Kitewerks

Der Schutz sensibler Daten im Kunden-Support

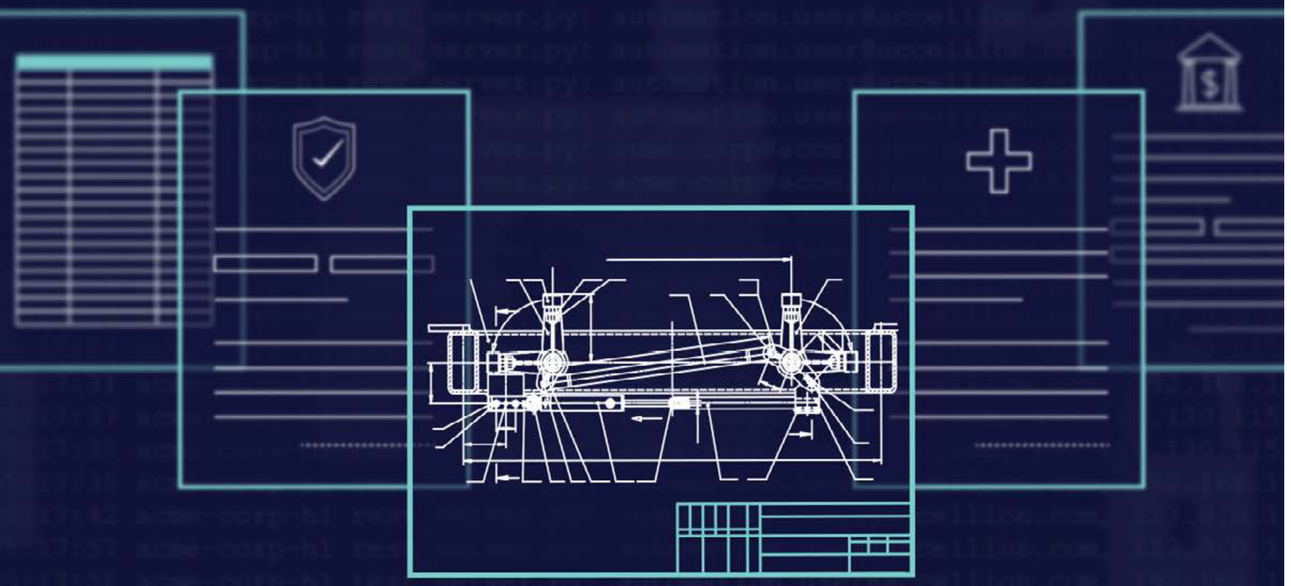
5 Best Practices für Compliance-relevante Daten in Prozessen der Kundenbetreuung

Einleitung

Mitarbeiter der Kundenbetreuung müssen schnell handeln, um das Kundenerlebnis zu verbessern und Abwanderung zu verhindern. Manchmal rotieren sie rund um die Uhr wie Feuerwehrleute, um einen komplexen Fall zu lösen, oder sie bearbeiten zahlreiche kleine Fälle an einem Tag. Führungskräfte dürfen allerdings nicht nachlässig werden, wenn es darum geht, ihr Unternehmen und ihre Kunden vor Compliance-Bußgeldern, Sicherheitsverletzungen und Reputationsverlusten zu schützen - selbst wenn sie ihren Kunden so schnell wie möglich helfen.

Da die Kunden Informationen weitergeben, die mit personenbezogenen Daten, geschützten Gesundheitsinformationen und privaten Finanzdaten gespickt sind, riskieren Sie Datenschutzverletzungen bei der Betreuung Ihrer Kunden. Weiß Ihr CISO, wie Ihre Servicemitarbeiter Kundendaten erhalten und speichern? Kennen und befolgen die Mitarbeiter Ihre Datenschutzrichtlinien - auch unter Druck? Können Sie dies einem Prüfer gegenüber beweisen?

Führende Unternehmen halten die Richtlinien ein und bieten gleichzeitig hervorragende Kunden- und Mitarbeitererlebnisse. Im Folgenden finden Sie fünf Best Practices für die Integration von Kundendaten in Ihre Governance-Richtlinien genau dort, wo Ihre Support-Mitarbeiter arbeiten: in ihren Vorgängen in Salesforce®.



01 Vermeiden Sie Compliance-Probleme

Behandeln Sie alle Kundendaten vertraulich

Jede Branche hat mit Kundendaten zu tun, die geschützte Gesundheitsinformationen, personenbezogene Daten, Finanzinformationen oder geistiges Eigentum enthalten, was die Einhaltung gesetzlicher Vorgaben wie GDPR/DSGVO, HIPAA und anderer Vorschriften erfordert. Wenn Kunden Ihren Mitarbeitern im Support eine Datei schicken, riskieren Sie jedes Mal einen Verstoß gegen den Datenschutz.

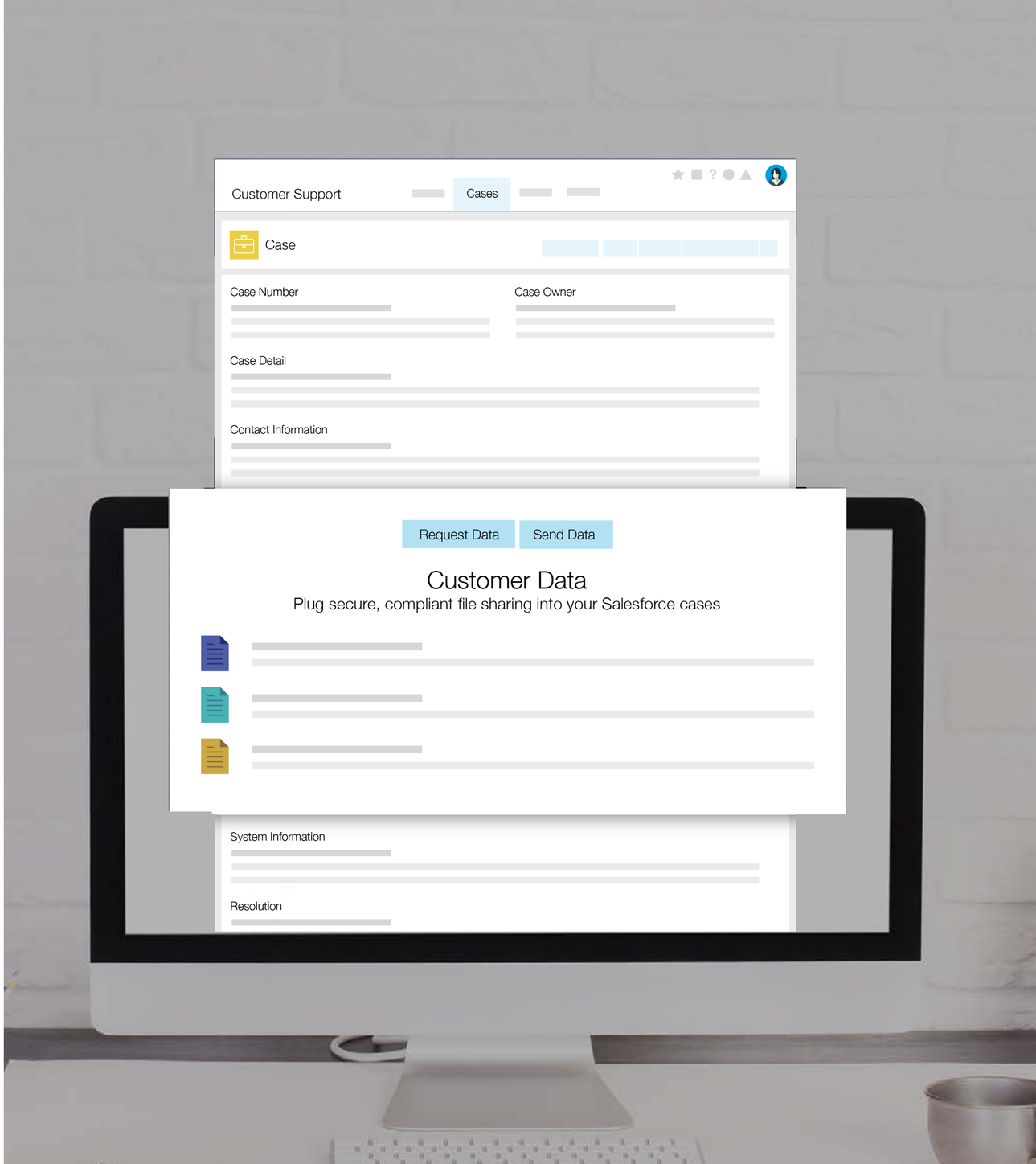
- Gesundheitswesen und Versicherung: Testergebnisse, Forderungen, Patientenakten
- Fertigung und Konstruktion: Computerunterstützte Entwürfe (CAD), Pläne, Budgets
- Finanzdienstleistungen: Steuerhistorien, Kontodaten, eidesstattliche Erklärungen zu Betrugsfällen, Inkassoschreiben
- Behörden: Steuerunterlagen, Beweismittel, Gewerbeanmeldungen, Daten von Gesundheitsdienstleistern
- Technologie: Protokolle, Screenshots, Pläne, Entwürfe

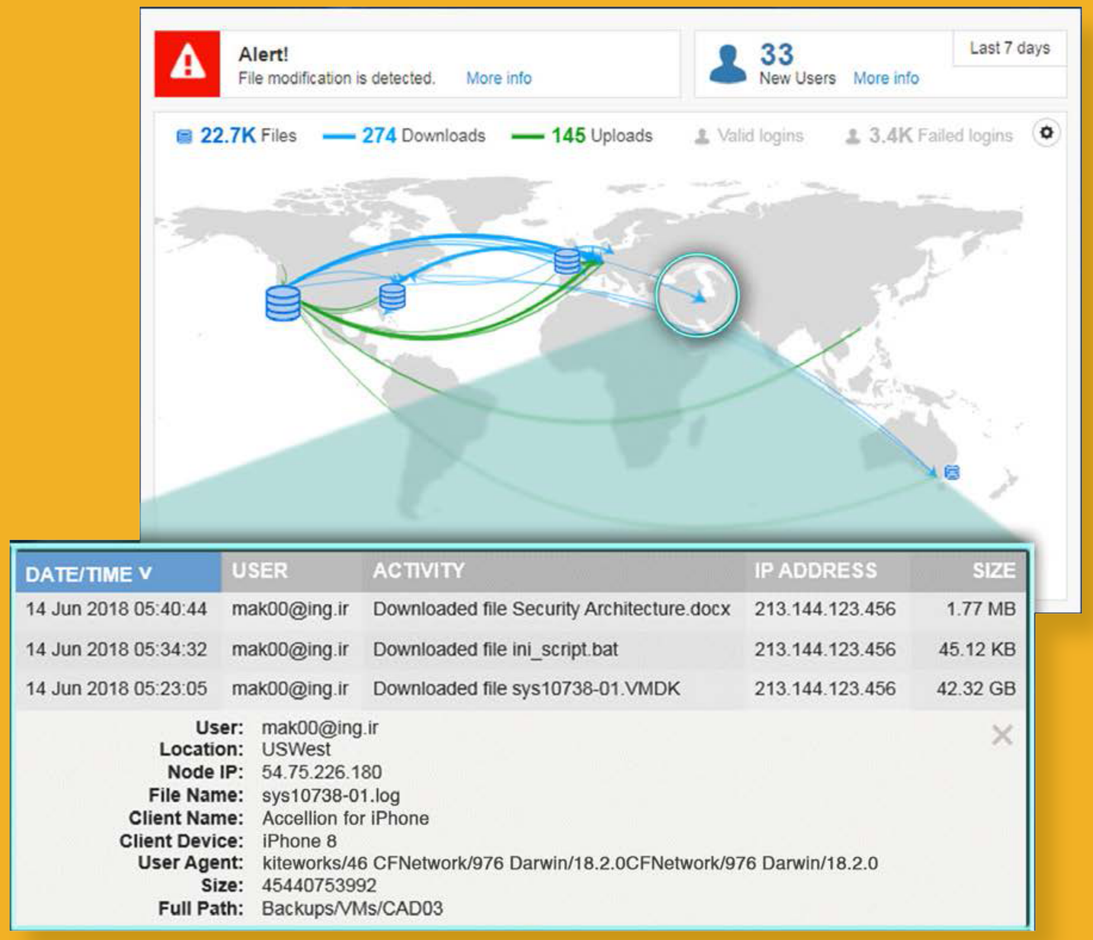
Ihre Support-Mitarbeiter müssen Kundendaten unter Einhaltung der Datenschutzgesetze bearbeiten, aber sie dürfen dabei nicht in ihrer Arbeit behindert werden. Setzen Sie ein Häkchen bei der Compliance, indem Sie die Durchsetzung der Richtlinien automatisieren und die Sicherheitsinfrastruktur Ihres Unternehmens nutzen, um Ihre Datenfreigabe-Software abzuschotten.

02 Sorgen Sie für einen 360-Grad-Blick

Verknüpfen Sie Kundendaten mit Vorgängen

Mitarbeiter können in ihrer Salesforce-Lösung auf eine zentrale Anzeige des jeweiligen Kunden zugreifen, die es ihnen ermöglicht, das Kundenerlebnis zu personalisieren. Wenn Sie jedoch ein konventionelles Portal oder eine Dateifreigabe in der Cloud bereitstellen, an die Kunden ihre Daten senden können, landen diese in einem isolierten Silo. Geben Sie Ihren Mitarbeitern stattdessen ein Plugin für Salesforce-Vorgänge an die Hand, mit dem sie Daten von ihren Kundenkontakten anfordern können. Lassen Sie das Plugin die Daten automatisch mit dem jeweiligen Vorgang verknüpfen und entsprechende Sicherheitsbefugnisse erteilen.





03 Verhindern Sie Datenschutzverletzungen

Transparenz für alle Support-Prozessdaten

Die Abwehr von Sicherheitsbedrohungen und Compliance-Risiken, die sich auf Ihre Support-Prozesse auswirken, ist eine anspruchsvolle Aufgabe. Sie müssen einen Überblick über jede Datei haben, die in Ihre Salesforce-Vorgänge eingeht oder diese verlässt. Gleichzeitig sollten Sie es Ihren Sicherheits-, Compliance- und Support-Teams einfach machen, Probleme innerhalb dieser Datenflut aufzuspüren.

Beginnen Sie mit der Implementierung eines Audit-Trails für alle Datenübertragungen zwischen Ihrem Kunden-Support und Ihren Kunden. Sobald Sie diese Metadaten haben, erstellen Sie übersichtliche und vollständige Echtzeit-Ansichten, die die wichtigsten Sicherheitsfragen zu Ihren Daten im Kunden-Support beantworten. Woher kommen sie? Wohin gehen sie? Wer sendet sie? Wer empfängt sie? Sind sie sensibel?

04 Vermeiden Sie Workarounds

Stellen Sie einfache Tools zur Verfügung, die die Benutzer verwenden möchten

Kundenbetreuer werden jedes Hindernis überwinden, wenn es gilt, ein Kundenproblem zu lösen. Sie können mit einem einfachen File-Sharing-Tool “heldenhaft” eine Blockade bei der Datenübertragung umgehen oder sogar unverschlüsselte E-Mails versenden. Allerdings bleiben Sie dann die Antwort schuldig, wenn die Prüfer fragen: Welche vertraulichen Kundendaten haben Sie? Sind sie verschlüsselt? Wer hat sie abgefangen?

Verhindern Sie Umgehungslösungen, indem Sie Ihren Mitarbeitern ermöglichen, Kundendaten zu senden und zu empfangen, ohne ihren Vorgang in Salesforce zu verlassen. Unterstützen Sie unbegrenzte Datenmengen und stellen Sie sicher, dass die Datenübertragung auch dann zuverlässig ist, wenn es die Netzwerke Ihrer Kunden nicht sind. Denken Sie daran, dass Ihre Kunden nicht geschult sind: Machen Sie Uploads und Downloads zum Kinderspiel.

CISOs geben strenge Richtlinien für die Datenspeicherung als Reaktion auf Datenschutz-bestimmungen und ständige Cyberangriffe vor, die Kundenbetreuer häufig dazu zwingen, Vorgangsdaten in Windows-Dateifreigaben oder SharePoint-Ordnern zu speichern.

05 Kosten senken und Compliance gewährleisten

Kontrollieren Sie, wo die Daten gespeichert werden

CISOs geben strenge Richtlinien für die Datenspeicherung als Reaktion auf Datenschutzbestimmungen und ständige Cyberangriffe vor, die Kundenbetreuer häufig dazu zwingen, Vorgangsdaten in Windows-Dateifreigaben oder SharePoint-Ordnern zu speichern. Das gibt Ihnen zwar die Kontrolle über die Kosten, aber es bedeutet auch zusätzliche Schritte für die Mitarbeiter, die das Kundenerlebnis beeinträchtigen und manuelle Compliance-Prozesse erfordern. Lassen Sie sie stattdessen die Daten direkt in ihren Salesforce-Vorgängen mit einem Plugin verwalten, das mit dem von Ihnen überwachten Datenspeicher lokal oder in einer privaten Cloud oder einer FedRAMP-autorisierten Umgebung verbunden ist. So haben Sie jederzeit die Kontrolle über die Kosten und die Einhaltung der gesetzlichen Vorgaben.

Kiteworks Private Content Network

- Sichere Speicherung
- Integrierter Audit-Trail
- CISO-Dashboard
- Compliance-Berichte
- Rollenbasierte Richtlinien

salesforce appexchange partner

Kiteworks

www.kiteworks.com

Juli 2022