Archivierung und DSGVO

Informationsbroschüre zum datenschutzkonformen Einsatz von xSuite Archive

Stand November 2022

xSuite Archive

Die datenschutzrechtlichen Verpflichtungen und Sanktionen sind mit Inkrafttreten der DSGVO erheblich ausgeweitet worden. Wir haben uns daher intensiv mit den Anforderungen auseinandergesetzt, um einen datenschutzkonformen Umgang mit unserer Software zu ermöglichen. Mit diesem Dokument möchten wir unseren Interessenten, Kunden und Partnern einen Überblick darüber geben, wie sie unsere Softwarelösung xSuite Archive datenschutzkonform einsetzen können.

Zu diesem Zweck beschreiben wir anhand der gesetzlichen Anforderungen, welche Funktionen und Einstellungsmöglichkeiten Ihnen bei der Nutzung des Archivs zur Verfügung stehen. Bitte beachten Sie, dass die datenschutzkonforme Nutzung der Software in der alleinigen Verantwortung des Anwenders liegt. Dazu gehört insbesondere auch die individuelle Konfiguration der Software sowie deren Funktionen. Dabei gilt der Grundsatz, dass das Schutzbedürfnis für personenbezogene Daten umso höher ist, je sensibler die Daten sind.

Die nachfolgenden Erläuterungen dienen lediglich Informationszwecken. Wir leisten ausdrücklich keine Rechtsberatung und übernehmen folglich auch keinerlei Haftung für die nachfolgenden Inhalte.

Wir empfehlen Ihnen, sich in Zweifelsfällen durch einen auf Datenschutz spezialisierten Rechtsanwalt beraten zu lassen.

Welche Anforderungen stellt die DSGVO an eine Archivlösung?

Auskunftsrecht der betroffenen Person (Art. 15 DSGVO)
Als Verantwortlicher sind Sie verpflichtet auf Nachfrage offenzulegen, welche personenbezogenen Daten Sie über die betroffene Person zu welchem Zweck verarbeiten. Dazu müssen Sie in der Lage sein, personenbezogene Daten schnell, einfach und vollständig zu finden. Grundsätzlich lassen sich personenbezogene Daten auf mehreren Ebenen in xSuite Archive recherchieren wie z.B. Volltext-Suche (Google-ähnliche Suche nach Dokumenteninhalten), Indexfeld-Suche (Suche über vordefinierte Felder wie z.B. Bearbeiter) oder Metadaten-Suche (Suche nach Eigenschaften von Daten- und Dokumenten z.B. Ersteller eines Dokuments). Welche dieser Möglichkeiten verfügbar ist, hängt natürlich wiederum von Ihrer individuellen Konfiguration ab.

Recht auf Berichtigung (Art. 16 DSGVO)
Als Verantwortlicher sind Sie verpflichtet, ggf. fehlerhafte Daten zu einer Person zu korrigieren. Es muss also möglich sein, Daten nicht nur gezielt zu finden, sondern sie auch zu ändern. Entscheidend hierfür ist die Frage, ob die Daten in einem führenden System (z.B. ERP) verwaltet werden oder direkt in xSuite Archive oder ob es sich um eine Mischform handelt. Für die Daten, die aus dem ERP angezeigt werden, muss die Änderung im ERP erfolgen. Für Daten, die im Archiv gespeichert wurden, können die Änderungen direkt in der jeweiligen Maske erfolgen. Je nach Konfiguration wird eine neue Version angelegt, dabei bleiben die vorherigen Daten zum Zwecke der Nachvollziehbarkeit der Änderungen gespeichert. Ist dies nicht erwünscht, kann dies in der Konfiguration angepasst werden.

Recht auf Löschung („Recht auf Vergessenwerden" Art. 17 DSGVO)
Als Verantwortlicher sind Sie verpflichtet personenbezogene Daten zu löschen, sobald der Verwendungszweck entfällt. Weiterhin sind Sie u.U. verpflichtet, der Aufforderung eines Betroffenen nachzukommen, über ihn gespeicherte personenbezogene Daten zu löschen. Nach der entsprechenden Suche kann ein Benutzer bei Vorliegen der erforderlichen Berechtigung die ausgewählten Datensätze in einem Vorgang löschen. Dabei empfiehlt es sich, selektiv vorzugehen und Einzelprüfungen vorzunehmen, da u.U. einzelne Dokumente aufgrund von andauernden Aufbewahrungspflichten noch nicht gelöscht werden dürfen. Hier ist zu prüfen, welche Daten und Dokumente archiviert werden.

Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
Gemäß der DSGVO muss es möglich sein, dass Datensätze in maschinenlesbarem Format von einem System auf ein anderes System übertragen werden können. Das xSuite Archive stellt eine Funktion bereit, um alle oder ausgewählte Datensätze und Dokumente zu exportieren, z.B. um sie einem Anwendenden offline bereitzustellen. Die Belege werden im gespeicherten Format exportiert, die Indexdaten als JSON. Darüber hinaus hat der Anwender die Möglichkeit, die Software so zu konfigurieren, dass ein Online-Zugriff auf alle oder bestimmte Inhalte möglich ist.

xSuite Archive als Teil einer Gesamtlösung
Unabhängig von den Funktionen die xSuite Archive im Standard bereitstellt, sollte das Archiv immer im Gesamtkontext betrachtet werden. Zu beachten ist beispielsweise, dass eine Löschung von Daten im Archiv nicht genügt, sofern das verbundene ERP System führend ist. In diesem Fall müssen die Daten dort geändert oder gelöscht werden.

Privacy by Design – Datenschutzrelevante Features und Optionen

Folgende Funktionalitäten und Optionen bietet Ihnen xSuite Archive, um datenschutzrechtliche Compliance zu ermöglichen bzw. erleichtern:

Benutzer, Authentifizierung und Passwörter
- xSuite Archive hat eine Berechtigungs- aber keine eigene Benutzerverwaltung. Die Benutzerverwaltung und -authentifizierung erfolgt gegen einen Dienst des xSuite Core. Das heißt weder Benutzerdaten oder -passwörter noch andere Identifikationsmerkmale der Nutzer werden in xSuite Archive gespeichert.
- xSuite Core, über das die Benutzerauthentifizierung erfolgt, setzt immer auf ein anderes System, z.B. Active Directory, auf. Dadurch werden die entsprechenden Authentifizierungsmechanismen und -einstellungen dieses Systems übernommen. So können Sie z. B. Passwortrichtlinien gemäß den Datenschutzrichtlinien Ihres Unternehmens umsetzen.
- Der Zugriff des Clients auf das System erfolgt ausschließlich über REST-Services. Diese werden in den Microsoft IIS gehostet, dort kann die Authentifizierung eingestellt werden.
- xSuite Archive wird mit einem Standard-Passwort der User-Role ausgeliefert, diese kann (und sollte) geändert werden.

Verschlüsselung
- Als Verschlüsselungsstandard wird AES-256 verwendet.
- Der Web-Zugriff des Clients auf das System erfolgt ausschließlich über REST-Services. Diese werden in den Microsoft IIS gehostet, dort kann eine Verschlüsselung (HTTPS) eingestellt werden.
- Die Kommunikation kann mit einem SSL-Zertifikat End2End verschlüsselt werden.
- Dem Archiv kann die Eigenschaft „Stream type = Crypted" hinzugefügt werden. Dadurch werden alle neu abgelegten Dokumente automatisch verschlüsselt.
- Nur die Kennwörter von Backend Usern (d.h. von Diensten, nicht von menschlichen Benutzern) werden im xSuite Archive gespeichert. Es gibt ein Tool, das zur Verschlüsselung der Kennwörter und Credentials dieser Backend User genutzt werden kann. Die Einstellung „salted" stellt dabei außerdem sicher, dass der Hash nicht nachvollzogen werden kann.

Caching
- Das Zwischenspeichern von Dokumenten kann deaktiviert werden.
- Passwörter werden nicht zwischengespeichert.

Mandantenfähigkeit
- Die Lösung ist mandantenfähig, um sicherzustellen, dass ein User nur auf die Daten seiner eigenen Unternehmenseinheit zugreifen kann.

Individuelle Rechtevergabe
- xSuite Archive verfügt über ein rollenbasiertes Berechtigungskonzept. Rechte (z.B. „Lesen“, „Schreiben“ oder „Administrieren“) können Rollen (z.B. „Mitarbeiter“ oder „Freelancer“) zugeordnet werden, ein Benutzer kann mehrere Rollen haben. Sollten sich die Rollen widersprechen, wiegt das Verbot höher als die Berechtigung.
- Die Rechtevergabe ist möglichst restriktiv aufgesetzt und erfolgt ähnlich wie bei Linux-Systemen: Es wird nicht definiert, was eine Rolle nicht darf, sondern was erlaubt ist. D. h. wenn nichts definiert ist, hat die Rolle auch keinerlei Berechtigungen.
- Es lässt sich einstellen, dass auch der Administrator nicht auf alle Dokumente zugreifen kann, dies empfiehlt sich z.B. für besonders sensible personenbezogene Daten wie Personalakten.

Logging
- xSuite Archive bietet verschiedene Loglevel für Änderungen an Dokumenten sowie Fehlermeldungen des Systems an. Das oberflächlichste Level ist ein Audit-Trail-Mitschnitt, das detaillierteste Level ist Trace, in diesem werden auch kleinste Informationen mitgeschnitten. Das Logging lässt sich nicht komplett deaktivieren, das heißt es können keine unbemerkten Änderungen an Dokumenten vorgenommen werden.
- Um Änderungen bei Dokumenten nachvollziehen zu können, gibt es eine automatische Versionierung bzw. Versionshistorie. Auf Basis von Indexfeldern wird kenntlich gemacht, wer welche Änderungen an einem Dokument vorgenommen hat.
- Es werden auch Änderungen an Feldinhalten protokolliert.
- Auch wenn ein Dokument durch einen Administrator gelöscht wird, wird dies protokolliert: Es wird festgehalten, dass es ein Dokument gab, wann und von wem es erstellt und gelöscht wurde. Inhalte des Dokuments (nur dort sollten überhaupt personenbezogene Daten enthalten sein) sind aber nicht Teil des Protokolls.
- Die Anmeldungen von Nutzern sowie Backend Usern werden protokolliert, auch wenn keinerlei Änderungen vorgenommen werden.

Hash
- Dokumente werden bei der Ablage im xSuite Archive mit einem Header mit Hash versehen, dadurch sind Dokumente im Filesystem vor Veränderungen geschützt. Die Files sind wiederum in Dokumentboxen abgelegt, die auch einen gehashten Header haben, sodass durch das doppelte Hashing eine Manipulation noch weiter erschwert wird.
- Es ist möglich, dass bei jeder Anzeige eines Dokuments im Client der Hash geprüft wird. Somit kann im Sinne der Datenintegrität jederzeit überprüft werden, ob ein Dokument geändert wurde.

Zeitstempel und Versionsnummer
- Das System stellt sicher, dass nicht 2 Prozesse oder User gleichzeitig ein Dokument verändern können. Nur der Prozess oder User, der zuerst auf das Dokument zugreift, kann Änderungen speichern. Dies unterstützt die Datenintegrität.

Legal Hold
- Es kann eine Veränderungssperre für alle Nutzer („Legal Hold“) gesetzt werden, wodurch Dokumente weder geändert noch gelöscht werden können.

Replikation
- Es können Replikations-Aufträge angelegt werden. Dadurch werden Replikate nach Wahl als Local oder Remote Copy erstellt. Die Replikate erhalten ein Change-Token um sicherzustellen, dass Replikat und Original identisch sind. Es ist möglich, mit der Option „Check Replication“ eine automatische Prüfung der Replikate zu aktivieren, um Datenintegrität zu gewährleisten.

Datensicherung
- xSuite Archive bietet eine Export-Schnittstelle zur Datensicherung. Best Practices für die Datensicherung sind im Administrator-Handbuch genauer erläutert.

Retention/automatische Löschung
- Dokumente können mit einem Verfallsdatum versehen werden. Ist das Verfallsdatum eines Dokuments erreicht, wird durch die Retention-Funktion dieses Dokument automatisch gelöscht. Diese Funktion unterstützt das Datenschutz-Erfordernis nach Speicherbegrenzung / Datenminimierung.
- Die Retention kann für einzelne Unterarchive unterschiedlich eingestellt werden. D.h. Sie können auch ein spezielles Archiv anlegen für Dokumente, die besonderes lange aufbewahrt werden müssen. Wenn Sie Ihre Dokumente nach Aufbewahrungsfristen klassifizieren und in unterschiedliche Unterarchive einordnen, können Sie mit Hilfe der Retention erreichen, dass Sie Dokumente nur so lange aufbewahren, wie notwendig.

Indexierung und Suche

- Um das Recht auf Vergessenwerden umsetzen zu können, müssen Sie Dokumente, die personenbezogene Daten enthalten, auch wiederfinden können. Um dies zu ermöglichen bietet das xSuite Archive umfangreiche Indexierungs- und Suchfunktionen.
- Indexierung: Damit Dokumente im Archiv auch wiedergefunden werden können, müssen sie indexiert werden.
- Such-Optionen: Um Ihnen zu ermöglichen, dass alle personenbezogenen Daten im Archiv auch wiederfinden, bietet unsere Lösung vielfältige Suchoptionen: Volltextsuche (Google-ähnliche Suche nach Dokumenteninhalten), Indexdaten-Suche (Suche über vordefinierte Felder wie z.B. Bearbeiter), Metadaten-Suche (Suche nach Eigenschaften von Daten- und Dokumenten z.B. Ersteller eines Dokuments), Google-like, schemafreie Suche, Autovervollständigung, Relations, Kategorie-Suche und One-Click-Filter.

Referenzlisten

- Neben den Suchfunktionen für die Benutzer hat der Administrator die Möglichkeit, Referenzlisten zu erstellen. Diese Referenzlisten können genutzt werden, um alle Daten zu einem bestimmten Suchwort zu ändern oder zu löschen. Diese Funktion erleichtert Ihnen, Ihrer Pflicht zur Auskunft bzw. Ihrer Pflicht zur Berichtigung falscher Informationen bzw. Ihrer Pflicht zur Löschung von Daten nachzukommen.

Auftragsverarbeitung und technisch-organisatorische Maßnahmen

Im Rahmen der Projekttätigkeit sowie der Pflege der Software kann nicht ausgeschlossen werden, dass unsere Mitarbeiter*innen mit personenbezogenen Daten in Berührung kommen. Aus diesem Grund halten wir eine vollständig vorausgefüllte Vereinbarung zur Auftragsverarbeitung für Sie bereit.

Darüber hinaus stellen wir Ihnen unsere technisch-organisatorischen Maßnahmen in einem separaten Dokument zur Verfügung.