MILLIONENRISIKO: DATENFRIEDHÖFE

Wieso die DSGVO Unternehmen dazu zwingt, ihre IT-Infrastruktur auf den Prüfstand zu stellen

In einer Pressemitteilung verkündete die Berliner Datenschutzbeauftragte am 5. November die Verhängung eines hohen Bußgeldes

14,5 Millionen Euro soll Deutsche Wohnen zahlen, da personenbezogene Daten in einem Archivsystem nicht DSGVO-konform gespeichert wurden.

Das Problem: Bei Deutsche Wohnen wurden Mieterdaten in einem Archiv gespeichert, ohne diese nach Ablauf einer nachvollziehbaren Nutzungsdauer wieder zu löschen. Seitdem die DSGVO im Mai 2018 in Kraft getreten ist, sind Unternehmen verpflichtet, die Speicherung personenbezogener Daten mit einem "Haltbarkeitsdatum" zu versehen, nach dessen Ablauf die Daten gelöscht werden müssen.

Die Datenschutzbeauftrage machte in ihrer Mitteilung deutlich, dass die bei Deutsche Wohnen festgestellten Mängel kein Einzelfall seien, und forderte Unternehmen auf, ihre Datenarchive zu überprüfen:
„Datenfriedhöfe, wie wir sie bei der Deutsche Wohnen SE vorgefunden haben, begegnen uns in der Aufsichtspraxis leider häufig. […] Ich empfehle allen datenverarbeitenden Stellen, ihre Datenarchivierung auf Vereinbarkeit mit der DS-GVO zu überprüfen."

Der Teufel liegt im Detail

Gerade in der heutigen Zeit, in der Unternehmen unter Hochdruck das Internet der Dinge ausbauen und in datenbasierte Geschäftsmodelle investieren, kann sich niemand erlauben, das mit der DSGVO verbundene Bußgeldrisiko auf die leichte Schulter zu nehmen. Doch der Teufel liegt im Detail und viele Unternehmen kommen ihrer Verantwortung nicht ausreichend nach. Denn Datenarchive, die aus der Zeit vor der DSGVO stammen, lassen sich architekturbedingt nur schwer an die neuen Anforderungen des Datenschutzes anpassen.

Die Anforderung: Ein heute abgelegter persönlicher Datensatz muss zu einem beliebigen Zeitpunkt in der Zukunft nachweislich unlesbar gemacht werden - egal ob er auf einer Festplatte in meinem Unternehmen oder dem Data Warehouse eines Dienstleisters wie Microsoft oder AWS liegt.

Volle Kontrolle bis ins letzte Bit

Die gute Nachricht: Es gibt eine moderne Software-Architektur, die durch den Einsatz von Verschlüsselungstechnologien die Konformität mit der DSGVO bis ins letzte Datenarchiv garantiert: Die sogenannte Event-Bus-Architektur.

Auf dem Event-Bus werden alle Zustandsänderungen chronologisch vollständig als sogenannte "Events" gespeichert. Der Event-Bus wird als "Single Source of Truth" archiviert, weshalb alle anderen Systeme ihre Daten aus dem Event-Bus beziehen. Dabei ist es möglich, die Vorgänge, die einer Person direkt zugeordnet werden können, zu markieren und individuell zu verschlüsseln. Die vergebenen Schlüssel werden in einem "Tresor" gespeichert. Das bedeutet, dass alle personenbezogenen Vorgänge auf dem Event-Bus unlesbar gemacht werden können, indem der zugehörige individuelle Schlüssel aus dem Tresor gelöscht wird. So können persönliche Daten im Event-Bus und in Backups dauerhaft und DSGVO-konform unleserlich gemacht werden.

Wegen der DSGVO-Konformität und weiterer Vorteile setzt Christoph Brand, Lead Developer der XCNT GmbH bei der Entwicklung von DRIVR - einem IOT-Backend - auf die Event-Bus-Architektur.

Sie möchten mehr darüber erfahren?
Kontaktieren Sie Christoph unter dsgvo@drivr.cloud

DRIVR

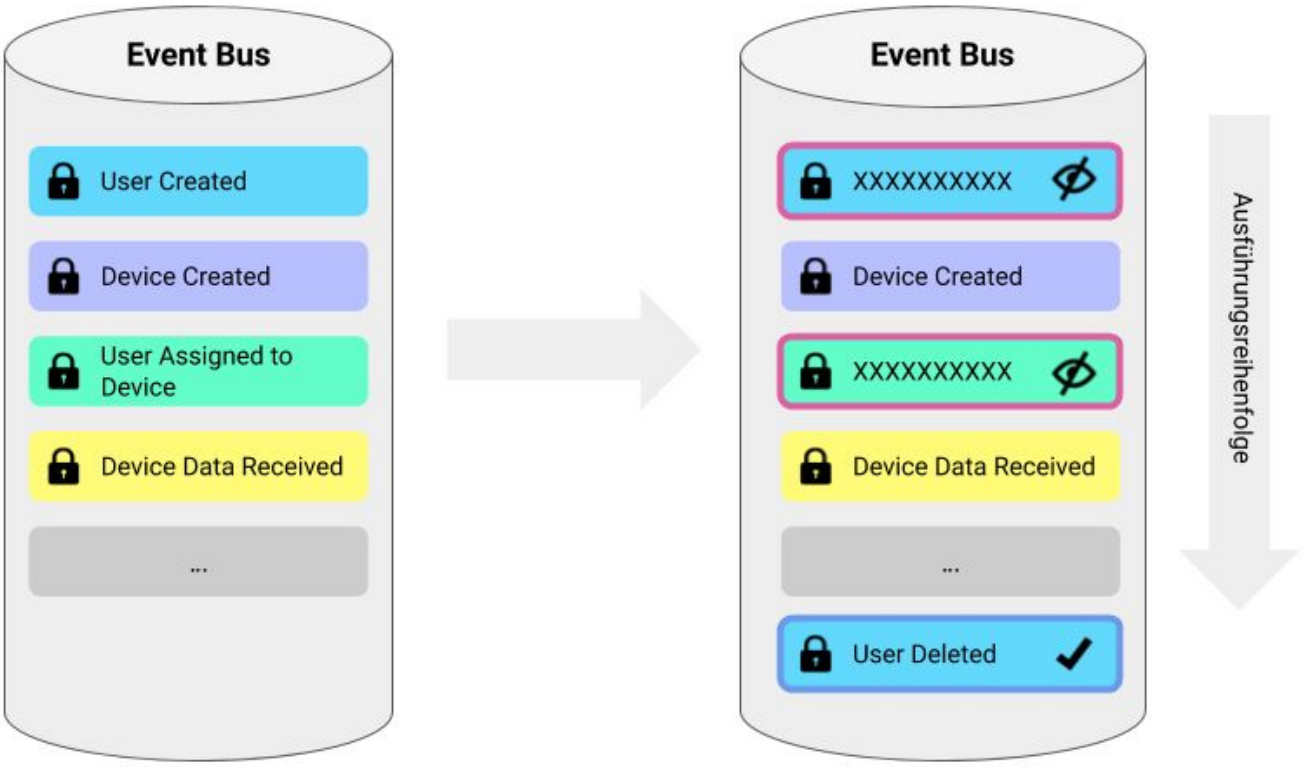

Abbildung: Funktionsprinzip der Löschung personenbezogener Daten in der Event-Bus-Architektur.

Links: Im Event-Bus werden verschiedene Events chronologisch gespeichert. Rechts: Wenn ein User gelöscht wird, werden die zugehörigen im Event-Bus gespeicherten personenbezogenen Daten unlesbar gemacht, indem der individuelle Schlüssel gelöscht wird. Da in der Event-Bus Architektur alle weiteren Services ihre Daten aus dem Event-Bus als "Single Source of Truth" beziehen, werden durch diesen Schritt die persönlichen Daten im gesamten System kontrolliert gelöscht.