support der Software
Amazon Web Services Inc.	Marcel-Breuer-Str. 12 80807 München	Bereitstellen von Web-Services und Hosting
Detect Value AG	Wiesenstraße 4 69190 Walldorf	Support BI Software

Anlage 2:
Beschreibung der technischen und organisatorischen Maßnahmen

Datensicherungsmaßnahmen

1. **<u>Zugangskontrolle</u>**
   Maßnahmen zur Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte

   - Automatisches Zugangskontrollsystem am Standort Eisenhutstraße (Der Zutritt zu den Räumlichkeiten in denen personenbezogene Daten verarbeitet werden, ist nur mittels der entsprechenden Chipkarte möglich.)
   - Über den Aufzug kann die Stockwerksauswahl nur über die Chipkarte erfolgen
   - Jedes Büro ist abschließbar.
   - Sicherheitsschlösser
   - Schlüsselregelung (protokollierte Schlüsselausgabe)
   - Protokollierung der Besucher
   - Personenkontrolle am Empfang durch eigenes Personal
   - Sorgfältige Auswahl von Wachpersonal
   - Chipkarten-/Transponder-Schließsystem
   - Videoüberwachung der Zugänge
   - Sorgfältige Auswahl von Reinigungspersonal
   - Tragepflicht von Berechtigungsausweisen

2. **<u>Datenträgerkontrolle</u>**
   Maßnahmen zur Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern

   - Es werden keine Datenträger für die Auftragsabwicklung verwendet.

3. **<u>Speicherkontrolle</u>**
   Maßnahmen zur Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten

   - DIN EN ISO 27001 zertifiziertes Rechenzentrum
   - Die Software-Systeme, die Möglichkeiten haben, personenbezogene Daten abzuspeichern, sind durch System/Benutzer-Berechtigungen vor unbefugten Eingaben geschützt.
   - Änderungen/Löschungen werden protokolliert – diese Audit-Tabellen sind geschützt und nur Administratoren zugänglich.
   - Schnittstellendateien, die personenbezogene Daten beinhalten, werden in einem unseren EDM-Systemen anonymisiert verarbeitet (Adressdaten sind mit ‚X' überschrieben).

4. <u>Benutzerkontrolle</u>

Maßnahmen zur Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte

- DIN EN ISO 27001 zertifiziertes Rechenzentrum
- Zuordnung von Benutzerrechten
- Passwortvergabe (schriftliche Passwortrichtlinie)
- Authentifikation von Benutzername / Passwort
- Zwei-Faktor-Authentisierung bei Systemanmeldungen von extern (falls ein User sich physisch nicht im Unternehmen befindet)
- Schlüsselregelung
- Protokollierung der Besucher
- Einsatz von Intrustion-Detection-Systemen
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Erstellen von Benutzerprofilen
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Sicherheitsschlösser
- Personenkontrolle am Empfang
- Einsatz von zentraler Smartphone-Administrations-Software
- Einsatz einer Software-Firewall

5. <u>Zugriffskontrolle</u>

Maßnahmen, die gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben

- DIN EN ISO 27001 zertifiziertes Rechenzentrum
- Berechtigungskonzept (Das Berechtigungskonzept ist dokumentiert und die Anzahl der Systemadministratoren, die auf die Protokollierungen Zugriff haben, ist auf ein Minimum begrenzt.)
- Anzahl von Administratoren auf das „Notwendigste“ reduziert
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Einsatz von datenschutzgerechten Aktenvernichtern bzw. Dienstleistern mit Zertifikat
- Verwaltung der Rechte durch Systemadministrator
- Passwortrichtlinie inkl. Passwortlänge und Fristen für den Passwortwechsel

6. <u>Übertragungskontrolle</u>

Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können

- DIN EN ISO 27001 zertifiziertes Rechenzentrum
- Einrichtung von Standleitungen bzw. VPN-Tunneln
- E-Mail-Verschlüsselung entsprechend gesetzlicher Vorgaben
- Nur im Webportal: Dokumentation der Empfänger von Daten und Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

7. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind

- DIN EN ISO 27001 zertifiziertes Rechenzentrum
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können

8. Transportkontrolle

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden

- Ein Transport von Datenträgern findet grundsätzlich nicht statt, da keine Datenträger für die Auftragsabwicklung verwendet werden.

Für die Übermittlung personenbezogen Daten werden folgende Sicherungsmaßnahmen ergriffen:

- Einrichtung von Standleitungen bzw. VPN-Tunneln
- E-Mail-Verschlüsselung
- Nur im Webportal: Dokumentation der Empfänger von Daten und Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

9. Wiederherstellbarkeit

Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können

- DIN EN ISO 27001 zertifiziertes Rechenzentrum
- Regelmäßige Erstellung von Datensicherungen
- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- Testen von Datenwiederherstellung
- Erstellen eines Backup- & Recoverykonzeptes

10. Zuverlässigkeit

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden

- DIN EN ISO 27001 zertifiziertes Rechenzentrum
- Aktives und passives Monitoring der Systeme auf diversen Ebenen:
- Hardware-Monitoring durch Hoster
- VMWare-Monitoring durch Hoster
- Anwendungsmonitoring durch Fachabteilungen und IT durch automatisches Alerting in Prozessfehlerfällen oder Über/Unterschreitung von Grenzen.
- Einsatz Nagios, VisualCron, Powershell

11. Datenintegrität

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können

- DIN EN ISO 27001 zertifiziertes Rechenzentrum
- Der Großteil der personenbezogenen Daten ist in Datenbanken abgelegt, die durch referentielle Integritäten die Datenintegrität gewährleisten können.
- Alle Systeme werden täglich gesichert und können wieder aufgebaut werden.
- Neue Software oder Versionen werden in Teststellungen getestet um solch ein Fehlverhalten zu vermeiden.

12. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

- Der Auftragsinhalt ist schriftlich in der Leistungsbeschreibung beschrieben
- Zwischen Auftraggeber und Auftragnehmer wird ein Vertrag zur Auftragsverarbeitung abgeschlossen
- DIN EN ISO 9001:2015 zertifiziertes Unternehmen

13. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind

- DIN EN ISO 27001 zertifiziertes Rechenzentrum
- Regelmäßige Erstellung von Datensicherungen
- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- Unterbrechungsfreie Stromversorgung (USV)
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Testen von Datenwiederherstellung
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Backup- & Recoverykonzeptes

14. Trennbarkeit

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können

- DIN EN ISO 27001 zertifiziertes Rechenzentrum
- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Erstellung eines Berechtigungskonzeptes
- Festlegung von Datenbankrechten
- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem

Anlage 3:
Art. 82 DS-GVO

1. Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

2. Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

3. Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

4. Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.

5. Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

6. Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen, die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.