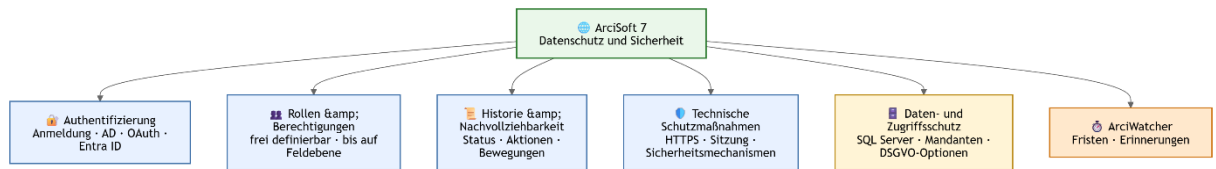


## ArciSoft 7

### Datenschutz und Sicherheit

#### 1. Überblick



ArciSoft 7 unterstützt Unternehmen bei der sicheren und nachvollziehbaren Verwaltung physischer Akten und Archivobjekte.

Die Anwendung ist so aufgebaut, dass Daten und Funktionen nur für berechtigte Benutzer zugänglich sind. Dazu nutzt ArciSoft 7 ein mehrstufiges Sicherheitsmodell aus Authentifizierung, Autorisierung, Berechtigungssteuerung, Protokollierung und technischen Schutzmaßnahmen. Ziel ist es, Aktenprozesse transparent, kontrollierbar und nachvollziehbar abzubilden.

#### 2. Zugriffsschutz und Anmeldung

Der Zugriff auf ArciSoft 7 erfolgt über definierte Anmeldeverfahren.

Je nach Projekt und Kundenumgebung können unterschiedliche Authentifizierungsverfahren eingesetzt werden, zum Beispiel:

- datenbankbasierte Anmeldung
- Windows- bzw. Active-Directory-Anmeldung
- OAuth 2.0
- Microsoft Entra ID

Nach erfolgreicher Anmeldung wird eine Benutzersitzung erstellt. Über diese Sitzung werden die zugehörigen Rollen, Berechtigungen und Systemzugriffe angewendet.

Bei Ablauf der Sitzung ist eine erneute Anmeldung erforderlich.

#### 3. Rollen und Berechtigungen

ArciSoft 7 arbeitet mit einem rollen- und berechtigungsbasierten Zugriffskonzept.

Rollen können kundenspezifisch angelegt, geändert und umbenannt werden. Dadurch lassen sich vorhandene Organisationsstrukturen und Zuständigkeiten individuell abbilden.

Über Berechtigungen wird gesteuert:

- welche Daten ein Benutzer sehen darf
- welche Akten bearbeitet werden dürfen
- welche Aktionen ausgeführt werden können
- welche Menüpunkte und Funktionen verfügbar sind
- welche Stammdaten angelegt, geändert oder gelöscht werden dürfen
- welche historischen Informationen eingesehen werden dürfen

Nicht erlaubte Funktionen werden in der Benutzeroberfläche ausgeblendet oder sind nicht auswählbar. Zusätzlich werden Berechtigungen serverseitig geprüft.

#### 4. Berechtigungen bis auf Feldebene

ArciSoft 7 unterstützt eine granulare Steuerung von Zugriffsrechten.

Je nach Konfiguration kann festgelegt werden, welche Informationen für bestimmte Benutzergruppen sichtbar, bearbeitbar oder verpflichtend sind. Dadurch können unterschiedliche Verantwortlichkeiten innerhalb einer Organisation sauber voneinander getrennt werden.

Beispielsweise können Benutzer nur bestimmte Akteninformationen sehen, während andere Felder nur für berechtigte Rollen sichtbar oder änderbar sind.

#### 5. Historie und Nachvollziehbarkeit

Wichtige Aktionen in ArciSoft 7 werden historisiert.

Dadurch können Bewegungen, Statusänderungen und relevante Bearbeitungsschritte nachvollzogen werden. Die Historie unterstützt Transparenz und Kontrolle im laufenden Archivprozess.

Nachvollziehbar sind insbesondere:

- Änderungen an Akteninformationen
- Statusänderungen
- Anforderungen und Ausleihen
- Rückgaben und Einlagerungen
- Weitergaben
- Aussonderungs- und Löschrprozesse
- relevante administrative Änderungen, sofern entsprechend protokolliert

Die Einsicht in historische Informationen ist ebenfalls berechtigungsgesteuert.

#### 6. Datenschutz und DSGVO-Unterstützung

ArciSoft 7 unterstützt die Einhaltung datenschutzrechtlicher Anforderungen durch klare Zugriffsregelungen, nachvollziehbare Prozesse und eine kontrollierte Berechtigungsvergabe.

Die Anwendung trägt dazu bei, personenbezogene oder sensible Informationen nur berechtigten Benutzern zugänglich zu machen.

Je nach Lizenz- und Projektumfang können zusätzliche Funktionen genutzt werden, zum Beispiel:

- mandantenfähige Datenhaltung
- DSGVO-Anonymisierung
- Audit-Funktionen
- rollenbasierte Zugriffsbeschränkungen
- Historisierung relevanter Aktionen

ArciSoft 7 ersetzt keine rechtliche Datenschutzprüfung, unterstützt jedoch die technische und organisatorische Umsetzung nachvollziehbarer Aktenprozesse.

## 7. Mandantenfähigkeit

ArciSoft 7 kann mandantenfähig betrieben werden, sofern das entsprechende Modul eingesetzt wird.

Die Mandantenfähigkeit ermöglicht eine logische Trennung von Datenbereichen. Dadurch können unterschiedliche Organisationseinheiten, Kundenbereiche oder getrennte Datenbestände innerhalb einer Installation abgebildet werden.

Der Zugriff auf mandantenbezogene Daten erfolgt abhängig von Benutzer, Rolle und Berechtigung.

## 8. Technische Schutzmaßnahmen

Für den sicheren Betrieb von ArciSoft 7 stehen verschiedene technische Schutzmaßnahmen zur Verfügung.

Dazu gehören insbesondere:

- verschlüsselte Kommunikation über HTTPS
- Einsatz eines gültigen TLS-/SSL-Zertifikats
- Sitzungsüberwachung
- automatische Abmeldung nach Sitzungsablauf
- Schutzmechanismen gegen typische Webangriffe
- Fehlerbehandlung ohne Anzeige sensibler Systeminformationen
- zentrale Bereitstellung der Anwendung über den Anwendungsserver
- Datenhaltung in einer Microsoft-SQL-Server-Datenbank

Der Betrieb über HTTPS wird empfohlen.

## 9. E-Mail-Benachrichtigungen und ArciWatcher

ArciSoft 7 kann E-Mail-Benachrichtigungen für definierte Prozesse versenden.

Dazu gehören beispielsweise Benachrichtigungen bei Anforderungen, Weitergaben, Rückgaben, Vorgängen oder Erinnerungen.

Das optionale Modul ArciWatcher überwacht definierte Fristen, beispielsweise überfällige Aktenrückgaben, und kann automatische Erinnerungen auslösen. Der Versand erfolgt über den angebundenen SMTP-Server.

## 10. Betrieb in der Kundeninfrastruktur

ArciSoft 7 wird typischerweise zentral in der IT-Umgebung des Kunden betrieben.

Dadurch verbleiben Anwendung, Datenbank und Betriebsverantwortung innerhalb der kundenseitig bereitgestellten Infrastruktur, sofern projektspezifisch nichts anderes vereinbart wurde.

Die konkrete Absicherung der Umgebung, z. B. Netzwerk, Server, Datenbank, Backup, Zertifikate und Benutzerverwaltung, erfolgt in Abstimmung mit der Kunden-IT.

## 11. Empfehlungen für einen sicheren Betrieb

Für einen sicheren und stabilen Betrieb werden folgende Maßnahmen empfohlen:

- regelmäßige Prüfung der Benutzer und Rollen
- Vergabe von Berechtigungen nach dem Prinzip der minimal erforderlichen Rechte
- Nutzung starker Passwörter oder zentraler Authentifizierung
- Betrieb über HTTPS
- regelmäßige Aktualisierung der Anwendung
- regelmäßige Sicherung der Datenbank
- Kontrolle von Protokollen und Fehlermeldungen
- Schulung der Anwender im Umgang mit Akten, Berechtigungen und sensiblen Daten
- regelmäßige Überprüfung der fachlichen Rollen- und Rechtevergabe

## 12. Kurzfazit

ArciSoft 7 verbindet strukturierte Aktenverwaltung mit einem flexiblen Sicherheits- und Berechtigungskonzept.

Durch definierbare Rollen, granulare Berechtigungen, Historisierung, optionale Mandantenfähigkeit, technische Schutzmaßnahmen und nachvollziehbare Prozesse unterstützt ArciSoft 7 einen kontrollierten und transparenten Betrieb in der Kundenumgebung.

