1 Datenschutzhinweise zur Nutzung der BlueID Lock Admin App

Zur Bereitstellung einer sicheren Infrastruktur für Berechtigungsmanagement und deren Anwendung stellt die BlueID GmbH die Lock Admin App zur Verfügung. Bei der Nutzung dieser App werden personenbezogene Daten verarbeitet.

Diese Lock Admin App wird von der BlueID GmbH und dem Tenant (Organisation/Kunde der BlueID) gemeinsam betrieben (Gemeinsam Verantwortliche i.S.v. Art. 26 DSGVO).

BlueID übernimmt alle Verpflichtungen der Datenschutzgrundverordnung und anderer nationaler Datenschutzgesetze der Mitgliedsstaaten sowie sonstiger datenschutzrechtlicher Bestimmungen für die Backend Funktionalität, der Tenant für den Bereich der Vergabe der Berechtigung zur Anwendung der Funktionalität. Dies betrifft insbesondere die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO, die Wahrnehmung der Rechte der betroffenen Person und die Informationspflichten gemäß den Artikeln 13 und 14. Unabhängig davon können Sie ihre Rechte als betroffene Person gegenüber jedem einzelnen der Verantwortlichen geltend machen.

1.1 Beschreibung und Umfang der Datenverarbeitung

Die BlueID Lock Admin App erlaubt die administrative Betreuung (Installation und Wartung von Schlössern) durch qualifiziertes Wartungspersonal. Die Einladung und Freischaltung des Accounts erfolgt hierbei durch den Tenant (Organisation/Kunde der BlueID).

Folgende Daten werden verarbeitet

Login Daten:

- Benutzername (frei wählbar, nicht zwingend personenbezogen)
- gehashtes Passwort

Mit dem Account verknüpfte Device Daten:

- Berechtigungen für die zu wartenden Schlösser
- Informationen über die Schlösser: Versionsinformationen, Hardwareinformationen, Fehlercodes

Protokolldaten:

- Zugriffe, Zugriffsversuche auf verwaltetet Schlösser (nach manuellem Abruf durch das Wartungspersonal)

1.2 Rechtsgrundlage für die Datenverarbeitung

Rechtsgrundlage für die Verarbeitung der Daten ist Art. 6 Abs. 1 lit. f DSGVO.
Sofern mit dem Administrator ein persönliches Vertragsverhältnis vorliegt ist die Rechtsgrundlage Art. 6 Abs. 1 lit. b DSGVO.

Wenn der Administrator Beschäftigter des Tenants ist, gilt für die Verarbeitung seiner Daten durch seinen Arbeitgeber Art. 88 DSGVO i. V. m. § 26 (1) Satz 1 BDSG n.F..

1.3 Zweck der Datenverarbeitung

Zweck der Verarbeitung der personenbezogenen Daten ist die Bereitstellung einer sicheren Infrastruktur für Berechtigungsmanagement und deren Anwendung in Schlössern.

Der Zweck der Verarbeitung der Daten innerhalb der App liegt in einer gesicherten Anmeldung (Login-Daten - Sicherung gegen Missbrauch), der Möglichkeit der Erstellung von Berechtigungen (Device Daten - Notwendig für die zu erfüllende Aufgabe) und der Nachvollziehbarkeit der Aktionen bei Fehlern (Protokolldaten – Fehleranalyse/Verbesserung des Produkts).

In den angegebenen Sachverhalten liegt auch das berechtigte Interesse an der Verarbeitung dieser Daten.

1.4 Dauer der Speicherung

Die während der App-Nutzung verarbeiteten Daten im Backend werden gelöscht, wenn diese für die Zwecke der Verarbeitung nicht mehr erforderlich sind. Unabhängig davon kann eine Erforderlichkeit bestehen, personenbezogene Daten weiter zu speichern, um vertraglichen oder gesetzlichen Verpflichtungen nachzukommen (z.B. Nachweispflichten, Aufbewahrungspflichten).

Die Daten auf dem Mobiltelefon werden gelöscht, wenn die App gelöscht wird.

1.5 Widerspruchs- und Beseitigungsmöglichkeit

Wenn die Admin Funktion nicht mehr weiter ausgeführt wird, ist es möglich, den Account über das Löschen der App aufzulösen.

In diesem Fall werden die persönlichen Daten (Benutzername, Passwort) gelöscht. Berechtigungs- und Devicedaten bleiben im Backend für eine weitere Nutzung durch den Tenant (Organisation/Kunde von BlueID) erhalten, um die Administration der Schlösser auf einen neuen Administrator zu übertragen.

Für Fragen bezüglich des Datenschutzes wenden Sie sich bitte an die BlueID GmbH oder direkt an unseren Datenschutzbeauftragten Herrn Dr. Kohfeldt (datenschutz@BlueID.net)