Anlage zur Vereinbarung zur Erbringung von IoT-Leistungen: BODAS Connect

1 Vereinbarung gemäß Art. 26 Abs. 1 S. 1 Datenschutz-Grundverordnung (DSGVO)

Präambel

Der KUNDE als Besteller auf dieser Plattform und die Bosch Rexroth AG, gemeinsam benannt als PARTEIEN, arbeiten im Rahmen der Nutzung von IoT-Services arbeitsteilig zusammen. Dabei kommt es auch zu einer Verarbeitung von personenbezogenen Daten im Sinne des Art. 4 Nr. 1 Datenschutzgrundverordnung (nachfolgend „**DSGVO**“). Um den datenschutzrechtlichen Anforderungen gerecht zu werden und die größtmögliche Transparenz für die betroffenen Personen zu gewährleisten vereinbaren die PARTEIEN daher das Folgende.

1.1 Definitionen

Begriffe, die innerhalb der DSGVO definiert und in dieser Vereinbarung verwendet werden, haben die in der DSGVO festgelegte Bedeutung. Im Übrigen gelten die folgenden Definitionen:

„**Anwendbares Datenschutzrecht**“ ist das jeweils für die Vertragspartner in der Europäischen Union geltende Datenschutzrecht, einschließlich der DSGVO und den im Hoheitsgebiet eines Mitgliedsstaates der Union zu beachtenden nationalen Datenschutzgesetzen (insb. dem BDSG).

„**Betroffenenrechte**“ meint ein Ersuchen einer betroffenen Person, mit denen Rechte nach Art. 15 – Art. 22 DSGVO geltend gemacht werden.

„**Datenschutzvorfall**“ meint eine Verletzung des Schutzes personenbezogener Daten nach Maßgabe der Begriffsbestimmung in Art. 4 Nr. 12 DSGVO.

„**Zuständige Partei**“ meint die Partei, die entsprechend der Bestimmung in Ziffer 3 für die Erfüllung datenschutzrechtlicher Pflichten nach dem anwendbaren Datenschutzrecht zuständig ist.

„**Boschinterne Dienstleister**“ wie in Punkt 4 dieser Vereinbarung aufgelistet

1.2 Anwendungsbereich

Diese Vereinbarung findet ausschließlich auf Tätigkeiten Anwendung, in deren Rahmen die PARTEIEN gemeinsam personenbezogene Daten verarbeiten und regelt die in diesem Zusammenhang bestehenden Rechte und Pflichten. Die Regelungen dieser Vereinbarung erstrecken sich auch auf Auftragsverarbeiter, die von den PARTEIEN zur Verarbeitung von personenbezogenen Daten eingesetzt werden.

Die PARTEIEN haben die Mittel und Zwecke der in Punkt 2.1 bis 2.3 dargestellten Verarbeitungstätigkeiten gemeinsam festgelegt.

Abseits der gemeinsam durchgeführten, sich aus Punkt 2.1 bis 2.3 ergebenden Verarbeitungstätigkeiten, sind die PARTEIEN jeweils eigenständige Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO und selbständig für die Einhaltung des anwendbaren Datenschutzrechts verantwortlich.

1.3 Einhaltung des Datenschutzes

Jede Partei gewährleistet die Einhaltung des anwendbaren Datenschutzrechts, insbesondere die Rechtmäßigkeit der durch sie auch im Rahmen der gemeinsamen Verantwortlichkeit durchgeführten Verarbeitungstätigkeiten.

Die PARTEIEN ergreifen alle erforderlichen Maßnahmen, damit die Rechte der betroffenen Personen, insbesondere nach den Art. 12 bis 22 DSGVO, innerhalb der gesetzlichen Fristen jederzeit gewährleistet werden können bzw. sind.

Die PARTEIEN stellen sicher, dass angemessene technische und organisatorische Maßnahmen im Sinne des Art. 32 DSGVO sowie des Sicherheitskonzeptes aus Punkt 3 dieses Dokuments getroffen und die Grundsätze des Art. 25 DSGVO („Privacy by Design“ und „Privacy by Default“) eingehalten werden und dokumentieren die Einhaltung jeweils selbständig.

1.4 Zuständigkeiten für einzelne Verarbeitungstätigkeiten und Benachrichtigungspflichten

Im Rahmen der gemeinsamen Verantwortlichkeit gehen die PARTEIEN arbeitsteilig vor. Die Zuständigkeiten für einzelne Verarbeitungstätigkeiten ergeben sich aus Punkt 2.1 bis 2.3.

Soweit die PARTEIEN Unregelmäßigkeiten oder Fehler im Hinblick auf die Einhaltung datenschutzrechtlicher Bestimmungen feststellen, werden sich die PARTEIEN unverzüglich gegenseitig informieren.

1.5 Erfüllung der Informationspflichten gegenüber betroffenen Personen

Der KUNDE verpflichtet sich, der betroffenen Person die gemäß Art. 13 und 14 DSGVO erforderlichen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache unentgeltlich zur Verfügung zu stellen.

Jede Partei verpflichtet sich, die Angaben zur Erstellung der Informationen gemäß Art. 13 und 14 DSGVO zur Verfügung zu stellen, soweit sie für einzelne Verarbeitungstätigkeiten verantwortlich ist.

Die PARTEIEN werden den Inhalt der Informationen gemäß Art. 13 und 14 DSGVO vor Beginn der Verarbeitungstätigkeit miteinander abstimmen.

1.6 Umsetzung der Betroffenenrechte

Die betroffenen Personen können die ihnen aus Art. 15- 22 DSGVO zustehenden Rechte gegenüber beiden PARTEIEN geltend machen.

Bosch Rexroth übernimmt die Umsetzung der Betroffenenrechte und die gegebenenfalls erforderliche Kommunikation mit den betroffenen Personen.

Soweit sich eine betroffene Person an eine der PARTEIEN in Wahrnehmung ihrer Betroffenenrechte wendet, verpflichten sich die PARTEIEN, dieses Ersuchen unverzüglich unabhängig von der Pflicht zur Gewährleistung des Betroffenenrechtes an die andere Partei weiterzuleiten.

Sollte eine betroffene Person die Löschung ihrer personenbezogenen Daten verlangen, so werden sich die PARTEIEN umgehend gegenseitig über diesen Umstand informieren. Die jeweils andere Partei kann der Löschung aus berechtigtem Grund widersprechen.

Die PARTEIEN unterstützen sich gegenseitig bei der Umsetzung der Betroffenenrechte.

1.7 Zugänglichmachung dieser Vereinbarung

Der KUNDE verpflichtet sich, den wesentlichen Inhalt dieser Vereinbarung den betroffenen Personen gemäß Art. 26 Abs. 2 DSGVO zur Verfügung zu stellen.

1.8 Meldepflichten bei Datenschutzverletzungen

Bosch Rexroth obliegt die aus Art. 33, 34 DSGVO resultierenden Melde- und Benachrichtigungspflichten gegenüber der Aufsichtsbehörde und den von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen.

Die PARTEIEN informieren sich binnen 24 Stunden nach Bekanntwerden gegenseitig über Verletzungen des Schutzes personenbezogener Daten, die im Rahmen dieser Vereinbarung verarbeitet werden.

Die PARTEIEN unterstützen sich gegenseitig bei der Aufklärung des Sachverhalts und einer gegebenenfalls erforderlichen Meldung an die Aufsichtsbehörde und die betroffenen Personen.

1.9 Datenschutzfolgenabschätzung

Sofern erforderlich unterstützen sich die PARTEIEN gegenseitig bei der Durchführung einer Datenschutzfolgenabschätzung gemäß Art. 35 DSGVO.

1.10 Auftragsverarbeitung

Die PARTEIEN verpflichten sich, beim Einsatz von Auftragsverarbeitern im Anwendungsbereich dieser Vereinbarung einen Vertrag nach Art. 28 DSGVO abzuschließen und die schriftliche Zustimmung der anderen Vertragspartei vor Abschluss des Vertrages einzuholen.

Die PARTEIEN informieren sich gegenseitig rechtzeitig über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von als Subunternehmer eingesetzten Auftragsverarbeitern und beauftragen nur solche Subunternehmer, die die Anforderungen des Datenschutzrechts und die Festlegungen dieses Vertrages erfüllen.

Die PARTEIEN erstellen eine Übersicht der Auftragsverarbeiter im Anwendungsbereich dieser Vereinbarung gemäß Anlage 4.3.

1.11 Internationale Datenübermittlung

Befindet sich eine PARTEI außerhalb der EU/des EWR und in einem Land, für das kein angemessenes Datenschutzniveau anerkannt wird, Die PARTEIEN schließen Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer oder andere geeignete Vereinbarungen, die den Schutz personenbezogener Daten gewährleisten.

1.12 Haftung

Unbeschadet der Regelungen des Art. 82 DSGVO und unbeschadet der Regelungen dieses Vertrages haften die PARTEIEN für den Schaden, der durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wird, im Außenverhältnis gemeinsam gegenüber den betroffenen Personen.

1.13 Sonstiges

Eine unwirksame oder undurchführbare Bestimmung dieser Vereinbarung berührt die übrigen Bestimmungen dieser Vereinbarung nicht. In einem solchen Fall wird die unwirksame oder undurchführbare Bestimmung automatisch durch eine wirksame und durchsetzbare Bestimmung ersetzt, die dem Zweck der ursprünglichen Bestimmung am nächsten kommt.

2 Erfassung von Datenverarbeitungstätigkeiten im Rahmen von Projekten in gemeinsamer Verantwortung (Art. 26 DSGVO)

2.1 Stammdaten

2.1.1 Basisinformationen

Bezeichnung der Verarbeitung: Stammdaten erfassen

Verantwortlich für die Stammdatenerfassung und Pflege ist der KUNDE

Ansprechpartner ist der kundenseitige Besteller/Einkäufer auf dem Rexroth-Marketplace sofern nicht anders vereinbart.

Beschreibung:

- Erfassen der Mitarbeiterdaten für Login
- Zuordnung der User zum Kunden
- Erfassen der Maschinendaten auf dem Device Portal und Data Management Portal

Datenfluss:

Ein Mitarbeiter des Kunden gibt relevante Angaben (z.B. Name, Vorname, Email, Telefon-Nummer) beim Online-Registrierungsportal von Bosch ein und erhält seine User-Kennung mit Passwort zurück. Diese Informationen werden bei unserem Boschinternen Dienstleister gespeichert. (einmalig)

Nach erfolgtem Login werden die Informationen zu den zu verwaltenden Geräten im Device Portal bzw. dem Data Management Portal erfasst. Die Eingaben zu den Geräten bzw. vorgenommene Änderungen an den Informationen werden in Log-Files gespeichert

(inkl. User-ID des Mitarbeiters des Kunden, der diese Änderungen vorgenommen hat). Diese Informationen werden bei unserem Boschinternen Dienstleister gespeichert.

Die Datenverarbeitung dient folgenden Zwecken:

- Lizenzierung und Registrierung
- Verwaltung von IoT-Devices inkl. Verwaltung durchgeführter Software-Updates auf diesen Geräten

2.1.2 Betroffene Personen und betroffene Datenarten

Von der Datenverarbeitung sind die Mitarbeiter des KUNDEN betroffen.

Folgende Datenarten sind von der Datenverarbeitung betroffen:

- persönliche Details
- Log- und Protokolldaten

2.1.3 Art und Weise der Datenverarbeitung

- Zur Verarbeitung der Daten wird die Server-Infrastruktur bei Boschinternen Dienstleister eingesetzt.
- Im Rahmen der Datenverarbeitung werden keine personenbezogenen Daten in einen Staat außerhalb der EU übermittelt oder dort verarbeitet.

2.1.4 Zusätzliche Regelungen in anderen Jurisdiktionen

- Russische Föderation
  - Keine Datenverarbeitung in Bezug auf russische Staatsbürger, da russische Staatsbürger keine personenbezogenen Daten wie eigene Namen als Login-Daten verwenden dürfen.

2.2 Device Management

2.2.1 Basisinformationen

Bezeichnung der Verarbeitung: Device Management

Verantwortlicher ist die Bosch Rexroth AG

Ansprechpartner beim Verantwortlichen ist die Abteilung DC-MH/PJ-IOT

Beschreibung:

Die Verarbeitung dient der Verwaltung der IoT-Endgeräte

Datenfluss:

Informationen (z.B. Seriennummer, MAC-Adresse, Software-Stand, Geoposition, Daten der SIM-Karte und weitere kunden-spezifische Angaben) zu den IoT-Endgeräten werden auf einem Server gespeichert. Durch maschinellen Abgleich der gespeicherten IoT-Daten aus der Seriennummer und dem gespeicherten Softwarestand mit den durch die Entwicklungsabteilungen gepflegten aktuellen Softwarenständen für das jeweilige Produkt werden Informationen zu neuen SW-Updates für die vorhandenen IoT-Endgeräte dem

Kunden bei der nächsten Anmeldung am Device Portal zur Verfügung gestellt. Der Status der IoT-Endgeräte wird dem KUNDE angezeigt. Entsprechende Daten werden nicht dauerhaft gespeichert. Diese Tätigkeiten werden durch unseren Boschinternen Dienstleister durchgeführt.

Die Datenverarbeitung dient folgenden Zwecken

- Verwaltung von IoT-Devices
- Ermittlung von Software-Updates zu den gespeicherten IoT-Devices
- Information über notwendige Updates bei nächster Anmeldung durch Mitarbeiter des KUNDEN

2.2.2 Betroffene Personen und betroffene Datenarten

Folgende Kategorien von Personen sind von der Datenverarbeitung betroffen:

- Mitarbeiter
- Mitarbeiter des KUNDEN

Diese Datentypen sind von der Datenverarbeitung betroffen:

- Log- und Protokolldaten

2.2.3 Art und Weise der Datenverarbeitung

Folgende technischen Mittel werden zur Datenverarbeitung eingesetzt

- Server-Infrastruktur bei Boschinternen Dienstleister.
- Cloudbasierte SaaS-Anwendung bei Externem Dienstleister zur Bereitstellung von Update-Paketen

Im Rahmen der Datenverarbeitung werden keine personenbezogenen Daten in einen Staat außerhalb der EU übermittelt oder dort verarbeitet.

2.3 Datenmanagement

2.3.1 Basisinformationen

Bezeichnung der Verarbeitung: Datenmanagement

Verantwortlicher ist die Bosch Rexroth AG

Ansprechpartner beim Verantwortlichen ist die Abteilung DC-MH/PJ-IOT

Beschreibung:

Datenhaltung, Datenverarbeitung und Datenvisualisierung

Datenfluss:

Daten (z.B. Geoposition, Prozessdaten wie Geschwindigkeit, Drücke, Verbrauch von Verbrauchsmaterialien) aus den angeschlossenen Maschinen werden auf Servern in Datenbanken gespeichert. Diese Daten sind auf den Datenbanken durchsuchbar. Die

Daten werden auf den Servern verarbeitet und in einem Frontend visualisiert. Die Daten können heruntergeladen werden. Darüber hinaus sind die Funktionen des Daten-Managements unabhängig vom Frontend per REST API ausführbar. Diese Tätigkeiten werden durch interne Dienstleister von Bosch Rexroth und Robert Bosch GmbH durchgeführt.

Die Datenverarbeitung dient zum Zweck der Übersicht und Analyse der Nutzung und des Verhaltens von Maschinenflotten

2.3.2 Betroffene Personen und betroffene Datenarten

Welche Kategorien von Personen können von der Datenverarbeitung betroffen sein?

- Mitarbeiter
- Mitarbeiter des KUNDEN

Welche Datentypen können von der Datenverarbeitung betroffen sein?

- Log- und Protokolldaten

2.3.3 Art und Weise der Datenverarbeitung

Welche technischen Mittel werden zur Datenverarbeitung eingesetzt?

Server-Infrastruktur bei Boschinternen Dienstleister.

Im Rahmen der Datenverarbeitung werden keine personenbezogenen Daten in einen Staat außerhalb der EU übermittelt oder dort verarbeitet.

3 Technisch-organisatorische Maßnahmen/Sicherheitskonzept

3.1 Maßnahmen zur Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b) DS-GVO)

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen
- Zugangskontrolle
  Keine unbefugte Systembenutzung, z. B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z. B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z. B. Mandantenfähigkeit, Sandboxing

3.2 Maßnahmen zur Gewährleistung der Integrität (Art. 32 Abs. 1 lit. b) DS-GVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur
- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind, z. B.: Protokollierung, Dokumentenmanagement

3.3 Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DS-GVO) z. B.

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z. B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne
- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z. B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen
- Belastbarkeit
  Systeme und Dienste (z. B. Speicher-, Zugriffs-, Leitungskapazitäten etc.) sind so ausgelegt, dass auch punktuelle hohe Belastungen oder hohe Dauerbelastungen von Verarbeitungen möglich sind

3.4 Maßnahmen zur Pseudonymisierung personenbezogener Daten z. B.

- Trennung von Kundenstammdaten und Kundenumsatzdaten
- Verwendung von Personal-, Kunden-, Lieferanten-Kennziffern statt Namen

3.5 Maßnahmen zur Verschlüsselung personenbezogenen Daten, z. B.

- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Hashing

3.6 Maßnahmen, um nach einem physischen oder technischen Zwischenfall die Verfügbarkeit personenbezogener Daten zu ihnen rasch wiederherzustellen, z. B.

- Back-up Konzept
- Redundante Datenspeicherung
- Doppelte IT-Infrastruktur
- Schatten-Rechenzentrum

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

- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Prüfungen des DSB, der IT-Revision
- Externe Prüfungen, Audits, Zertifizierungen

4 Unterauftragnehmer der PARTEIEN

Name, Adresse des 1. Unterauftragnehmers:

Robert Bosch Manufacturing Solutions GmbH
Bosch Connected Industries

Leistungsumfang: Nexeed Device Portal

Ort der Datenverarbeitung: Wernerstraße 51, 70469 Stuttgart

Verarbeitung / Zugang zu personenbezogenen Daten (Datentyp und Kreis der betroffenen Personen)

Datentyp:
Login Daten der IoT Devices
Kommunikationsdaten (Email; Bosch global User ID (CIAM))
Andere: TenantID (MandatesID), Nutzer Zugangsrollen und Zugangsrechte, Device Information, Device Backups

Kreis der betroffenen Personen:
Kunden oder Nutzer des Service (hier: Nutzer des Device Portals)

Name, Adresse des 2. Unterauftragnehmers

Robert Bosch GmbH

Leistungsumfang: Bosch IoT Insights

Ort der Datenverarbeitung: Postfach 300240, 70442 Stuttgart, GERMANY

Verarbeitung / Zugang zu personenbezogenen Daten (Datentyp und Kreis der betroffenen Personen)

Datentyp:
Communication data (Email; Bosch global User ID (CIAM))
Andere: Device Information, Lokalisierung, Technische Fahrzeugdaten, TenantID, User access roles and user access rights

Kreis der betroffenen Personen:
Kunden oder Nutzer des Service (hier: Nutzer des Data Management Portals)