

Axon Evidence, unsere in der Cloud gehostete Lösung, wird auf einer Infrastructure as a Service (IaaS)-Plattform betrieben, die von Microsoft Azure bereitgestellt wird. Alle Azure-Rechenzentren und Infrastrukturdienste sind nach ISO 27001 zertifiziert und erfüllen die DSGVO-/GDPR-Anforderungen an die Datensicherheit.

Axon Evidence wird in Microsoft Azure-Rechenzentren in der Europäischen Union (Niederlande und Irland) gehostet. Somit wird sichergestellt, dass alle Beweisdaten, einschließlich der Datensicherung (Backup), in der EU gehostet werden und dort verbleiben.

Ein grundlegender Vorteil der gehosteten Software-as-a-Service (SaaS) Lösung besteht darin, dass sie eine automatische, elastische Skalierung für bestimmte große Arbeitslasten über die Microsoft Azure Cloud unterstützt. Die Anwendung überwacht automatisch die CPU-Auslastung und die Menge der Anfragen, um festzustellen, wann zusätzliche Maschinen hinzugefügt oder entfernt werden müssen. Axon verwaltet aktuell mehr als 300 PB (Petabyte) an Daten und 500.000 Benutzerkonten in unserem globalen Kundennetzwerk.

WIE IHRE DATEN IN DER CLOUD GESCHÜTZT SIND:

ZUGANG UND AUTHENTIFIZIERUNG

Die Kunden sind innerhalb der Axon Cloud Services logisch segmentiert und können nicht auf die Daten anderer Kunden zugreifen. Axon-Mitarbeiter haben keinen Zugriff auf die Daten eines Kunden ohne dessen ausdrückliche Genehmigung. Eine Ausnahme bildet ein kleines Team von Systemadministratoren, die nur im Falle eines Systemnotfalls auf die Daten zugreifen können. Um Zugang zu Kundendaten zu erhalten, authentifiziert sich dieses Team über mindestens zwei Faktoren (Benutzername und Passwort sowie ein zeitbasiertes Sicherheits-Token). Alle Mitarbeiter, die im Rahmen ihrer beruflichen Tätigkeit mit Daten von Kunden in Berührung kommen können, unterliegen zusätzlichen Sicherheitsüberprüfungen oder entsprechenden lokalen Entscheidungsprozessen.

VERSCHLÜSSELUNG

Die Beweisdaten werden bei der Übertragung und bei der Speicherung verschlüsselt. Axon verwendet ausgereifte, geprüfte Verfahren zur Verwaltung von Verschlüsselungscodes, die den ISO 27000-Normen entsprechen.

Datenverschlüsselung bei der Übermittlung:

- TLS 1.2 Implementierung mit 256-Bit-Verbindung, RSA 2048-Bit-Schlüssel, Perfect Forward Secrecy

Verschlüsselung von gespeicherten Beweisdaten:

- CJIS-konform, NSA Suite B 256 Bit AES-Verschlüsselung

GEMEINSAME VERANTWORTUNG FÜR DIE SICHERHEIT

Axon Evidence verwendet eine Multi-Mandanten-Architektur. Jeder Kunde hat seinen eigenen isolierten Mandanten und sein eigenes Speicherkonto.

Es ist wichtig, die Kunden über die Maßnahmen zu unterrichten, die Axon zur Sicherung von Axon Evidence unternimmt, da diese von unseren fortschrittlichen Sicherheitsfunktionen, Kontrollmechanismen und Sicherheitsprogrammen profitieren.

Durch die Verwendung dieser Sicherheitsmechanismen können Kunden einen Grad an Datensicherheit erreichen, der weit über das hinausgeht, was bei einer On-Premise- oder Hybrid-Lösungen möglich ist. Es ist jedoch auch von entscheidender Bedeutung, dass die Kunden die Sicherheitspraktiken, die in ihrer Verantwortung und unter ihrer Kontrolle liegen, verstehen und umsetzen.



AUTHENTIFIZIERUNG

- Multi-Faktor-Authentifizierungsoptionen für die Benutzeranmeldung und vor administrativen Aktionen (einmaliger Code per SMS oder Telefonrückruf)
- Anpassbare Passwortlänge und komplexe Passwortanforderungen
- Anpassbares Limit für fehlgeschlagene Anmeldungen und Dauer der Sperre
- Erzwungene Sitzungs-Timeout-Einstellungen
- Obligatorische Kontrollfragen bei der Authentifizierung von neuen Standorten aus
- Beschränkung des Zugriffs auf bestimmte IP-Bereiche (Beschränkung des Zugriffs auf genehmigte Bürostandorte)



SICHERES TEILEN

- Behördeninterner, behördenübergreifender und externer Austausch von Beweismitteln ohne Datentransfer, Datenvervielfältigung, physische Datenträger oder E-Mail Anhänge
- Detaillierte Protokollierung der Beweiskette (chain-of-custody) beim Austausch
- Widerruf des Zugriffs auf zuvor freigegebene Inhalte
- Verhindern, dass ein Empfänger eines freigegebenen Inhalts Beweise herunterlädt oder erneut weitergibt



AUTORISIERUNG & ERLAUBNIS

- Granulare rollenbasierte Rechteverwaltung
- Verwaltung von Anwendungsberechtigungen (z. B. bestimmten Nutzern die Nutzung der webbasierten Schnittstelle, nicht aber einer mobilen Anwendung erlauben)
- Integration mit Verzeichnisdiensten (z.B. Active Directory) für eine optimierte und sichere Benutzerverwaltung



AUDITIERUNG UND BENUTZERBERICHTERSTATTUNG UND -VERWALTUNG

- Detaillierte, manipulationssichere Protokollierung von Administrator- und Benutzeraktivitäten
- Intuitives Administrations-Webportal zur Verwaltung von Benutzern, Berechtigungen und Rollen

INTEGRITÄT DER BEWEISE

Axon Evidence enthält Funktionen, die die Integrität und Authentizität digitaler Beweismittel sicherstellen. Diese Funktionen stellen sicher, dass die Beweise die Anforderungen an die Beweiskette erfüllen und dass sie nachweislich authentisch und frei von Manipulationen sind.

- Forensischer Fingerabdruck jeder einzelnen digitalen Beweismittels unter Verwendung der Hash-Funktion SHA nach Industriestandard. Die Integrität wird vor und nach dem Hochladen überprüft, um sicherzustellen, dass während der Übertragung keine Änderungen vorgenommen wurden.
- Vollständig manipulationssichere Aufzeichnungen zur Beweismittelprüfung. Protokolliert das Wann, Wer und Was für jedes Beweismittel. Diese Aufzeichnungen können nicht bearbeitet oder geändert werden, auch nicht von Administratoren.
- Die originalen digitalen Beweismittel werden nie verändert, auch nicht, wenn Ausschnitte (Videosegmente) erstellt werden.
- Löschschutz, einschließlich Löschgenehmigungs-Workflows, Löschenachrichtigungs-E-Mails und einer Wiederherstellungsfrist für die Wiederherstellung versehentlich gelöschter Beweisdateien.

Axon hat ein Compliance-Programm mit wesentlichen Datenschutz- und Sicherheitsrichtlinien und -praktiken entwickelt, um die Daten zu schützen, die unsere Systeme durchlaufen. Diese Richtlinien und Praktiken werden auf die Daten angewendet, die wir im Auftrag eines Kunden verarbeiten, und sind auch in das Produktdesign und die Funktionalität der Axon-Produkte integriert. Auf diese Weise können Kunden die Handhabung und den Austausch digitaler Beweise regeln, um ihre Anforderungen gemäß den verschiedenen Datenschutzgesetzen zu erfüllen.

Axon erfüllt die Anforderungen der Datenschutz-Grundverordnung (DSGVO), wie sie in das nationale Recht der jeweiligen Mitgliedstaaten umgesetzt wurde und wir gehen mit unserem Compliance-Programm noch einen Schritt weiter.

Um unseren Kunden einen transparenten Rahmen zur Messung unserer Datenschutz- und Sicherheitspraktiken zu bieten - insbesondere unserer Softwareentwicklungs- und Datenverwaltungspraktiken - hat es sich Axon zur Aufgabe gemacht, allgemein anerkannte Zertifizierungen und Berichterstattungsprozesse zu befolgen und zu erhalten, die Industriestandard-Praktiken nachweisen.

- ISO 27001:2013 - Verwaltung der Informationssicherheit
- ISO 27002:2013 - Informationssicherheitskontrollen
- ISO 27017:2015 - Informationssicherheitskontrollen für Cloud-Dienste
- ISO 27018:2019 - Schutz personenbezogener Daten in der Cloud
- ISO 27701:2019 - Datenschutz-Informationssystem
- Cloud Security Alliance Security Trust Assurance and Risk (CSA STAR) - Level 1 & Level 2
- Erfüllung des AICPA SOC 2 Typ 2 Berichterstattung Standard
- ISO 9001:2015 - Qualitätsmanagement-System

AUFBEWAHRUNG UND LÖSCHUNG

Axon Evidence ermöglicht es dem Kunden, die Aufbewahrungsfristen für digitale Beweismittel gemäß seinen internen Aufbewahrungsrichtlinien und -verfahren zu definieren. Daher kontrolliert der Kunde die Aufbewahrung und Löschung seiner Beweisdaten und Metadaten in Axon Evidence. Axon Evidence kann wöchentliche Nachrichten mit einer Zusammenfassung anstehender behördenweiter Löschungen an alle Kundenadministratoren automatisieren und ermöglicht eine 7-tägige Wiederherstellungsfrist nach der Löschung. Die Verarbeitung der Datenlöschung kann asynchron über Speichersysteme und Rechenzentren hinweg erfolgen. Während und nach der Verarbeitung der finalen Datenlöschung können Beweise nicht wiederhergestellt werden.

Falls ein Kunde die Nutzung von Axon Evidence einstellt (Vertragskündigung), wird Axon innerhalb von 90 Tagen nach der Kündigung keine digitalen Beweismittel löschen. Auf schriftliche Anfrage wird Axon einen schriftlichen Nachweis erbringen, dass alle Kundeninhalte erfolgreich gelöscht und aus Axon Evidence entfernt wurden, wie in den Axon Cloud Services Datenschutzbestimmungen beschrieben:

<https://www.axon.com/legal/cloud-services-privacy-policy>.

DATENSCHUTZ

Neben den aktuellen Datenschutz- und Sicherheitsfunktionen ist Axon bestrebt, seine Produkte und sein Compliance-Programm weiterzuentwickeln und zu verbessern. Diese Verbesserungen können unseren Kunden dabei helfen, die strengen Datenschutz- und Sicherheitserwartungen ihrer Gemeinschaften und des regulatorischen Umfelds zu erfüllen. Darüber hinaus wird sich Axon Prüfungen durch Kunden sowie Aufsichtsbehörden oder anderen zuständigen Behörden unterziehen. Wir verpflichten uns dazu:

- Einhaltung der sich ändernden Datenschutz- und Sicherheitsanforderungen durch kontinuierliche Beobachtung der Entwicklung von Datenschutzgesetzen und Branchenstandards
- Gegebenenfalls Durchführung von Datenschutz-Folgenabschätzungen

Axon bietet eine solide Datenverarbeitungsvereinbarung an, die alle erforderlichen Bedingungen der DSGVO / GDPR und UK-GDPR enthält und somit sicherstellt, dass Axon vertraglich verpflichtet ist, unsere Datenschutz- und Sicherheitsverpflichtungen zu erfüllen. Die Anbieter sind vertraglich verpflichtet, die gleichen Datenschutz- und Sicherheitsverpflichtungen einzuhalten, die Axon gegenüber seinen Kunden eingeht.

Für die Datenaufbewahrung bietet Axon einen konfigurierbaren Ansatz, der es den Kunden ermöglicht, den Zeitrahmen für die Datenaufbewahrung zu definieren, der für ihre Beweisdaten gilt. Bei den "Data Subject Rights" (Rechte der betroffenen Person) haben die Kunden die Kontrolle über ihre Daten, so dass sie auf Anfragen von Personen reagieren können, die ihre DSGVO- / GDPR- und UK-GDPR-"Data Subject Rights" ausüben. Axon unterstützt die Kunden, wenn zusätzliche Hilfe benötigt wird, um diese Anfragen zu erfüllen.

Die oben genannten Funktionen zeigen einige der datenschutz- und sicherheitsorientierten Funktionen, die bei Axon verfügbar sind. Weitere Informationen finden Sie unter [axon.com/privacy](https://www.axon.com/privacy) und [axon.com/security](https://www.axon.com/security).