Vertrag über die Auftragsverarbeitung

zwischen

Firma: Hier den Text eingeben

Strasse: Hier den Text eingeben

PLZ: Hier den Text ein Ort: Hier den Text eingeben

(nachfolgend „**Auftraggeber“**)

und

E-Charge Pay by K3S GmbH
Rheinpromenade 2
40789 Monheim
Deutschland

(nachfolgend „**Auftragnehmer“**)

(nachfolgend einzeln oder gemeinsam „**Partei“** oder „**Parteien“**)

Inhaltsverzeichnis

ABSCHNITT I

1. Zweck und Anwendungsbereich

1.1 Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.

1.2 Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

1.3 Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

1.4 Die Anhänge I bis IV sind Bestandteil der Klauseln.

1.5 Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

1.6 Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

2. Unabänderbarkeit der Klauseln

2.1 Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

2.2 Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

3. Auslegung

3.1 Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

3.2 Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

3.3 Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

4. Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

ABSCHNITT II

PFLICHTEN DER PARTEIEN

5. Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

6. Pflichten der Parteien

6.1 Weisungen

6.1.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann

während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

6.1.2 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die der Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

6.2 **Zweckbindung**

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

6.3 **Dauer der Verarbeitung personenbezogener Daten**

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet

6.4 **Sicherheit der Verarbeitung**

6.4.1 Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung

6.4.2 Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

6.5 **Sensible Daten**

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

6.6 **Dokumentation und Einhaltung der Klauseln**

6.6.1 Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

6.6.2 Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

6.6.3 Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

6.6.4 Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

6.6.5 Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

6.7 Einsatz von Unterauftragsverarbeitern

6.7.1 Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 4 Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

6.7.2 Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

6.7.3 Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

6.7.4 Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

6.7.5 Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder

zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

6.8 **Internationale Datenübermittlung**

6.8.1 Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

6.8.2 Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 6.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

7. Unterstützung des Verantwortlichen

7.1 Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

7.2 Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben 6.1.1 und 6.1.2 befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

7.3 Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 7.2 zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

7.3.1 Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

7.3.2 Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutzfolgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

7.3.3 Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

7.3.4 Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679

7.4 Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

8. Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

8.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

8.1.1 bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten

führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

8.1.2 bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

8.1.2.1 die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

8.1.2.2 die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

8.1.2.3 die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

8.2 Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

8.3 **Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten**

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

8.3.1 eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

8.3.2 Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

8.3.3 die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

8.4 Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

8.5 Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III

SCHLUSSBESTIMMUNGEN

9. Verstöße gegen die Klauseln und Beendigung des Vertrags

Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

9.1 Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

9.1.1 der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

9.1.2 der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

9.1.3 der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

9.2 Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 6.1.2 verstoßen.

9.3 Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Hier den Text eingeben , den Hier den Text eingebe

Ort

_____

Unterschrift Auftraggeber

Hier den Text eingeben Hier den Text eingeben

Name Funktion des Unterzeichners

Monheim am Rhein , den Hier den Text eingebe

_____

Unterschrift Auftragnehmer

Kai Schmidt Geschäftsführer

ANHANG I

Liste der Parteien

Verantwortlicher

Name:	Hier den Text eingeben
Anschrift:	Hier den Text eingeben
Name:	Hier den Text eingeben
Funktion:	Hier den Text eingeben
Email:	Hier den Text eingeben
Telefon:	Hier den Text eingeben

Hier den Text eing

Beitrittsdatum

Unterschrift

Auftragsverarbeiterin

Name:	E-Charge Pay by K3S GmbH
Anschrift:	Rheinpromenade 2, 40789 Monheim
Name	Kai Schmidt
Funktion	Geschäftsführer
Email:	k.schmidt@echarge-pay.de
Telefon	+49 2173 2643720

Hier den Text einc

Beitrittsdatum

Unterschrift

ANHANG II

Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:
Beschäftigte, Kunden

Kategorien personenbezogener Daten, die verarbeitet werden:
Stammdaten, Kontaktdaten, Beschäftigtendaten, Nutzungsdaten, Inhaltsdaten

Art der Verarbeitung:
Erfassen und zusammenstellen von Daten zur Ermöglichung der Abrechnung von elektronischen Ladevorgängen für Fahrzeuge

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:
Auftragserfüllung und Vertragsmanagement, Gestaltung, Betrieb und Verfügbarkeit digitaler Produkte, Informationssicherheit

Dauer der Verarbeitung:
Vertragsdauer sowie Aufbewahrung im Rahmen der gesetzlichen Aufbewahrungsfristen

Gegenstand der Verarbeitung durch (Unter-)Auftragsverarbeiter:
Hosting der Software und Datenbanken

Art der Verarbeitung durch (Unter-)Auftragsverarbeiter:
Speicherung der Software und Datenbanken sowie der anfallenden Daten

Dauer der Verarbeitung durch (Unter-)Auftragsverarbeiter:
Vertragsdauer sowie Aufbewahrung im Rahmen der gesetzlichen Aufbewahrungsfristen

ANHANG III

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

Die E-Charge Pay by K3S GmbH trifft folgende Festlegungen über die von ihr umzusetzenden technischen und organisatorischen Maßnahmen:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Folgende Maßnahmen verhindern, dass unbefugte Personen Zutritt zu Datenverarbeitungsanlagen haben:

- ✓ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)
- ✓ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)
- ✓ Sicherheitstüren / -fenster
- ✓ Zaunanlagen
- ✓ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- ✓ Werkschutz, Pförtner
- ✓ Alarmanlage
- ✓ Videoüberwachung
- ✓ Spezielle Schutzvorkehrungen des Serverraums
- ✓ Spezielle Schutzvorkehrungen für die Aufbewahrung von Backups und anderen Datenträgern
- ✓ Nicht-reversible Vernichtung von Datenträgern
- ✓ Sperrbereiche
- ✓ Besucherregelung (z.B. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)
- ✓ Regelungen für das Home-Office (Betriebs-/Dienstvereinbarung)

1.2 Zugangskontrolle

Folgende Maßnahmen verhindern, dass unbefugte Dritte Zugang zu Datenverarbeitungsanlagen haben:

- ✓ Persönlicher und individueller Login bei Anmeldung am System/Netzwerk
- ✓ Autorisierungsprozess für Zugangsberechtigungen
- ✓ Begrenzung der befugten Benutzer
- ✓ Personalisierte Chipkarten, Token, PIN-/TAN, Zwei-Faktor-Authentifizierung, etc.
- ✓ Protokollierung des Zugangs
- ✓ Zusätzlicher Login für bestimmte Anwendungen
- ✓ Firewall

1.3 Zugriffskontrolle

Folgende Maßnahmen stellen sicher, dass unbefugte Dritte keinen Zugriff auf Daten haben:

- ✓ Verwaltung und Dokumentation von differenzierten Berechtigungen
- ✓ Abschluss von Verträgen zur Auftragsverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von Daten Gegenstand der Leistung des Auftragnehmers ist.
- ✓ Auswertungen/Protokollierungen von Datenverarbeitungen
- ✓ Autorisierungsprozess für Berechtigungen
- ✓ Genehmigungsroutinen
- ✓ Profile/Rollen
- ✓ Verschlüsselung von Datenträgern
- ✓ Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf mobile Datenträger (z.B. Kopierschutz, Sperrung von USB-Ports, Data Loss Prevention System/DLP)
- ✓ Funktionstrennung (Segregation of Duties)
- ✓ Nicht-reversible Löschung von Datenträgern

1.4 Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- ✓ Speicherung der Datensätze in physikalisch getrennten Datenbanken
- ✓ Verarbeitung auf mindestens logisch getrennten Systemen
- ✓ Zugriffsberechtigungen nach funktioneller Zuständigkeit
- ✓ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
- ✓ Mandantenfähigkeit von IT-Systemen
- ✓ Verwendung von Testdaten
- ✓ Trennung von Entwicklungs- und Produktionsumgebung

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung von Daten erfolgt so, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

Es ist sichergestellt, dass Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert, entfernt oder sonst verarbeitet werden können und überprüft werden kann, welche Personen oder Stellen Zugriff auf Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- ✓ Verschlüsselung von E-Mail oder E-Mail-Anhängen
- ✓ Verschlüsselung von Datenträgern
- ✓ Gesicherter File Transfer oder sonstiger Datentransport
- ✓ Physikalische Transportsicherung
- ✓ Qualifizierte elektronische Signatur
- ✓ Verschlüsseltes WLAN
- ✓ Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort)
- ✓ Regelung zum Umgang mit mobilen Datenträgern (z.B. Laptop, USB-Stick, Mobiltelefon)
- ✓ Protokollierung von Datenübertragung oder Datentransport
- ✓ Protokollierung von lesenden Zugriffen
- ✓ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten
- ✓ Sichere VPN-Verbindung

2.2 Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- ✓ Zugriffsrechte
- ✓ Systemseitige Protokollierungen
- ✓ Dokumenten Management System (DMS) / Enterprise Content Management System (ECMS) mit Änderungshistorie
- ✓ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- ✓ Vieraugenprinzip

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Durch folgende Maßnahmen ist sichergestellt, dass Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

- ✓ Sicherheitskonzept für Software- und IT-Anwendungen
- ✓ Backup Verfahren
- ✓ Aufbewahrungsprozess für Backups (z.B. brandgeschützter Safe, getrennter Brandabschnitt)
- ✓ Gewährleistung der Datenspeicherung im gesicherten Netzwerk
- ✓ Bedarfsgerechtes Einspielen von Sicherheits-Updates und Software-Patches sowie AV-Signaturen

- ✓ Spiegeln von Festplatten
- ✓ Unterbrechungsfreie Stromversorgung (USV)
- ✓ Brand- und/oder Löschwasserschutz des Serverraums
- ✓ Klimatisierter Serverraum
- ✓ Virenschutz
- ✓ Firewall
- ✓ Notfallplan
- ✓ Erfolgreiche Notfallübungen
- ✓ Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1 Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- ✓ Datenschutzleitbild des Auftragnehmers
- ✓ Datenschutz-Richtlinie des Auftragnehmers
- ✓ Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit
- ✓ Verpflichtung der Mitarbeiter auf die Vertraulichkeit
- ✓ Hinreichende Schulungen der Mitarbeiter im Datenschutz
- ✓ Führen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO)
- ✓ Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)

4.2 Management bei Datenschutzverletzungen

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- ✓ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- ✓ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber betroffenen Personen (Art. 34 DSGVO)

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Datenschutzfreundliche Voreinstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Verarbeitungen zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben oder Eingabemöglichkeiten festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden. Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export-

und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden) oder die Verfügbarkeit bestimmter Verarbeitungen, Funktionen oder Protokollierungen.

4.4 Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass Daten nur nach Weisungen des Auftraggebers verarbeitet werden:

- ✓ Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten der Parteien
- ✓ Prozess zur Erteilung und/oder Befolgung von Weisungen
- ✓ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- ✓ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- ✓ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
- ✓ Unabhängige Auditierung der Weisungsgebundenheit
- ✓ Verpflichtung der Beschäftigten auf die Vertraulichkeit
- ✓ Vereinbarung von Vertragsstrafen für Verstöße gegen Weisungen
- ✓ formalisiertes Auftragsmanagement
- ✓ dokumentiertes Verfahren zur Auswahl von Unterauftragnehmern
- ✓ standardisiertes Vertragsmanagement zur Kontrolle von Unterauftragnehmern

Hier den Text eingeben , den Hier den Text eingebe

Ort

_____

Unterschrift Auftraggeber

Hier den Text eingeben Hier den Text eingeben

Name Funktion des Unterzeichners

Monheim am Rhein , den Hier den Text eingeben

_____

Unterschrift Auftragnehmer

Kai Schmidt Geschäftsführer