Datenschutzerklärung Betriebssystem be.ENERGISED

Diese Datenschutzerklärung gilt für die digitalen Kommunikationsmittel, für die iOS- und Android-Versionen der da emobil GmbH & Co KG App sowie für die da emobil GmbH & Co KG Ladestationen, welche den Kunden zur Verfügung gestellt werden, und erklärt unter anderem den Umgang mit personenbezogenen Daten im Zusammenhang mit den erwähnten Informationen, Apps und Ladestationen.

Einzelne Informationen und Apps können Links auf andere Anbieterinnen und Anbieter innerhalb und außerhalb der da emobil GmbH & Co KG enthalten, auf die sich die Datenschutzerklärung nicht erstreckt. Für diese Inhalte übernimmt die da emobil GmbH & Co KG keine Haftung.

Ergänzungsvereinbarung zur Softwarevereinbarung bezüglich

(die „Vereinbarung“)

Einhaltung der EU-Datenschutz-Grundverordnung (DSGVO) - Bestimmungen für Auftragsverarbeiter

da emobil GmbH & Co KG
Josef-Wilberger-Straße 53
6020 Innsbruck
E-Mail: support@da-emobil.com

im Folgenden einzeln als „Partei“ und gemeinsam als „Parteien“ bezeichnet

1. Begriffsbestimmungen

Für die Zwecke dieser Ergänzungsvereinbarung haben die folgenden Begriffe die folgende Bedeutung:

Unter „Datenschutz-Vorschriften“ werden die DSGVO und alle anwendbaren nationalen Gesetze, Vorgaben und Verordnungen, welche die DSGVO umsetzen, verstanden (in der jeweils geltenden Fassung);

„Betroffene Person“, „Verantwortlicher“, „Auftragsverarbeiter“ oder „Verarbeitung“ haben jeweils die in der DSGVO geregelte Bedeutung;

„DSGVO“ meint die Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr solcher Daten;

„Aufsichtsbehörde“ meint die Datenschutz-Aufsichtsbehörde, welche für die Verarbeitung personenbezogener Daten durch den Verantwortlichen zuständig ist.

2. Hintergrund

2.1 Der Sub CPO (für die Zwecke dieser Ergänzungsvereinbarung: der „Verantwortliche“) beauftragt [da emobil GmbH & Co KG] (für die Zwecke dieser Ergänzungsvereinbarung: der „Auftragsverarbeiter“) mit der Verarbeitung personenbezogener Daten, wie in der Anlage 1 näher beschrieben wird.

2.2 Die Parteien verpflichten sich, alle geltenden Anforderungen der Datenschutz-Vorschriften einzuhalten. Diese Ergänzungsvereinbarung dient lediglich als Zusatz. Sie entlastet eine Partei nicht von ihren Pflichten aus den Datenschutz-Vorschriften und ersetzt diese auch nicht.

3. Die Pflichten des Auftragsverarbeiters

3.1 Bei der Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen wird der Auftragsverarbeiter:

3.1.1 die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten, worüber er vorab vom Verantwortlichen unterrichtet wird, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; 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;

3.1.2 Dritten keinen Zugang zu den im Rahmen dieser Vereinbarung übermittelten personenbezogenen Daten gewähren, mit Ausnahme der Mitarbeiter, die direkt unter seiner Verantwortung handeln oder mit ihm verbundene Unternehmen und in jedem Fall nur insoweit, als ein solcher Zugriff auf personenbezogene Daten für die Erbringung von Dienstleistungen im Rahmen dieser Vereinbarung erforderlich ist. Der Auftragsverarbeiter haftet in jedem Fall für die Verarbeitungstätigkeiten solcher Dritter.

3.1.3 sicherstellen, dass für alle Mitarbeiter, die Zugang zu den personenbezogenen Daten haben und/oder zur Verarbeitung der personenbezogenen Daten berechtigt sind, die Verpflichtung besteht, die personenbezogenen Daten streng vertraulich zu behandeln;

3.1.4 geeignete technische, physische und organisatorische Sicherheitsmaßnahmen einführen, die vom Verantwortlichen überprüft und genehmigt werden, einschließlich, je nach Fall: (i) die Pseudonymisierung und Verschlüsselung personenbezogener Daten; (ii) die dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung; (iii) die rasche Wiederherstellung der Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall; und (iv) die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung;

Einzelheiten zu den Sicherheitsmaßnahmen sind aus der Anlage 2 zu entnehmen.

3.1.5 angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in den

Datenschutz-Vorschriften genannten Rechte der betroffenen Person nachzukommen. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich benachrichtigen, nachdem er von einem Antrag direkt durch eine betroffene Personen Kenntnis erhalten hat, ohne jedoch auf diesen Antrag zu antworten, es sei denn, er wurde dazu anderweitig ermächtigt;

3.1.6 den Verantwortlichen unverzüglich (zumindest innerhalb eines Zeitraums, der es dem Verantwortlichen ermöglicht, seinen (Mitteilungs-)Pflichten gemäß der DSGVO nachzukommen) schriftlich benachrichtigen, sobald er Kenntnis von (i) einem/einer unzulässigen, nicht autorisierten oder unrechtmäßigen Zugriff, Nutzung, Offenlegung oder irgendeinem anderen Ereignis erhält, welches die Verfügbarkeit, Integrität oder Vertraulichkeit von personenbezogenen Daten beeinträchtigt, die vom Verantwortlichen gemäß dieser Vereinbarung verarbeitet werden; und/oder (ii) einer rechtsverbindlichen Aufforderung zur Offenlegung personenbezogener Daten durch eine Strafverfolgungsbehörde erhält, sofern dies nicht anderweitig verboten ist, wie zum Beispiel durch ein Verbot zur Wahrung der Vertraulichkeit bei strafrechtlichen Ermittlungen;

3.1.7 den Verantwortlichen bei der Erfüllung seiner Verpflichtungen unterstützen, (i) geeignete technische und organisatorische Sicherheitsmaßnahmen einzuführen; (ii) Verletzungen des Schutzes personenbezogener Daten der Aufsichtsbehörde und/oder betroffenen Personen mitzuteilen; (iii) Datenschutz-Folgenabschätzungen durchzuführen und, falls erforderlich, vorher die Aufsichtsbehörde zu konsultieren;

3.1.8 nach Ablauf oder Beendigung der Vereinbarung alle personenbezogenen Daten nach Wahl des Verantwortlichen und ohne zusätzliche Kosten für den Verantwortlichen, entweder löschen oder dem Verantwortlichen zurückgeben und vorhandene Kopien löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Zu diesem Zweck werden die Parteien nach der Beendigung dieser Vereinbarung in gutem Glauben zusammenarbeiten, um alle Dienstleistungen im Rahmen dieser Vereinbarung so schnell wie vernünftigerweise möglich und mit minimalen Auswirkungen auf die Geschäftstätigkeit einer der Parteien auslaufen zu lassen. Auf Verlangen des Verantwortlichen wird der Auftragsverarbeiter ausreichende Nachweise erbringen, dass er die personenbezogenen Daten unwiderruflich gelöscht hat. Jede Rückgabe von personenbezogenen Daten an den Verantwortlichen hat auf elektronischem Wege in einem allgemein anerkannten strukturierten Datenformat zu erfolgen. Wenn es nicht möglich ist, die personenbezogenen Daten zurückzugeben oder unwiderruflich zu löschen, ist der Auftragsverarbeiter verpflichtet, den Verantwortlich unverzüglich darüber zu informieren. In diesem Fall garantiert der Auftragsverarbeiter, dass die personenbezogenen Daten vertraulich behandelt und nicht mehr verarbeitet werden;

3.1.9 zum Nachweis der Einhaltung dieser Ergänzungsvereinbarung vollständige und genaue Aufzeichnungen und Informationen (das „Verzeichnis“) führen, das Verzeichnis dem Verantwortlichen verfügbar machen und es für die Durchführung von Audits zur Verfügung stellen, einschließlich Inspektionen durch den Verantwortlichen oder den von ihm benannten Prüfer;

3.1.10 Der Auftragsverarbeiter benennt, sofern er dazu nach der DSGVO oder anderen anwendbaren nationalen und/oder lokalen Rechtsvorschriften verpflichtet ist, einen Datenschutzbeauftragten;

3.1.11 Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich informieren, falls er der Auffassung ist, dass eine Weisung gegen die Datenschutz-Vorschriften verstößt.

4. Internationale Übermittlungen

Der Auftragsverarbeiter wird keine personenbezogenen Daten in einem Land außerhalb des Europäischen Wirtschaftsraums („EWR“) verarbeiten oder dahin übertragen, es sei denn, der Verantwortliche hat vorher seine ausdrückliche schriftliche Zustimmung erteilt und der Auftragsverarbeiter hat die Standardvertragsklauseln gemäß des Durchführungsbeschlusses (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der DSGVO, Amtsblatt L 199/31 vom 7.6.2021 (die „Musterklauseln“) in der jeweils gültigen Fassung unterzeichnet. Der Auftragsverarbeiter garantiert, dass diese Übermittlung und Verarbeitung unter Einhaltung der Bestimmungen der Musterklauseln erfolgt, es sei denn, eine andere geeignete Garantie wäre verfügbar und wurde durch die Parteien vereinbart. Die in Ziffer 3 genannten Verpflichtungen des Auftragsverarbeiters gelten auch im Falle einer Übermittlung in ein Land außerhalb des EWR.

5. Unterauftragsverarbeitung

5.1 Der Auftragsverarbeiter darf Unterauftragsverarbeiter nur nach ausdrücklicher vorheriger schriftlicher Zustimmung des Verantwortlichen beauftragen. Die Liste der vom Verantwortlichen genehmigten Unterauftragsverarbeiter findet sich in Anlage 3. Die Parteien halten Anlage 3 jeweils auf dem neuesten Stand.

5.2 Der Auftragsverarbeiter bestätigt, dass er mit dem Unterauftragsverarbeiter eine schriftliche Vereinbarung schließt, die im Wesentlichen ähnliche Bestimmungen wie in dieser Ergänzungsvereinbarung enthält.

5.3 Im Verhältnis zwischen dem Verantwortlichen und dem Auftragsverarbeiter bleibt der Auftragsverarbeiter für alle Handlungen und Unterlassungen eines von ihm gemäß dieser Ziffer 5 ernannten Unterauftragsverarbeiters vollständig haftbar.

Anlage 1 – Beschreibung der verarbeiteten Daten

Kategorien personenbezogener Daten

[da emobil GmbH & Co KG verwendet personenbezogene Daten zu keinem anderen Zweck als jenem der Vertragserfüllung. Da emobil GmbH & Co KG verpflichtet sich, personenbezogene Daten ausschließlich nach den Vorgaben der EU-Datenschutzgrundverordnung (DSGVO) und des österreichischen Datenschutzgesetzes (DSG) sowie gemäß den Bestimmungen dieser Vereinbarung zu verarbeiten.]

Sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen.

Art der Verarbeitung

Technische Speicherung von da emobil GmbH & Co KG zur Durchführung und Abrechnung von Ladevorgängen elektrisch betriebener Fahrzeuge. Folgende Personenstammdaten werden verarbeitet: Kundennummer, Vorname, Familienname, Anschrift, Geschlecht, Geburtsdatum, Erworbene Titel, Umsatzsteuer-Identifikationsnummer, Firmenbuchnummer, Bankverbindung bestehend aus IBAN, BIC und Name des kontoführenden Bankinstituts. Die Daten werden ausgenommen von natürlichen Personen bearbeitet, die zur Nutzung des Services autorisiert wurden.]

Zweck(e) der Datenverarbeitung

[Technische Speicherung zur Durchführung und Abrechnung von Ladevorgängen elektrisch betriebener Fahrzeuge. Es handelt sich um Angaben, die zur eindeutigen Identifikation einer natürlichen Person innerhalb eines Netzwerkes erforderlich sind (beispielsweise Tag-ID der RFID-Karte) sowie die mit einem Ladevorgang verbundenen Log-Information zu Energiemengen, Standort und Nutzungszeit der Ladeinfrastruktur.]

Dauer der Verarbeitung und Zeitraum, in welchem die Daten gespeichert werden. Wenn die Speicherfrist nicht angegeben werden kann, die Kriterien, die diese Frist bestimmen:

Die Dauer bei Beendigung der Vertragsbeziehungen oder nach jederzeitiger Aufforderung durch den Verantwortlichen hat da emobil GmbH & Co KG sämtliche im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten dem Verantwortlichen auf dessen dokumentierte Weisung hin entweder in einem gängigen Format auszuhändigen oder datenschutzgerecht zu vernichten.

Findet ein internationaler Datentransfer gemäß Ziffer 4 statt? Wenn ja, in welche Länder und unter Einhaltung welcher geeigneter Garantien gemäß Kapitel 5 der DSGVO (Art. 44-50 DSGVO):

Die Verarbeitung der Daten findet ausschließlich in Mitgliedsstaaten der Europäischen Union oder in Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder in

solchen Drittstaaten, für die ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Art 45 DSGVO oder geeignete Garantien gemäß 46 DSGVO vorliegen, statt.

Sub-Dienstleister	**Art der Verarbeitung**
Hubject GmbH, EUREF-Campus 22, D-10829 Berlin	Betrieb von Roamingnetzwerken/ Ladevorgangs- und Rechnungsdaten.
wherever SIM GmbH, Humboldtstraße 53, Haus A, D-22083 Hamburg	Betrieb Simkarten APN Netzwerk Europa, Abwicklung von OCPP-Kommunikation / Identifikationsdaten von Endnutzern.
IGS Systemmanagement GmbH & Co KG, Dorfplatz 5, A-4533 Piberbach	Betrieb eines Reportingsystems, dass Buchungssätze in die definierten Bilanz- und GUV-Schemata einbettet.
DGR Datenverarbeitungs gesmbH Dr. Adolf-Schärf-Straße 24, A-4053 Haid	ERP-System im Zusammenhang mit Stammdaten, Materialwirtschaft und Angebotslegungen.
ChargePoint Austria GmbH, Salzburger Straße 26, 5550 Radstadt	Betrieb der Abrechnungssoftware / alle in be.ENERGISED (Abrechnungssoftware) erfassten Daten. https://trust.chargepoint.com/
Gutmann GmbH, Fürstenweg 87, 6020 Innsbruck	Ausgewählte Mitarbeiter sind für den Versand, pflege der Kundendaten und Abrechnung in Bezug auf Roaming-Ladekarten zuständig.
Fiegl & Spielberger GmbH, Langer Weg 28, 6020 Innsbruck	Ausgewählte Mitarbeiter für Bilanzierung, Buchhaltung und EDV.
FileZilla (Software)	Betrieb von Datenübertragung mittels FTP und SFTP.
Bitrix24 Limited, Poseidonos, 1, Egkomi 2406 Nikosia, Zypern	Betrieb eines CRM-Systems, inklusive des Tools der Aufgabenerstellung und Projektübersicht.
ASSIST Notfallservice GmbH, Baumgasse 129, 1030 Wien	Vermittlung und Durchführung von Dienst- und Serviceleistungen im Mobilitätsbereich.

Anlage 2: Technische und organisatorische Maßnahmen (TOMs)

1. Da emobil GmbH & Co KG wird durch Schulungen, Arbeitsanweisungen sowie entsprechende Kontrollen der Mitarbeiter die datenschutzgerechte Auftragsabwicklung gewährleisten;

2. Da emobil GmbH & Co KG verpflichtet seine mit der Verarbeitung personenbezogener Daten befassten Mitarbeiter schriftlich zur Vertraulichkeit sowie zur Wahrung des Datengeheimnisses gemäß §6 DSG;

3. Da emobil GmbH & Co KG hat geeignete Maßnahmen getroffen, um personenbezogene Daten gegen zufällige Zerstörung oder Verlust zu schützen. Der Schutz vor zufälliger Zerstörung personenbezogener Daten betrifft im Wesentlichen die Absicherung, durch den Unterauftragsverarbeiter has-to-be, gegen Umwelteinflüsse, wie z.B. Feuer, Naturgewalt, Einbruch, Tiere, elektromagnetische Felder etc. Dies erfolgt einerseits durch übliche Objektschutzmaßnahmen (Brand- und Überspannungsschutz, unterbrechungsfreie Stromversorgung, redundante Datenanbindung) der Rechenzentren, in denen personenbezogene Daten gespeichert werden, sowie durch eine entsprechende Datensicherung mit einem nachgelagerten Wiederherstellungskonzept, welches eine Datenwiederherstellung innerhalb angemessener Frist ermöglicht.

4. Da emobil GmbH & Co KG verhindert durch eine Zugangskontrolle die Verarbeitung personenbezogener Daten durch Unbefugte, Der Zugang zu Datenverarbeitungssystem und Datenträgern und deren Benutzungsmöglichkeit durch Unbefugte wird, soweit technisch und organisatorisch möglich, verhindert.

5. Da emobil GmbH & Co KG hat ein Berechtigungssystem zur Zugangskontrolle in seinem organisatorischen Verantwortungsbereich installiert. Das Berechtigungssystem genügt den Anforderungen der Funktionstrennung bei der Verarbeitung personenbezogener Daten.

6. Da emobil GmbH & Co KG verhindert durch geeignete Maßnahmen bei der Weitergabe personenbezogener Daten, dass diese bei der elektronischen Übertragung, dem Transport oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder entfernt werden können. Geeignete Maßnahmen in diesem Sinn sind insbesondere die Verschlüsselung und die Nutzung gesicherter Übertragungswege. Die Weitergabekontrolle greift auch dann ein, wenn die Übertragung personenbezogener Daten beispielsweise zu Wartungs- oder weiteren Verarbeitungszwecken (z.B. zum Zweck der Archivierung) vorgenommen wird.

7. Das Firmennetzwerk ist gegen das öffentliche Netzwerk durch eine Hardware-Firewall geschützt. Datenträger innerhalb des Unternehmens sowie der Rechenzentren sind verschlüsselt. Datenbanken in Rechenzentren werden ausschließlich verschlüsselt betrieben. Windows-Einzelplatzcomputer sind mit Virenscannern ausgestattet. Sicherheitsrelevante Software-Updates werden regelmäßig automatisiert in die vorhandene Software eingespielt.

8. Da emobil GmbH & Co KG verhindert durch eine Zugangskontrolle die Verarbeitung personenbezogener Daten durch Unbefugte. Da emobil GmbH & Co KG hat ein Berechtigungssystem zur Zugangskontrolle in seinem organisatorischen Verantwortungsbereich installiert. Das Berechtigungssystem genügt den Anforderungen der Funktionstrennung bei der Verarbeitung personenbezogener Daten. Das Beobachten oder Ausspähen von personenbezogenen Daten durch Unbefugte wird durch geeignete Abschirmmaßnahmen verhindert. Manuelle Schließanlage mit elektronisch kodierten Schlüsseln an dem Standort von da emobil GmbH & Co KG. Der Gebäudezutritt von Reinigungs- und Wartungspersonal wird namensscharf dokumentiert.

9. Da emobil GmbH & Co KG hat geeignete Maßnahmen getroffen, durch die überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingeben, verändert oder entfernt worden sind.

10. Es bestehen Regelungen bzgl. Der Computersysteme inkl. deren Dokumentation bei Beendigung von Arbeitsverhältnissen. Sicherheitsrelevante Software-Updates werden regelmäßig automatisiert in die vorhandene Software eingespielt.

11. Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit;

Das Firmennetzwerk und das Netzwerk der Rechenzentren sind gegen das öffentliche Netzwerk durch eine Hardware-Firewall geschützt. Es werden Virenscanner für alle eingehenden Daten verwendet (sowohl Mail als auch Web). Windows-Einzelplatzcomputer sind mit Virenscannern ausgestattet. Sicherheitsrelevante Software-Updates werden regelmäßig automatisiert in die vorhandene Software eingespielt. Backups werden ausschließlich verschlüsselt durchgeführt, Backup-Medien werden gesichert verwahrt.

12. Da emobil GmbH & Co KG wird insbesondere durch Schulungen, Arbeitsanweisungen sowie entsprechende Kontrollen der Mitarbeiter die datenschutzgerechte Auftragsabwicklung gewährleisten.

13. Personenbezogene Daten werden dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Bei Beendigung der Vertragsbeziehung oder nach jederzeitiger Aufforderung durch den Verantwortlichen hat da emobil GmbH & Co KG sämtliche im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten auf dessen dokumentierte Weisung hin entweder in einem gängigen Format auszuhändigen oder datenschutzgerecht zu vernichten.

14. Da emobil GmbH & Co KG stell sicher, dass der Zugang zu allen relevanten Daten, Systemzugänge und Systemsicherheit permanent sichergestellt werden. Dies gelingt durch die Klärung der Verantwortlichkeiten und die Vergabe der Zugriffsrechte.

15. Es ist überprüf- und feststellbar, an welche Stellen eine Übermittlung personenbezogener Daten durch Datenübertragungseinrichtungen vorgesehen ist. Geeignete Maßnahmen in diesem Sinn sind insbesondere die Verschlüsselung und die Nutzung gesicherter Übertragungswege. Es erfolgt kein postalischer Versand von Datenträgern. Nach Beendigung des Rahmenvertrages werden dem Verantwortlichen

alle in seinem Auftrag verarbeiteten personenbezogenen Daten auf Wunsch maschinenlesbar zur Verfügung gestellt und nach Bestätigung der Lesbarkeit, spätestens jedoch nach Ablauf einer angemessenen Frist, sämtliche Administrator- und Benutzerkonten inkl. aller personenbezogener Daten, die keiner gesetzlichen Aufbewahrungspflicht unterliegen, gelöscht.