Datenschutzhinweis

ASSA ABLOY
Opening Solutions

Informationen zur Clex private-Schließsystemfamilie (CX2120, CX2130, CX2140, CX2160, CX2170)

23.01.2026

Experience a safer and more open world

Hersteller / Dienstleister:
Uhlmann & Zacher GmbH, Gutenbergstraße 2-4, 97297 Waldbüttelbrunn

1. Einleitung

1.1 Allgemeines

Diese Datenschutzerklärung erläutert, wie Daten, die durch die Clex private-Schließsystemfamilie (das „**Produkt**“) generiert oder erfasst werden, abgerufen, verwendet und weitergegeben werden (einschließlich der Bereitstellung von ClexFWProg, Keyng App, Keyng Software, Clex Key App, ClexTouch (der „**Dienst**“)), und wie die Daten im Übrigen gemäß den Anforderungen von Artikel 3 des EU-Datenschutzgesetzes verarbeitet werden.

1.2 Produkt- und Servicebeschreibung

Die Clex private-Schließsystemfamilie (CX2120, CX2130, CX2140, CX2160, CX2170) ist eine globale Plattform für das Zutrittsmanagement. Das Produkt generiert Audit-Trails (Anmeldeinformationstyp, Anmeldeinformations-ID(s) – ohne Zuordnung von Benutzernamen), Ereignisprotokolle (wichtige Geräteereignisse außer Kartenlesevorgängen), Diagnosezähler, Batteriestatus sowie Sensor- oder Betriebsalarme der Schließkreise. Die Daten werden während des Betriebs erfasst und auf dem Gerät, dem Smartphone oder dem PC des Systemadministrators gespeichert. Die Audit-Trails werden dauerhaft gespeichert, bis sie durch neuere Datensätze überschrieben werden.

1.3 Dateninhaber

Clex-Systeme werden vom Systeminhaber/Kunden vor Ort gehostet. Daher hat nur der Systeminhaber Zugriff auf die generierten Daten.

1.4 Nutzungsbedingungen und Servicequalität

Die neueste Version finden Sie online unter folgender Adresse:
https://www.uhlmannzacher.com/de/de/agb

2. Daten, die das Produkt generieren kann

Produktname	Art der Daten	Format	Geschätztes Volumen	Häufigkeit der Datensammlung	Datenaufbe-wahrung
Clex private Schließsystem-familie (CX2120, CX2130, CX2140, CX2160, CX2170)	Audit-Trails (Anmeldeinforma-tionstyp, Anmeldeinforma-tions-ID oder IDs - ohne Kenntnis des zugehörigen Benutzernamens), Ereignisprotokolle einschließlich wichtiger Geräte-ereignisse mit Ausnahme von Kartenleseaktivitäten, verschiedene Zähler für Diagnosedaten, Batteriestatus, Sensor- oder Betriebsalarme der Schließkreise.	Byte-Array, nur maschinen-lesbar	Prüfeinträge: jeweils 16 Byte nach dem FIFO-Prinzip (First-In, First-Out), bis zu 512 Einträge; Zähler werden auf dem Gerät gespeichert und bei Bedarf übertragen.	Die Daten werden kontinuierlich und in Echtzeit generiert.	Die Protokolle der Sperren werden so lange gespeichert, bis sie durch neuere Datensätze überschrieben werden.

3. Vom Dienst erhaltene Daten

Dienstname	Art der Daten	Format	Geschätztes Volumen	Datenaufbewahrung
Clex SCT	Systemprotokoll (Benutzeraktivitäten, Fehler, Importe)	Textprotokoll (ca. 250 Bytes/Eintrag)	Etwa 250 Bytes pro Eintrag	Wird aufbewahrt, bis der Benutzer es löscht oder die Protokollrotation erfolgt
ClexFWProg	Protokolle aktualisieren	XML (gzipped)	Ca. 3.000 Bytes pro Update (XML, gzipped)	Wird nur bei manueller Aktualisierung gespeichert; wird nach der Übertragung gelöscht
Keyng App	Systemprotokoll, Ereignis-/Zugriffsprotokoll des Produkts	Byte-Array (Ereignisse), Textprotokoll (Systemprotokoll)	50 Bytes (Systemprotokoll), 20 Bytes (Ereignis)	Wird beibehalten, bis der Benutzer die App löscht oder neu installiert.
Keyng Software	Systemprotokoll, Ereignis-/Zugriffsprotokoll des Produkts	Einfacher Text	50 Bytes (Systemprotokoll), 20 Bytes (Ereignis)	Wird lokal gespeichert, bis der Benutzer es löscht oder die Protokollrotation erfolgt
Clex Key App	Ereignisprotokoll der Zugriffsversuche, Systemprotokoll mit technischen Details	Byte-Array (Ereignis), Textprotokoll (System)	20 Bytes (Ereignis), 50 kB (Systemprotokoll)	Ereignisprotokolle pro Versuch; Systemprotokolle bis zur Löschung oder Neuinstallation

4. Datenzugriff und Benutzerfunktionen

Direkter Datenzugriff	Indirekter Datenzugriff	Datenlöschung
Benutzer können über Konfigurationstools, mobile Apps oder PC-Software direkt auf Prüfprotokolle und Ereignisprotokolle zugreifen.	N/A – Uhlmann & Zacher ist kein Dateninhaber. Der Systembetreiber ist der Dateninhaber.	Benutzer können Produktdaten löschen, indem sie das Gerät auf Werkseinstellungen zurücksetzen oder die Daten über die Service-Software löschen.

5. Wie Sie die Freigabe von Daten beantragen

Da die vom Dienst generierten Daten direkt vom Systeminhaber/Kunden oder dessen Zutrittskontrollsystemanbieter verwaltet werden, können diese, wie oben beschrieben, direkt auf die generierten Daten zugreifen und sie nach eigenem Ermessen mit Dritten teilen.

6. Recht auf Einreichung einer Beschwerde

Wenn Sie der Ansicht sind, dass unsere Verarbeitung Ihrer Daten Ihre Rechte gemäß den geltenden Gesetzen verletzt, haben Sie das Recht, eine Beschwerde bei der zuständigen Behörde in Ihrem Zuständigkeitsbereich einzureichen.

7. Geschäftsgeheimnisse

In einigen Fällen können Daten aus den verbundenen Produkten oder zugehörigen Diensten Geschäftsgeheimnisse enthalten, die uns oder unseren Partnern gehören. Geschäftsgeheimnisse werden nur dann geschützt und offengelegt, wenn zuvor alle erforderlichen Maßnahmen zum Schutz ihrer Vertraulichkeit getroffen wurden, insbesondere im Hinblick auf Dritte. In Ausnahmefällen kann unser Zugriff auf Daten aufgrund von Geschäftsgeheimnissen eingeschränkt sein.

8. Laufzeit und Kündigung

Ihre Vereinbarung zur Nutzung des Dienstes beginnt mit dem Datum Ihrer Zustimmung zu den Nutzungsbedingungen und gilt für die Dauer Ihrer Nutzung. Sie können den Vertrag beenden, indem Sie die in der Kündigungsklausel beschriebenen Schritte befolgen.

9. Kontaktinformationen

Sollten Sie Fragen zu den durch das Produkt oder den Service generierten Daten haben, zögern Sie nicht, uns unter order@uundz.de zu kontaktieren.