Zusatzbedingungen Datenschutz - technische und organisatorische Maßnahmen (ZB/MD)

Anlage ZBMD zum Vertrag _____ (Nr. [*Rahmen*]vertrag, falls bereits vorhanden).
Die hier beschriebenen technischen und organisatorischen Maßnahmen werden verbindlich festgelegt zwischen Klicken Sie hier, um Text einzugeben. (Auftraggeber) und **innogy eMobility Solutions GmbH** (Auftragnehmer).

1. Vertraulichkeit

1.1 Zutrittskontrolle

1.1.1 Es erfolgt eine Speicherung und/oder Verarbeitung von personenbezogenen Daten des Auftraggebers:
☒ In den Büroräumen des Auftragnehmers
☒ Im Rechenzentrum bzw. in Serverräumen des Auftragnehmers
☐ Bei folgendem IT-Dienstleister (z.B. Cloud-Anbieter): _____
oder ☐ nicht zutreffend

1.1.2 Die Gebäude sind mit folgenden Maßnahmen gesichert:

		Alarmanlage	Video-überwachung	Sonstiges	nicht zutreffend
1.1.2.1	Bürogebäude:	☒	☒	_____	☐
1.1.2.2	Rechenzentrum:	☐	☐	_____	☐

1.1.3 Der Zutritt zu den Räumlichkeiten ist mit folgenden Maßnahmen gesichert:

		manuelle Schließanlage	Chipkarten-zugangssystem	Sonstiges*	nicht zutreffend
1.1.3.1	Büroräume:	☒	☐	_____	☐
1.1.3.2	Serverräume:	☒	☐	_____	☐
1.1.3.3	Rechenzentrum:	☒	☐	_____	☐

* Bspw. Vereinzelungsanlagen, biometrische Zutrittskontrolle

1.1.4 Die Dokumentation der Zutrittsberechtigungen erfolgt namensscharf:
☐ ja ☒ nein ☐ nicht zutreffend

1.1.5 Regelungen zum Gebäudezutritt von Firmenfremden / Gästen / Besuchern:

		Namensscharfe Dokumentation ja	nein	Zutritt und Aufenthalt nur in Begleitung von Aufsichtspersonal	nicht zutreffend
1.1.5.1	Büroräume:	☒	☐	☒	☐
1.1.5.2	Serverräume:	☒	☐	☐	☐
1.1.5.3	Rechenzentrum:	☒	☐	☐	☐

1.1.6 Regelungen zum Gebäudezutritt von Reinigungs- und Wartungspersonal:

		Namensscharfe Dokumentation ja	nein	Zutritt und Aufenthalt nur in Begleitung von Aufsichtspersonal	nicht zutreffend
1.1.6.1	Büroräume:	☒	☐	☐	☐
1.1.6.2	Serverräume:	☒	☐	☐	☐
1.1.6.3	Rechenzentrum:	☒	☐	☐	☐

1.1.7 Es bestehen Regelungen bzgl. der Entziehung von Gebäudezutrittsberechtigungen und Zugriffsrechten zu Computersystemen inkl. Dokumentation für Mitarbeiter bei Beendigung des Arbeitsverhältnisses:
☒ ja ☐ nein

1.2 Zugangskontrolle

1.2.1 Das Firmennetzwerk ist gegen das öffentliche Netzwerk durch eine Firewall geschützt:
☒ ja ☐ nein
wenn ja:
1.2.1.1 Typ: _____
1.2.1.2 Aktualisierungsverfahren und -häufigkeit: _____

1.2.2 Es werden regelmäßig Penetrationstests aller zum Internet geöffneten IP-Adressen durchgeführt:
☒ ja ☐ nein

1.2.3 Die Mitarbeiter werden auf folgende Passwortvorgaben verpflichtet:
1.2.3.1 ☒ Individuell geheim zu haltendes Computerkennwort für jeden Mitarbeiter
1.2.3.2 ☐ Mindestlänge, wenn zutreffend: Anzahl Zeichen/Komplexität: _____
1.2.3.3 ☐ Wechselrhythmus, wenn zutreffend bitte Zeitintervall angeben: _____
1.2.3.4 ☐ Automatische Verriegelung des Bildschirms nach Zeitintervall: _____

1.2.4 An den folgenden Übergängen zum Firmennetz werden Virenscanner eingesetzt:
☒ E-Mail-Account ☐ FTP ☐ Web

1.2.5 Einsatz eines Virenscanners auf allen Servern:
1.2.5.1 ☒ ja Aktualisierungsverfahren und -häufigkeit: _____
1.2.5.2 ☐ nein Angabe von Betriebssystem und Begründung: _____
oder ☐ nicht zutreffend, Begründung: _____

1.2.6 Einsatz eines Virenscanners auf allen Einzelarbeitsplatzcomputern:
1.2.6.1 ☒ ja Aktualisierungsverfahren und -häufigkeit: Einschließlich Windows
1.2.6.2 ☐ nein Angabe von Betriebssystem und Begründung: _____
oder ☐ nicht zutreffend, Begründung: _____

1.2.7 Sicherheitsrelevante Softwareupdates werden regelmäßig und automatisiert in die vorhandene Software eingespielt:
☒ ja ☐ nein

1.2.8 Folgende Mitarbeiter haben auf dem Einzelarbeitsplatzcomputer lokale Administrationsrechte:
Administratoren, Entwickler, Techniker: ☒ ja ☐ nein
Anwender: ☒ ja ☐ nein

1.2.9 Mitarbeiter haben Internetzugangsberechtigung:
1.2.9.1 ☒ ja ☐ nein
wenn ja: restriktive, von Mitarbeitern nicht änderbare Browserkonfiguration eingerichtet:
1.2.9.2 ☒ ja ☐ nein ☐ nicht zutreffend

1.3 Zugriffskontrolle

1.3.1 Berechtigungskonzepte sind vorhanden und werden dokumentiert:
☒ ja ☐ nein

1.3.2 Die Organisation der Berechtigungsvergabe wird namensscharf dokumentiert (insb. wer darf welche Rechte vergeben):
☒ ja ☐ nein

1.3.3 Die Berechtigungen werden nach dem Need-to-know-Prinzip vergeben und namensscharf aktualisiert und dokumentiert:
☒ ja ☐ nein

1.3.4 Anzahl der Administratoren mit der Berechtigung, Datenbestände des Auftraggebers ganz oder in großen Mengen zu kopieren/extrahieren: _____

1.3.5 Anzahl Mitarbeiter (keine Administratoren!) mit der Berechtigung, Datenbestände des Auftraggebers ganz oder in großen Mengen zu kopieren/extrahieren: _____
Formate, in denen der Export erfolgen kann (z.B. csv, xlsx): _____

1.3.6 Folgende Komponenten der Arbeitsplatzcomputer wurden verriegelt/deaktiviert, damit keine Datenexporte extern gespeichert werden können:
☐ USB-Ports
☐ CD-/DVD-Brenner
☐ Speicherkartenslots
☐ andere mobile Datenträger, wenn zutreffend welche: _____
oder ☒ Es erfolgt keine Deaktivierung von Komponenten

1.3.7 Fernwartungs-/Fernzugriffszugänge sind vorhanden für:
☐ weitere Dienstleister
☒ Mitarbeiter
Wenn Fernwartungs-/Fernzugriffszugänge vorhanden sind, bitte folgende Angaben ergänzen:
1.3.7.1 Art der Authentisierung (z.B. Passwort, oder PIN und Token): _____
1.3.7.2 Bei Passwort Authentisierung – Abweichungen zu den Angaben unter 1.2.3: _____
1.3.7.3 Verwendete Protokolle bzw. Mechanismen (z.B.: SSH, VPN, RDP): _____
1.3.7.4 Zusätzliche Sicherheitsmaßnahmen (z.B. individuelle Sitzungsfreigabe): _____
oder ☒ Es sind keine Fernwartungs-/Fernzugriffszugänge vorhanden

1.3.8 Es existieren beim Auftragnehmer Regelungen für mobiles Arbeiten (z.B. im Home-Office), um hierbei Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Datenverarbeitung sicherzustellen (diese Angaben ersetzen nicht die gemäß Anlage ZB/D erforderliche Zustimmung des Auftraggebers für mobiles Arbeiten):
1.3.8.1 ☒ ja ☐ nein
Es erfolgt eine Unterweisung der Mitarbeiter zum mobilen Arbeiten inkl. namensscharfer Dokumentation:
1.3.8.2 ☐ ja ☒ nein
oder ☒ nicht zutreffend

1.4 Trennungskontrolle

1.4.1 Welche Maßnahmen werden zur Separierung der Daten des Auftraggebers ergriffen:
☐ eigener, extra für den Auftrag vorgesehener Mandant
☐ netzwerktechnische Separierung durch folgende Maßnahmen: _____
oder ☒ nicht zutreffend

1.4.2 Es besteht ein Berechtigungskonzept für vorgenannte Mandanten bzw. Netzwerksegmente, das den Datenzugriff von Mitarbeitern ausschließt, die nicht für den Auftraggeber tätig sind:
☐ ja ☐ nein ☒ nicht zutreffend

1.4.3 Mitarbeiter werden schriftlich dazu verpflichtet, Informationen aus Datenbeständen des Auftraggebers nicht in andere Projekte/Zwecke mit einzubringen:
☐ ja ☐ nein ☒ nicht zutreffend

2. Integrität

2.1 Weitergabekontrolle

2.1.1 Falls Daten mittels Datenträger (z.B. Papierdokumente, Festplatte, USB-Stick, CD) zwischen Auftraggeber und Auftragnehmer übermittelt werden:

Die per digitalem Datenträger übermittelten Daten werden verschlüsselt: ☐ ja ☒ nein

2.1.1.1 Wenn ja, Verfahren bitte erläutern: _____

2.1.1.2 Rückmeldeverfahren an den Auftraggeber bei Erhalt oder vermutetem Verlust: _____

oder ☐ kein Einsatz von Datenträgern

2.1.2 Eingesetzte Verschlüsselungsart für Datenaustausch zwischen Auftraggeber und Auftragnehmer, falls Daten auf elektronischem Wege übermittelt werden:

2.1.2.1 ☒ SFTP

2.1.2.2 ☒ S/MIME

2.1.2.3 ☐ HTTPS (z.B. Web-Schnittstelle, Cloud-Speicher), bitte erläutern: _____

2.1.2.4 ☐ SSL-VPN oder Citrix, bitte erläutern: _____

2.1.2.5 ☐ Sonstige, Verfahren bitte erläutern: _____

oder ☒ keine elektronische Übermittlung von Daten

2.1.3 Werden personenbezogene Daten des Auftraggebers beim Auftragnehmer gespeichert:

☐ ja, unverschlüsselt ☐ja, verschlüsselt ☒ nein

2.1.3.1 wenn Daten verschlüsselt gespeichert werden, Erläuterung des Verfahrens: _____

2.1.4 Wie werden die in Backups enthaltenen Daten des Auftraggebers geschützt (z.B. gesicherte Aufbewahrung der Backupmedien, Verschlüsselung der Backups):

_____

oder ☒ es werden keine Backups von Daten des Auftraggebers durchgeführt

2.1.5 Löschung der Daten des Auftraggebers:

2.1.5.1 Wie werden die Daten gelöscht (z.B. gemäß welchen Standards / welcher Norm):

Elektronische Daten in Systemen: Ja ☐ nicht zutreffend

Elektronische Datenträger: _____ ☐ nicht zutreffend

Papierdokumente: Ja ☐ nicht zutreffend

2.1.5.2 In welcher Frist erfolgt die Datenlöschung bzw. Datenträgerentsorgung:

_____

oder ☐ nicht zutreffend

2.1.5.3 Wie erfolgt die Dokumentation der Datenlöschung bzw. Datenträgerentsorgung:

_____

oder ☒ nicht zutreffend

2.1.6 Maßnahmen zum Schutz von Daten des Auftraggebers (auch temporären) auf mobilen Geräten:

Mobile Arbeitsplatzrechner / Datenträger etc. (z.B. Sichtschutzfolie auf Bildschirmen, Verschlüsselung; bitte ggfs. Details zur Verschlüsselung angeben):

2.1.6.1 _____ ☐ keine Maßnahmen ☒ nicht zutreffend

Smartphones, Tablets etc. (z.B. Mobile Device Management, Verschlüsselung; bitte ggfs. Details zur Verschlüsselung angeben):

2.1.6.2 _____ ☐ keine Maßnahmen ☒ nicht zutreffend

2.2. Eingabekontrolle

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

☐ ja ☐ nein ☒ nicht zutreffend

2.2.2 Es besteht ein restriktives Zugriffskonzept für vorgenannte Log-Files:

☐ ja ☐ nein ☒ nicht zutreffend

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

3.1.1 Angaben zu Datensicherungen (Backups):

3.1.1.1 Häufigkeit der Backups (Intervall): _____

3.1.1.2 Anzahl vorgehaltener Generationen von Backups: _____

oder

☒ nicht zutreffend

3.1.2 Aufbewahrungsort von Sicherungsdatenträgern:

☐ Safe ☐ Externe Auslagerung ≥5km (Luftlinie) Entfernung

oder ☒ nicht zutreffend

3.1.3 Wiederanlaufzeit nach vollständiger Zerstörung des Rechenzentrums in Tagen: _____

oder ☒ nicht zutreffend

3.1.4 Es bestehen Verträge für die Wartung von IT-Systemen durch Externe:

☒ ja, ausschließlich innerhalb der EU ☐ ja, Zugriff aus Drittländern möglich ☐ nein

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Auftragskontrolle

4.1.1 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
☒ ja ☐ nein

4.1.2 Die Mitarbeiter werden schriftlich auf das Fernmeldegeheimnis[1] verpflichtet
☐ ja ☒ nein

4.1.3 Folgende schriftliche Zusatzerklärungen (im Zusammenhang mit Datenschutz und Datensicherheit sowie im Zusammenhang mit mobilem Arbeiten) holt der Auftragnehmer von seinen Mitarbeitern ein: Nein

4.1.4 Falls Subauftragnehmer beauftragt wurden, die Zugriff auf Daten des Auftraggebers haben:

4.1.4.1 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 sowie, wenn zutreffend, der Betriebssicherheit gemäß Artikel 4 RiLi 2002/58/EG i.V.m. RiLi 2009/136/EG:
☒ ja ☐ nein

4.1.4.2 Es gibt Subauftragnehmer außerhalb der EU, die Zugriff auf Daten des Auftraggebers haben:
☐ ja ☒ nein

4.1.4.3 Subauftragnehmer, die Zugriff auf Daten des Auftraggebers erhalten, halten die in dieser Checkliste vereinbarten technischen und organisatorischen Maßnahmen genauso wie der Auftragnehmer selbst ein und haben deren Einhaltung vertraglich zugesichert:
☐ ja ☒ nein

oder ☐ es wurden keine Subauftragnehmer beauftragt, die Zugriff auf Daten des Auftraggebers haben

4.1.5 Es erfolgen Schulungen der Mitarbeiter zum Datenschutz inkl. namensscharfer Dokumentation:
☐ ja ☒ nein

4.1.6 Für das Unternehmen des Auftragnehmers bestehen zurzeit folgende Zertifikate/Datenschutzkonzepte, die mit dieser Checkliste eingereicht werden (bitte Angabe von Titel und Datum): _____

4.1.7 Falls die Dienstleistung unter Zuhilfenahme von Cloud-Services erbracht wird (vgl. 1.1.1, 2.1.2, 4.1.4), wird ein Architekturbild mit eingereicht, aus dem die eingesetzten IT-Komponenten, Orte der Speicherung und die verwendeten Protokolle hervorgehen (bitte Angabe von Titel und Datum): _____

4.2 Sonstiges

4.2.1 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 (z.B. ISO 27001/2): _____
☐ Alternatives Verfahren (bitte benennen): _____

oder ☐ nicht zutreffend, Begründung: _____

4.2.2 Falls die Leistungen dieses Vertrages auch die Bereitstellung von Diensten oder die Entwicklung von Software umfassen (z.B. „Software as a Service“): Im Unternehmen des Auftragnehmers existieren Regelungen (bitte Angabe von Titel und Datum)

4.2.2.1 zum „Datenschutz durch Technikgestaltung“, um das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen (bspw. durch Maßnahmen wie Pseudonymisierung) zu berücksichtigen:
_____

4.2.2.2 zur Verwendung personenbezogener Daten in der Softwareentwicklung: _____

oder ☐ nicht zutreffend

4.2.3 Im Unternehmen des Auftragsnehmers existieren Regelungen zum Umgang mit Sicherheitsvorfällen:

4.2.3.1 ☒ nein ☐ ja (bitte die Regelung benennen): _____

Stellen diese auch eine unverzügliche Meldung an den Auftraggeber sicher?

4.2.3.2 ☒ nein ☐ ja (bitte Verfahren erläutern): _____

5. Unterschrift

Wir versichern, dass die hier getätigten Angaben dem aktuellen Stand der bei uns umgesetzten technischen und organisatorischen Maßnahmen zum Datenschutzniveau und zur Datensicherheit entsprechen. Abweichungen der hier getätigten Angaben sind unmittelbar an den Auftraggeber des Rahmenvertrages gem. Satz 1 dieser Checkliste zu melden.

_____
Name und Vorname der verantwortlichen Person, die die Checkliste ausgefüllt hat (Blockschrift)

_____ _____
Ort, Datum Unterschrift Auftragnehmer und Firmenstempel

[1] Gem. ePrivacy-Richtlinie oder -Verordnungen in ihrer jeweils gültigen Fassung i.V.m. nationalen Regelungen zum Fernmeldegeheimnis, z.B. § 88 TKG (für Deutschland).