COMPLEO

The power to move

Anlagen zu Vertrag
über die Verarbeitung personenbezogener Daten

Anlage 1

1. Gegenstand und Dauer der Auftragsverarbeitung

1.1 Gegenstand

Der Gegenstand des Auftrags ist eine oder wiederkehrende Servicedienstleistung(en) in Form von Wartung, Reparatur oder Entstörung von eMobility-Ladestationen. (im Folgenden Leistungsvereinbarung).

1.2 Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung. Eine vorzeitige Beendigung der Laufzeit durch fristlose Kündigung ist im Falle einer Verletzung von gesetzlichen oder vertraglichen Datenschutzbestimmungen zulässig. Gleiches gilt, wenn der Auftragnehmer eine berechtigte Weisung des Auftraggebers nicht ausführen will oder kann.

2. Konkretisierung des Auftragsinhalts

2.1 Zweck der Verarbeitung

Die Datenverarbeitung erfolgt zu folgendem Zweck: Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in der Leistungsvereinbarung unter B2 konkret beschrieben.

2.2 Ort der Verarbeitung

Die Erbringung der vertraglich vereinbarten Leistung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

2.3 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Berufs-, Branchen- oder Geschäftsbezeichnung
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Verbrauchs- und Netzzustandsdaten aus Netz- und Messstellenbetrieb
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Vertragsabrechnungs- und Zahlungsdaten

2.4 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen**:**

- Kunden
- Mitarbeiter

3. Qualitätssicherung und sonstige Pflichten des Auftragnehmers gem. Art. 28 Abs. 3 s. 1 DSGVO

3.1 Kontaktdaten Datenschutzbeauftragter Die Kontaktdaten des Beauftragten für den Datenschutz (gemäß Art. 39, 38 DSGVO) lauten:

Karsten Schulz

datenschutz@compleo-cs.de
M: +49 151 22631968

4. Unterauftragsverhältnisse gem. Art. 28 Abs. 3 s. 2 lit. d DSGVO i.v.m. Art. 28 Abs. 2 und 4 DSGVO

4.1 Der Auftraggeber stimmt hiermit der Beauftragung nachfolgender Unterauftragnehmer zu:

- Name/Firma
  Deutsche Telekom Individual Solutions & Products GmbH
  Anschrift
  Marianne-Baecker-Allee 15, 30449 Hannover
  Deutschland
  (Teil-)leistung
  Service-Dienstleistung vor Ort

- Name/Firma
  synfis Service GmbH Deutschland
  Anschrift
  Gerberstr. 4, 30916 Isernhagen
  Deutschland
  (Teil-)leistung
  Service Dienstleistung vor Ort

Compleo Charging Software GmbH, Ezzestraße 8, 44379 Dortmund, Germany
info@compleo-cs.com | compleo-charging.com

- Name/Firma

  TSG Deutschland GmbH & Co.KG

  Anschrift

  Lothstrasse 1a, 80335 München
  Deutschland

  (Teil-)leistung

  Service-Dienstleistung vor Ort

Compleo Charging Software GmbH, Ezzestraße 8, 44379 Dortmund, Germany
info@compleo-cs.com | compleo-charging.com

Anlagen zu Vertrag
über die Verarbeitung personenbezogener Daten

Anlage 2
Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

Es wird vom Auftragnehmer ein für die konkrete Auftragsverarbeitung angemessenes Schutzniveau gewährleistet. Dies wird wie folgt beschrieben:

1. Vertraulichkeit

1.1 Zutrittskontrolle (Rechenzentrum)Die Gebäude sind mit einer Alarmanlage gesichert.

a. Die Eingangstüren des Gebäudes sind mit folgender Schließanlage versehen:
- Chipkartenzugangssystem

b. Die Dokumentation der Zutrittsberechtigungen vorgenannter Schließanlage erfolgt namensscharf.

c. Der Gebäudezutritt von Firmenfremden/ Gästen/Besuchern wird namensscharf dokumentiert.

d. Der Gebäudezutritt von Reinigungs- und Wartungspersonal wird namensscharf dokumentiert.

e. Es bestehen Regelungen bzgl. der Entziehung von Gebäudezutrittsberechtigungen inklusive Dokumentation für Mitarbeiter bei Beendigung des Arbeitsverhältnisses.

1.2 Es besteht ein gesondertes Zutrittskonzept für Serverräume inkl. namensscharfer Dokumentation.

1.3 Zugangskontrolle

a. Das Firmennetzwerk ist gegen das öffentliche Netzwerk durch eine Hardware-Firewall geschützt.

b. Es werden regelmäßig Penetrationstests aller zum Internet geöffneten IP-Adressen durchgeführt.

c. Die Mitarbeiter werden auf folgende
- Passwortvorgaben verpflichtet:
- Individuell geheim zu haltendes Computerkennwort für jeden Mitarbeiter
- Keine Sammelkennwörter
- Mindestlänge, wenn zutreffend: Anzahl Zeichen/Komplexität: 7 Zeichen
- Wechselrhythmus, wenn zutreffend bitte Zeitintervall angeben: alle 3 Monate

d. An den folgenden Übergängen zum Firmennetz werden Virenscanner eingesetzt:
- E-Mail-Account
- Web

e. Der Einsatz eines Virenscanners auf allen Einzelarbeitsplatzcomputern ist sichergestellt.

f. Sicherheitsrelevante Softwareupdates werden regelmäßig und automatisiert in die vorhandene Software eingespielt. Mitarbeiter haben Internetzugangsberechtigung mit restriktiver, von Mitarbeitern nicht änderbarer Browserkonfiguration.

1.2 Zugriffskontrolle

a. Berechtigungskonzepte sind vorhanden und werden dokumentiert.

b. Die Organisation der Berechtigungsvergabe wird namensscharf dokumentiert (insb. wer darf welche Rechte vergeben).

c. Die vergebenen Berechtigungen werden namensscharf dokumentiert.

d. Folgende Komponenten der Arbeitsplatzcomputer wurden verriegelt/ deaktiviert, damit keine Datenexporte extern gespeichert werden können:
- CD-/DVD-Brenner

e. Fernwartungs-/Fernzugriffszugänge sind vorhanden für:
- weitere/externe Dienstleister
- Mitarbeiter

1.4 Trennungskontrolle

f. Es besteht ein Berechtigungskonzept für vorgenannten Mandanten, dass den Datenzugriff von Mitarbeitern ausschließt, die nicht für den Auftraggeber/Leistungsempfänger tätig sind.

g. Mitarbeiter werden dazu verpflichtet, Informationen aus Datenbeständen des Auftraggebers nicht in andere Projekte/Zwecke mit einzubringen.

Compleo Charging Software GmbH, Ezzestraße 8, 44379 Dortmund, Germany
info@compleo-cs.com | compleo-charging.com

2. Integrität

2.1 Weitergabekontrolle

a. Eingesetzte Verschlüsselungsart für Datenaustausch zwischen Auftraggeber und Auftragnehmer:
   - SFTP
   - S/Mime

b. Die per Datenträger versendeten Daten werden verschlüsselt.

c. Erläuterung des Rückmeldeverfahrens an den Auftraggeber bei erhaltenem Datenträger oder vermutetem Datenträgerverlust:
   - telefonisch

d. Backupmedien werden gesichert aufbewahrt.

e. Wie und wann werden die Daten des Auftraggebers nach Auftragsende gelöscht (elektronische Datenträger/Papierdokumente):
   - Nach Aufforderung des Auftraggebers

f. Maßnahmen zum Schutz von Daten des Auftraggebers (auch temporären) auf mobilen Arbeitsplatzrechnern:
   - Verschlüsselung durch Bitlocker, aber grundsätzlich Daten nur auf Servern

2.2 Eingabekontrolle

a. Es werden Log-Files für die Nachvollziehbarkeit der Löschung/Änderung von Daten des Auftraggebers namensscharf je Mitarbeiter angelegt.

b. Es besteht ein restriktives Zugriffskonzept für vorgenannte Log-Files.

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

a. Aufbewahrungsort von Sicherungsdatenträgern:
   - Externe Auslagerung in 3km (Luftlinie) Entfernung

b. Es bestehen Wartungsverträge für die Wartung von IT-Systemen durch Externe.

4. Wiederherstellbarkeit

4.1 Disaster-Recovery-Plan:

a. Es ist ein Disaster-Recovery-Plan definiert, um im Notfall den Geschäftsbetrieb wiederherstellen zu können Test Disaster- Recovery-Plan: Ein definierter Disaster- Recovery-Plan ist hinsichtlich der Umsetzbarkeit getestet worden, somit kann die tatsächliche Umsetzbarkeit nachgewiesen werden Wiederherstellungsmöglichkeiten:

b. Für folgende Bereiche lassen sich Zustände oder Daten wiederherstellen: Installationen, Daten, Systemdateien und Datencontainer, Log- Daten, Benutzerkonten und Konfigurationen (Einstellungen und Freigaben

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Auftragskontrolle

a. Die Mitarbeiter des Auftragnehmers, die personenbezogene Daten des Auftraggebers verarbeiten oder Zugriff hierauf haben, haben sich schriftlich zur Vertraulichkeit beim Umgang mit personenbezogenen Daten verpflichtet.

b. Folgende schriftliche Zusatzerklärungen (im Zusammenhang mit Datenschutz und Datensicherheit) holt der Auftragnehmer von seinen Mitarbeitern ein:
   - IT-Sicherheitsrichtlinie

c. Es werden/wurden Subauftragnehmer beauftragt, die Zugriff auf Daten des Auftraggebers haben.

d. Mit Subauftragnehmern, die Daten des Auftraggebers verarbeiten, bestehen Verträge zur Auftragsverarbeitung im Sinne des Artt. 4 Nr. 8 i.V.m. 28 EU DS-GVO.

e. Subauftragnehmer, die Zugriff auf Daten des Auftraggebers erhalten, halten die in dieser Checkliste vereinbarten technischen und organisatorischen Maßnahmen im gleichen Maße wie der Auftragnehmer selbst ein und haben deren Einhaltung vertraglich zugesichert.

f. Es erfolgen Schulungen der Mitarbeiter zum Datenschutz inkl. namensscharfer Dokumentation.

g. Für das Unternehmen des Auftragnehmers bestehen zurzeit folgende Zertifikate/ Datenschutzkonzepte, die mit dieser Checkliste eingereicht werden (Angabe bitte unter Angabe von Titel und Datum):
   - ISO 9000, innogy Cyber Security Baseline Controls Version 2.0 (Präzisierung ISO IEC 27002), ISO 27001

h. Folgendes Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gem. Art. 32 (1) DS-GVO kommt beim Auftragnehmer zum Einsatz:
   - ISMS, nach folgendem Standard: ISO 27001

Compleo Charging Software GmbH, Ezzestraße 8, 44379 Dortmund, Germany
info@compleo-cs.com | compleo-charging.com