WHITEPAPER

RECHTLICHE ANFORDERUNGEN AN DIE DATENARCHIVIERUNG IN DEUTSCHLAND

Um die wachsenden Datenmengen rechtskonform zu archivieren, sind zahlreiche Compliance Vorgaben zu beachten. In diesem Whitepaper erhalten Sie einen Überblick über die wesentlichen Aspekte des deutschen Rechts im Hinblick auf die gesetzeskonforme Archivierung von Unternehmensdaten.

INHALTSVERZEICHNIS

WHITEPAPER

RECHTLICHE ANFORDERUNGEN AN DIE DATENARCHIVIERUNG IN DEUTSCHLAND

1. EINLEITUNG

Die zunehmende Digitalisierung von Unternehmensdaten stellt neue Anforderungen an den Umgang und die Archivierung von Geschäftsinformationen. Um die wachsenden Datenmengen rechtskonform zu archivieren, sind neben internen Compliance Vorgaben zahlreiche gesetzliche Vorschriften zu beachten. Werden diese nicht eingehalten, drohen den Unternehmen empfindliche Strafen oder sogar langfristige Image-Schäden. Zeitgleich entwickeln sich die IT Landschaften und Speichertechnologien kontinuierlich weiter, was die Planungs- und Zukunftssicherheit von Datenmanagement Lösungen erschwert.

Die deutschen Gesetze hinsichtlich des Datenschutzes und der Informationssicherheit sollen einen verlässlichen Schutz der Integrität, Vertraulichkeit und Verfügbarkeit von Unternehmensdaten schaffen. Das vorliegende Whitepaper dient dazu, Ihnen als Orientierungshilfe einen Überblick über die wesentlichen Aspekte des deutschen Rechts im Hinblick auf die gesetzeskonforme Archivierung von Unternehmensdaten zu geben. Im Folgenden werden:

1. die EU-DSGVO (Datenschutz-Grundverordnung)
2. die GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff)
3. das IT-Sicherheitsgesetz
4. und der Schutz von Geschäftsgeheimnissen

sowie deren Anforderungen an die Langzeitarchivierung und das Management von Unternehmensdaten behandelt.

Das Dokument ist rein informativer Natur, hat keinen Anspruch auf Vollständigkeit und bezweckt keine Rechtsberatung. Die Übersicht der rechtlichen Rahmenbedingungen wurde durch Werner Bachmann, Rechtsanwalt mit den Schwerpunkten IT Compliance und Datenschutz bei Friedrich Graf von Westphalen & Partner mbB, ausgearbeitet.

2. DIE EU-DATENSCHUTZGRUNDVERORDNUNG (EU-DSGVO)

Die Regelungen der EU-DSGVO dienen dazu, eine weitreichende Vereinheitlichung des europäischen Datenschutzes zu schaffen und einen umfassenden Schutz personenbezogener Daten zu gewährleisten. Die neuen Anforderungen gelten seit dem 25. Mai 2018 und betreffen alle Unternehmen mit Sitz in der EU und Unternehmen, die personenbezogene Daten über Menschen, die in der EU leben, erheben, verarbeiten und nutzen.

Die DSGVO hat großen Einfluss auf die Archivierung und das Management von Daten, da sich ein wesentlicher Bestandteil der Regelungen auf den transparenten Umgang mit personenbezogenen Daten im Hinblick auf deren Erhebung, Speicherung, Verarbeitung, den Schutz, und die Löschung bezieht. In diesem Zusammenhang müssen vielerlei Anforderungen z. B. an die Integrität, Vertraulichkeit und die Verschlüsselung von Daten eingehalten werden und nachweisbar sein. Diese Nachweispflicht gilt für den Auftraggeber wie für den Auftragsverarbeiter.

Die Regelungen sind für viele Unternehmen mit hohen Risiken und ungewissen Kosten verbunden. Bis zu 4% des globalen Jahresumsatzes oder 20 Millionen Euro betragen die Strafzahlungen im Fall einer schwerwiegenden Verletzung der DSGVO. Dass diese Strafen nicht nur zur Abschreckung dienen, sondern in der Realität angewendet werden, haben bereits mehrere große Fälle seit der Einführung eindrucksvoll bewiesen. Zudem sind Datenschutzverstöße oft mit einem Image-Risiko für die Unternehmen verbunden.

AUSWIRKUNGEN DER DSGVO AUF DIE DATENSPEICHERUNG UND -ARCHIVIERUNG

Eine datenschutzorientierte Archivierung bildet eine wesentliche Grundlage für die Einhaltung der DSGVO. Viele der Anforderungen lassen sich mit einer zentralen Datenmanagement- und Speicherlösung (inkl. Retention Management) einfacher umsetzen.

Für Unternehmen ist es elementar, dass sie im Detail wissen, wie ihre Tools und Lösungen die Anforderungen der DSGVO erfüllen. Daher werden im Folgenden die wichtigsten Regelungen und die damit verbundenen Anforderungen an eine Archivierungslösung ausgeführt.

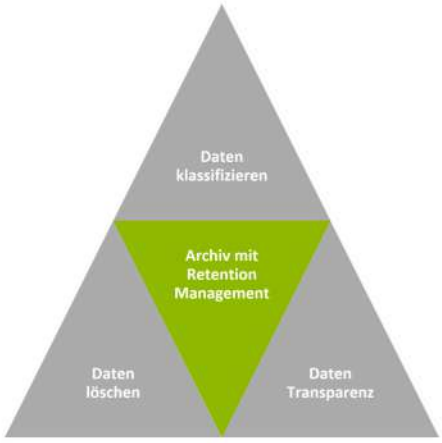
DATENMINIMIERUNG

Laut Art. 5 (1c) der DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Eine Archivierungslösung muss demnach so gestaltet sein, dass keine unnötigen Duplikate erstellt werden. Nutz- und Metadaten müssen getrennt verarbeitet werden. In der Lösung dürfen personenbezogene Daten zudem nicht in den Metadaten gespeichert oder mit ihnen kombiniert werden.

SPEICHERBEGRENZUNG UND AUFBEWAHRUNGSFRISTEN

Die DSGVO fordert nach Art 5 (1e), dass personenbezogene Daten nicht länger als erforderlich aufbewahrt und z. B. nur für ausschließlich im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke länger gespeichert werden dürfen.



Dies bedeutet, dass eine Archivierungslösung in der Lage sein muss, konkrete Aufbewahrungsfristen für die Daten festzulegen. Daten müssen zum einen fristgerecht gelöscht werden können. Zum anderen müssen auch sehr langer Aufbewahrungsfristen ermöglicht werden. Hierbei stellen Zeitstempel, Sperrkonzepte und eine WORM (Write-Once-Read-Many) Funktionalität die korrekte Speicherung von Daten im Rahmen der gesetzlichen Aufbewahrungspflichten sicher.

INTEGRITÄT UND VERTRAULICHKEIT

Gemäß Art. 5 (1f) der DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Hierzu gehört auch der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Verlust, Zerstörung oder Schädigung.

Eine Archivierungslösung muss demnach eine Zugriffskontrolle aufweisen, um unautorisierten Datenzugriff zu verhindern. Die Datenintegrität kann sichergestellt werden, indem alle Informationen (Nutzdaten, Metadaten, Hash-Werte) in sicheren Archivcontainern gespeichert werden. Diese Archivcontainer können zusätzlich verschlüsselt werden (z. B. mit AES-256 Verschlüsselung). Die Archivlösung sollte zudem korrupte oder ungültige Daten automatisch erkennen und mit validen Daten ersetzen (Self-Healing). Mithilfe einer Mandantenfähigkeit kann zudem eine sichere Trennung von Archivdaten in unterschiedlichen Repositories mit unterschiedlichen Zugriffsrechten stattfinden.

AUSKUNFTSRECHT DER BETROFFENEN PERSON

Laut Art. 15 der DSGVO hat eine betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Wenn dies der Fall ist, so hat die Person ein Recht auf Auskunft über diese personenbezogenen Daten.

Archivierungslösungen müssen in der Lage sein, alle archivierten (personenbezogenen) Daten schnell und umfassend zu finden und abzurufen. Eine zentrale Speicherplattform erleichtert hierbei die Datensuche. Die Datensuche kann zusätzlich vereinfacht werden, wenn eine Integration in E-Discovery und Suchtools gegeben ist.

RECHT AUF LÖSCHUNG (VERGESSENWERDEN)

Die DSGVO schreibt in Art. 17 vor, dass die betroffene Person das Recht auf Löschung der gespeicherten personenbezogenen Daten hat, sofern einer der in Art. 17 definierten Gründe zutrifft. Dies gilt nicht, soweit die Verarbeitung dieser Daten erforderlich ist (z. B. zur Erfüllung einer rechtlichen Verpflichtung).

Archivierungssysteme müssen einerseits in der Lage sein, archivierte Daten aus Datenschutzgründen vor Ablauf der Aufbewahrungsfrist gemäß einem speziellen und klar definierten Prozesse zu löschen (Special Delete). Zum anderen müssen Aufbewahrungsfristen verlängert werden können, sofern dies nötig und rechtskonform ist (Legal Hold).

VERANTWORTUNG DES FÜR DIE VERARBEITUNG VERANTWORTLICHEN

Gemäß Art. 24 der DSGVO muss sichergestellt werden können, dass die Verarbeitung und Speicherung von Daten gemäß den Vorgaben der DSGVO erfolgt. Hierfür muss ein Nachweis erbracht werden können.

Eine Archivierungslösung muss eine kontinuierliche Überwachung der umgesetzten technischen Maßnahmen ermöglichen. Demnach müssen beim Archivieren und Lesen alle Zugriffe und durchgeführten Aktionen wie z. B. Löschversuche und Änderungen in einer Dokumentation datenschutzkonform protokolliert, revisionssicher archiviert und vor Veränderungen geschützt werden (z. B. mithilfe von Audit-Trails). Auch eine Prüfung und Zertifizierung der Archivlösung durch eine unabhängige Instanz ist ein sinnvoller Schritt.

DATENSCHUTZ DURCH TECHNIKGESTALTUNG UND DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

Art. 25 der DSGVO fordert, dass Datenschutzgrundsätze sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung wirksam umgesetzt werden.

Eine Archivierungslösung muss Datenschutzgrundsätze demnach wirksam umsetzen und datenschutzfreundliche Voreinstellungen aufweisen. Dabei müssen die Voreinstellungen der Lösung für die Daten im Hinblick auf die Menge der Datenerhebung, den Umfang ihrer Verarbeitung, die Speicherfrist und die Zugänglichkeit datenschutzfreundlich ausgelegt sein. Bei der Auswahl der Lösung sollte darauf geachtet werden, dass die Lösung durch eine unabhängige Stelle (z. B. die KPMG) auf die Einhaltung der Anforderungen der DSGVO geprüft und zertifiziert wurde.

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Gemäß Art. 30 der DSGVO muss ein Verzeichnis aller Verarbeitungen wie z. B. eine allgemeine Beschreibung der technischen Maßnahmen für die Sicherheit der Verarbeitung und Speicherung geführt werden.

Archivierungslösungen müssen in der Lage sein, ein solches Verzeichnis automatisch zu erstellen. Eine Audit-Trail Historie, in der alle Events (Erstellung, Lesezugriff, etc.) auf die archivierten Daten revisionssicher dokumentiert werden, hilft bei der Erfüllung dieser Anforderung. Bei der Wahl der Archivlösung sollte berücksichtigt werden, dass zudem alle Änderungen an der Konfiguration zur späteren Nachvollziehbarkeit in einem Changelog protokolliert werden.

SICHERHEIT DER VERARBEITUNG

Nach Art. 32 der DSGVO muss im Hinblick auf Verarbeitungssicherheit ein dem Risiko angemessenes Schutzniveau gewährleistet werden. Die Archivierungslösung sollte Daten sicher verschlüsseln (z. B. mittels AES-256 Verschlüsselung) und eine dauerhafte Integrität und Verfügbarkeit der Verarbeitungssysteme gewährleisten. Verfügt das Archiv über eine Funktion, die Archivdaten repliziert, Fehler identifiziert und korrupte Objekte automatisch repariert, können logische oder technische Fehler aus dem System-A das replizierte System-B nicht beeinflussen. Die Systeme müssen zudem in der Lage sein, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall schnell wiederherzustellen.

3. DIE GRUNDSÄTZE ORDNUNGSMÄSSIGER BUCHFÜHRUNG UND DOKUMENTATION (GOBD)

Die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) umfasst Regelungen, die beim Einsatz einer Software-gestützten Buchführung eingehalten werden müssen. Die GoBD trat am 1. Januar 2015 in Kraft und löste die bis dahin geltenden

- GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen)
- und GoBS (Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme)

ab. Die Anforderungen der GoBD sind für jedes buchführungs- und aufzeichnungspflichtige Unternehmen in Deutschland bindend.

Das Ziel der Verordnung ist es, angesichts der steigenden Anzahl und Verschiedenartigkeit der eingesetzten Systeme einheitliche Regelungen und Rechtsklarheit für Unternehmen zu schaffen. Zudem soll durch die Führung und Aufbewahrung von steuerlich relevanten Geschäftsdaten ein schneller Ablauf der Betriebsprüfung durch das Finanzamt sichergestellt werden.

Wesentliche Bestandteile der Verordnung sind die Erfassung, Bearbeitung und Archivierung von Belegen und steuerlich relevanten Unterlagen. Gemäß der GoBD müssen alle Geschäftsvorfälle über den gesamten Aufbewahrungszeitraum

- nachvollziehbar,
- vollständig,
- richtig,
- zeitgerecht,
- geordnet
- und unveränderbar

aufbewahrt und wiedergegeben werden können. Darüber hinaus ist eine Verfahrensdokumentation zu führen.

Eine Nicht-GoBD-konforme Speicherung von Daten kann enorme Konsequenzen für Unternehmen nach sich ziehen. Wird bei einer Betriebsprüfung festgestellt, dass die Anforderungen der GoBD nicht eingehalten werden, kann dies beispielsweise die Verwerfung der gesamten Buchführung oder hohe Steuernachzahlungen zur Folge haben.

AUSWIRKUNGEN DER GOBD AUF DIE DATENSPEICHERUNG UND -ARCHIVIERUNG

Welche Dokumente und Unterlagen sind gemäß der GoBD revisionssicher aufzubewahren?

Die GoBD schreibt die rechtskonforme Aufbewahrung sowohl eingehender als auch ausgehender Dokumente und Unterlagen vor. Unter anderem müssen folgenden Dokumente aufbewahrt werden:

- Belege
- E-Mails
- Geschäftsbriefe
- Bücher und Aufzeichnungen
- Eingangs- und Ausgangsrechnungen

Die entsprechenden Aufbewahrungsfristen der Dokumente und Unterlagen werden in der Abgabenverordnung (AO) definiert. Demnach gilt beispielsweise eine Aufbewahrungsfrist von 10 Jahren für Buchungsbelege, Rechnungen, Bankunterlagen und Lageberichte. Eine Aufbewahrungsfrist von 6 Jahren gilt z. B. für Geschäftsbriefe.

Die Grundsätze der GoBD müssen während der gesamten Aufbewahrungsdauer der Dokumente und Unterlagen eingehalten werden. Eine Archivierungslösung muss daher die Definition von Aufbewahrungsfristen ermöglichen. Hierbei kann eine WORM-basierte Aufbewahrungsfrist jedem Datensatz ein Ablaufdatum zuordnen. Zudem muss die Archivierungslösung ermöglichen, dass Daten fristgerecht gelöscht und zudem sehr lange Aufbewahrungsfristen gesetzt werden können.

WELCHE AUSWIRKUNGEN HABEN DIE REGELUNGEN DER GOBD AUF DIE DATENARCHIVIERUNG?

Belege und steuerpflichtige Unterlagen können mithilfe einer geeigneten Archivierungslösung revisionssicher archiviert werden und den Unternehmen somit die Verantwortung für eine GoBD-konforme Datenhandhabung abnehmen. Im Folgenden werden daher die wichtigsten Grundsätze der GoBD und ihre Auswirkungen auf ein GoBD-konforme Datenarchivierung geschildert.

NACHVOLLZIEHBARKEIT UND NACHPRÜFBARKEIT

Laut Art. 3.1 der GoBD müssen Buchungen oder sonstige erforderlichen Aufzeichnungen durch Belege nachvollziehbar sein und lückenlos protokolliert werden. Bei einer Betriebsprüfung ist ein Zugriff auf diese Belege innerhalb eines angemessenen Zeitraums zu ermöglichen. Dabei muss der Prüfer die Geschäftsvorfälle für die gesamte Aufbewahrungsdauer lückenlos nachvollziehen können.

Eine Archivierungslösung muss so beschaffen sein, dass sie die Integrität der Belege und steuerlich

relevanten Unterlagen sichert. Eine Audit-Trail-Historie und ein Changelog sorgen dafür, dass Zugriffe und etwaige Änderungen an den Datensätzen über die gesamte Aufbewahrungsdauer protokolliert werden und sich nachverfolgen lassen. Verfügt die Archivierungslösung über Suchtools oder eine Integration in E-Discovery, können archivierte Belege und Unterlagen schnell gefunden werden.

VOLLSTÄNDIGKEIT

Laut Art. 3.2.1 der GoBD müssen alle Belege vollständig und lückenlos aufbewahrt werden. In diesem Zusammenhang sind Aufbewahrungsfristen von 6 bzw. 10 Jahren einzuhalten (AO). Die Dokumente dürfen nicht gelöscht werden, bevor die entsprechenden Aufbewahrungsfristen abgelaufen sind. Bei einer Betriebsprüfung müssen diese Daten wiedergegeben werden können.

Mithilfe einer Archivierungslösung müssen Datensätze mit einem Zeitstempel versehen und die WORM-basierte Aufbewahrungsdauern sowie Sperrkonzepte definiert werden können. Dabei muss während der gesamten Aufbewahrungsdauer Schutz vor Datenverlust, -beschädigung oder -zerstörung geboten sein.

RICHTIGKEIT

Archivierte Belege müssen die Geschäftsvorfälle laut Art 3.2.2 der GoBD wahrheitsgetreu darstellen. Demgemäß müssen die Belege über den gesamten Aufbewahrungszeitraum in unveränderter Form aufbewahrt werden.

Eine Archivierungslösung muss die archivierten Daten gemäß dem tatsächlichen Zustand archivieren und während der gesamten Aufbewahrungsdauer vor unbefugten Manipulationen, Änderungen und Löschungen schützen. Alle Zugriffe auf das Datenarchiv sind dabei lückenlos zu protokollieren – z. B. in einer Audit-Trail Historie und Changelog. Um die Datenintegrität sicherzustellen, sollten Systeme korrupte oder ungültige Daten erkennen und optimalerweise automatisch reparieren bzw. wiederherstellen können.

ZEITGERECHTE BUCHUNGEN UND AUFZEICHNUNGEN

Gemäß Art. 3.2.3 der GoBD müssen Belege und Dokumente „zeitgerecht“ gebucht werden. Das bedeutet, dass ein zeitlicher Zusammenhang zwischen den Vorgängen und ihrer Buchung bestehen muss. Demnach ist ein Geschäftsvorfall möglichst unmittelbar nach seiner Entstehung zu erfassen. Des Weiteren muss ein zeitnaher Zugriff auf die Daten ermöglicht werden.

Im Hinblick auf den zeitnahen Datenzugriff sollte die Archivierungslösung über Möglichkeiten verfügen, archivierte Belege und Dokumente schnell – beispielsweise über Such- Tools oder Integration in E-Discovery wiederzufinden. Werden Datensätze mit Metadaten versehen, kann eine Datensuche beschleunigt werden. Die zentrale Aufbewahrung und Speicherung der Daten in einem System bildet die Basis für die spätere Verarbeitung, Suche und Beweisführung.

ORDNUNG UND KLARHEIT

Art. 3.2.4 der GoBD fordert eine systematische Erfassung sowie übersichtliche, eindeutige und nachvollziehbare Buchungen von Geschäftsvorfällen. Demnach sind Bücher und Aufzeichnung nach einem bestimmten Ordnungsprinzip zu führen. Belege müssen so gesammelt und aufbewahrt werden, dass die Geschäftsvorfälle leicht, identifizierbar feststellbar und für einen die Lage des Vermögens darstellenden Abschluss unverlierbar sind. Laut Art. 3.2.4 der GoBD müssen Geschäftsvorfälle so verarbeitet werden, dass innerhalb einer angemessenen Zeit ein Überblick über die Vermögens- und Ertragslage gewährleistet wird. Zudem müssen Buchungen unverzüglich lesbar gemacht werden können.

Eindeutigkeit und Nachvollziehbarkeit implizieren, dass Belege so aufbewahrt werden müssen, wie sie eingegangen sind.

UNVERÄNDERBARKEIT UND DATENSICHERHEIT

Art 3.5.2 der GoBD fordert, dass Daten vor unbefugtem Zugang, Manipulation oder Verlust geschützt werden müssen.

Archivierte Daten dürfen nicht mehr verändert oder gelöscht werden und sind gegen unbefugte Zugänge und Zugriffe zu schützen (z. B. durch eine AES-256 Verschlüsselung). Jegliche Zugriffe und Änderungen müssen gekennzeichnet und lückenlos protokolliert werden sowie nachvollziehbar sein. Für Unternehmen ist dies eine essentielle Anforderung, da die Buchführung nicht mehr ordnungsgemäß ist, wenn die Daten nicht ausreichend geschützt oder nicht mehr vorgelegt werden können.

VERFAHRENSDOKUMENTATION

Die GoBD fordert, dass alle Prozesse und Abläufe einer Aufbewahrung in einer Verfahrensdokumentation protokolliert werden – aus organisatorischer und technischer Sicht. Dies dient dazu, den GoBD Grundsatz der Nachvollziehbarkeit einzuhalten. Die Aufbewahrungsdauer der Verfahrensdokumentation entspricht dabei den Aufbewahrungsdauern der jeweiligen Belege und steuerlich relevanten Unterlagen, für die diese aufgesetzt wurde. Für die Verfahrungsdokumentation gelten die sonstigen GoBD Anforderungen genauso wie auch für Belege und steuerlich relevante Unterlagen.

4. DAS IT-SICHERHEITSGESETZ

Das IT-Sicherheitsgesetz trat im Juli 2015 in Kraft und definiert Regelungen für den Schutz von kritischen Infrastrukturen (KRITIS) in Deutschland. Das Gesetz dient der Erhöhung der Sicherheit informationstechnischer Systeme und gilt für alle Betreiber kritischer Infrastrukturen.

Betreiber Kritischer Infrastrukturen sind laut § 2 BSIG dazu verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.

AUSWIRKUNGEN DES IT SICHERHEITSGESETZES AUF DIE DATENSPEICHERUNG UND -ARCHIVIERUNG

Das IT-Sicherheitsgesetz spielt im Kontext der Datensicherheit, Verfügbarkeit und Archivierung eine wichtige Rolle. Die wesentlichen Anforderungen des IT-Sicherheitsgesetz im Hinblick auf Datenarchivierungslösungen werden im Folgenden zusammengefasst.

VERFÜGBARKEIT

Die Verfügbarkeit der archivierten Daten muss während der gesamten Archivierungsdauer sichergestellt werden. Ein plattenbasierter Archivspeicher (JBOD/SAN/NAS) gewährleistet hierbei schnelle Zugriffszeiten und eine hohe Verfügbarkeit.

DATENINTEGRITÄT UND AUTHENTIZITÄT

Eine Archivierungslösung sollte Funktionen für Integritätschecks, Erkennung korrupter Datensätze und die Ersetzung mit validen Daten sowie Mandantenfähigkeit aufweisen, um Datenintegrität sicherzustellen.

VERTRAULICHKEIT

Eine Zugriffskontrolle und Changelog zeichnet alle Zugriffe und Vorfälle bei der Datenarchivierung auf. Mithilfe einer AES-256 Verschlüsselung können unautorisierte Zugänge zu Archivdaten unterbunden werden.

NACHWEISPFLICHT

Für die Betreiber von Kritischen Infrastrukturen gilt eine Nachweispflicht. Hierbei muss vor dem BSI alle zwei Jahre nachgewiesen werden, dass für die IT-Systeme der aktuelle Stand der Technik eingehalten wird. Sofern die IT-Systeme dem Stand der Technik entsprechen, bieten archivierte Daten die Basis für die Erstellung von Analysen und Berichte z. B. bezüglich der Anzahl und Zeitpunkte der Angriffe und des Ausmaßes einer Störung.

Eine Archivierungslösung bietet dabei die Möglichkeit, Dokumenten wie z. B. Datenschutzhandbücher, Zertifikate, Nachweise, Vorfallsberichte, Pläne und Analysen zu archivieren und vorzulegen. Mithilfe der Archivierungslösung sollten archivierte Dokumente und Daten mit Metadaten versehen werden können. Des Weiteren sind bei der Archivierung datenschutzrechtliche Vorgaben einzuhalten.

5. DER SCHUTZ VON GESCHÄFTSGEHEIMNISSEN

In Umsetzung der entsprechenden EU-Richtlinie zum Schutz von Geschäftsgeheimnissen ist das deutsche Recht mit Wirkung zum April 2019 grundlegend geändert worden. Wo das alte Recht nur kaufmännische Informationen (Geschäftsgeheimnisse) und technisches Know-how (Betriebsgeheimnisse) schützte, ist der Schutzbereich nach neuem Recht wesentlich erweitert worden.

Alle Informationen, die geheim gehalten werden und von kommerziellem Interesse sind, unterliegen dem Geheimnisschutz. Geschützt sein können also technisches Know-how, etwa Verfahren, Konstruktionspläne, Algorithmen, Prototypen oder Rezepturen, aber auch geschäftliche Informationen wie Kundenlisten, Business-Pläne oder Werbestrategien. Wesentliche und zugleich entscheidende Voraussetzung ist jedoch, dass diese geheimen Informationen nur dann geschützt sind, wenn deren Inhaber sie mit den nach den „Umständen angemessenen Geheimhaltungsmaßnahmen“ sichert. Wird ihr der Inhaber der Information nicht gerecht, so verliert er den Geheimnisschutz.

Die nach den Umständen angemessen Sicherungsmaßnahmen, die zu verlangen sind, bestehen zum einen aus organisatorischen Maßnahmen – Beschränkung des Personenkreises entsprechend dem „Need to know“-Prinzip, vertragliche Absicherung durch Geheimhaltungsbestimmungen – aber ganz wesentlich auch aus technischen Maßnahmen.

Die Datenhaltung in Produktivsystemen wie Archivsystemen müssen dem Stand der Technik unter Berücksichtigung des Schutzgrades der Informationen und der damit verbundenen angemessenen Kosten der technischen Absicherung entsprechen.

6. ERFÜLLUNG DER RECHTLICHEN VORGABEN MIT SOFTWARE-DEFINED ARCHIVING UND ITERNITY ICAS

Die Software-Defined Archiving Lösung iCAS ermöglicht eine rechts- und datenschutzkonforme Speicherung und Archivierung wichtiger Unternehmensdaten. Schlüsselfunktionen von iCAS sind der Schutz der Integrität und Verfügbarkeit kritischer Daten sowie die Verwaltung der Aufbewahrungsfristen auf Speicherebene. Die Softwarelösung arbeitet als Middleware zwischen Geschäftsanwendungen/ Datenquellen (z. B. DMS, ECM, ERP) und der Speicherinfrastruktur (z. B. NAS, DAS, SAN, Cloud) und sichert Daten unabhängig von der eingesetzten Speichertechnologie. iCAS wurde durch die KPMG geprüft und zertifiziert.

Die Funktionen von iTernity iCAS im Überblick:

- Mittels der patentierten und zertifizierten CSC-Technologie (Content Storage Container), bietet iCAS WORM-Funktionalität (Write Once Read Many) zum Schutz der Daten. Die CSC-Technologie legt die zu archivierenden Daten und Dokumente gemeinsam mit den zugehörigen Metadaten, dem Erstellungs- und Aufbewahrungsdatum in Datencontainern ab. Diese können auf beliebige Datenträger gespeichert werden und bleiben über SHA-512-Bit-Hashwerte verifizierbar. Somit können die Archivdaten jederzeit auf ihre Integrität geprüft werden.
- Die Unabhängigkeit der Softwarelösung von der genutzten Speicher- und Serverhardware bietet deutliche Kostenvorteile gegenüber hardwaregebundenen Archivsystemen (Blackbox-Systemen). Diese Unabhängigkeit bietet zudem enorme Flexibilität und ermöglicht es Unternehmen ihre Infrastruktur auf dem Stand der Technik zu halten und gleichzeitig ihre Investitionen in diese Infrastruktur zu schützen.
- Durch die Trennung der eigentlichen Archivfunktionalität von den Funktionen der DMS- /ECM-Lösungen ist eine höhere Sicherheit der Archivdaten gewährleistet. Zudem können Daten aus verschiedenen Anwendungen leicht in einzelnen Bereichen (Repositories) innerhalb eines Zentral-Archivs abgelegt werden, was die Administration des Archivs optimiert.
- Die Flexibilität und Offenheit von iCAS ermöglicht eine effiziente Nutzung bereits vorhandener oder neu erworbener Speicherkapazität und damit deutliche Kosteneinsparungen. Investitionen in Hardware, Software und Schulungen bleiben geschützt, da diese Komponenten auch für das Archiv genutzt werden können. Die Integration der Archivdaten in bestehende Backup- und Wiederherstellungsprozesse kann ebenfalls problemlos erfolgen.
- Während den langen Aufbewahrungszeiten von 10 oder mehr Jahren wird es technologische

Weiterentwicklungen der Speichertechnologien geben. Diese und die dazugehörigen Systeme können aufgrund der Offenheit von iCAS einfach in das Archivkonzept integriert werden.

- Für die langfristige Verfügbarkeit ist es wichtig, dass die Archivdaten möglichst einfach und kostengünstig während des laufenden Betriebs auf neue Speichersysteme migriert werden können. Da die iCAS Archivcontainer selbsttragend sind, können sie einfach migriert und anschließend verifiziert werden.
- iCAS kann die Archivdaten nach dem sicheren AES-256 Standard verschlüsseln und dadurch verschiedene Privacy-Anforderungen erfüllen (wie z. B. DSGVO oder PCI-DSS im Finanzsektor).
- Die Self-Healing Funktionalität von iCAS ermöglicht ein Monitoring des Archivs, das inkonsistente Archivobjekte identifiziert und diese automatisch repariert. Die durch iCAS auf zwei Speicherziele replizierten Daten werden dabei stetig auf ihre Integrität überwacht. Da iCAS die Archivobjekte inhaltsbezogen und objektorientiert verwaltet (content-aware-storage), kann sichergestellt werden, dass Anwender langfristig immer auf valide Archivdaten zugreifen können.

7. FAZIT

Eine gesetzeskonforme Aufbewahrung und Archivierung von Daten und Dokumenten kann nur durch organisatorische und technische Maßnahmen erreicht werden. Die EU-DSGVO, die GoBD, das IT Sicherheitsgesetz und die Regelungen zum Schutz von Geschäftsgeheimnissen definieren hierfür klare Vorgaben und Einschränkungen.

Für Unternehmen reicht der Einsatz eines Dokumentenmanagementsystems (DMS) oder die reine Speicherung/Fileablage nicht aus. Dokumente, die durch ein DMS/ECM auf einer Fileablage gespeichert wurden, lediglich nicht zu löschen, stellt keine gesetzeskonforme Aufbewahrung der Daten dar.
Bei diesem Vorgehen werden die gesetzlichen Anforderungen z. B. an die Integritätssicherung und unveränderbare Speicherung der Dokumente nicht erfüllt.

Nur wenn man die Dokumente während der gesamten Aufbewahrungsdauer innerhalb einer angemessenen Frist findet, sie dann in ihrem Zusammenhang noch versteht und nachweisen kann, dass sie nicht nachträglich verändert wurden, liegen beweiskräftige Dokumente vor. Eine softwarebasierte Lösung, wie iTernity iCAS, erfüllt genau diesen Zweck. Die Archivierungslösung sichert die Integrität und Verfügbarkeit wichtiger Unternehmensdaten und verwaltet die Aufbewahrungsfristen auf Speicherebene. Die Softwarelösung iCAS gewährleistet damit die Einhaltung verschiedener gesetzlicher Standards (EU-DSGVO, GoBD, IT-Sicherheitsgesetz, Basel III, SOX, HIPAA, SEC 17a-4 etc.) und bietet eine sichere Plattform für verschiedene Datenquellen und Geschäftsanwendungen – zukunftssicher, datenschutzkonform und hardwareunabhängig.

8. WEITERFÜHRENDE LITERATUR

- Erfahren Sie in verschiedensten Referenzstories, wie Unternehmen aus allen Branchen von Software-Defined Archiving profitieren
- Eine zentrale Archivierungs-Plattform als Basis für DSGVO Compliance: So erfüllen Sie die konkreten DSGVO Anforderungen mit iCAS
- Compliance und Datenintegrität für SAP Archivdaten: So schützen Sie Ihre SAP Dokumente und Daten auf lange Sicht

iTernity GmbH

WIR BRINGEN IHRE DATEN SICHER IN DIE ZUKUNFT

Wir sichern Ihre geschäftskritischen Daten. Ihr Vertrauen ist unser Ansporn und eine Investition in die Zukunft. Das Ergebnis: mehr Sicherheit, weniger Aufwand, keine Sorgen.

Unsere DNA ist Archivierung, unsere Mission die langfristige Verfügbarkeit und Integrität von Unternehmensdaten aller Art. Unser Fokus liegt auf Ihren Herausforderungen, egal ob Datenschutz, Kostendruck, Datenwachstum, Cyber-Angriffe, Zeitmangel oder Komplexität – wir bringen Ihre Daten sicher in die Zukunft.

KONTAKTIEREN SIE UNSERE EXPERTEN

Heinrich-von-Stephan-Straße 21 | 79100 Freiburg
info@iTernity.com | +49 761 590 34 810 | www.iTernity.com