Rechtliche Anforderungen an die Archivierung

Know-how Die gesetzlichen Anforderungen an die Archivierung sind komplex. Ein Überblick der Vorgaben und Pflichten, die bei der Aufbewahrung von Dokumenten gelten.

Von Reto Zbinden

Information Governance hat zum Ziel, die Bearbeitung von Informationen basierend auf Grundsätzen, Leitlinien und Weisungen unternehmensweit zu steuern und zu optimieren und ist ein ganzheitlicher Ansatz zur Verwaltung von Unternehmensinformationen mittels definierter Prozesse, Rollen, Kontrollen und Metriken, die allesamt Informationen konsequent als wertvolles Business Asset behandeln.

Information Governance bietet den Rahmen für den sicheren, vertraulichen und rechtskonformen Umgang mit Informationen, der es dem jeweiligen Unternehmen und dessen berechtigten Mitarbeitenden ermöglicht, Informationen entsprechend ihrer Vertraulichkeits-, Verfügbarkeits- und Integritätsanforderungen gezielt, effizient und effektiv zur bestmöglichen Aufgabenerfüllung und Erreichung wirtschaftlich optimaler Resultate zu bearbeiten.

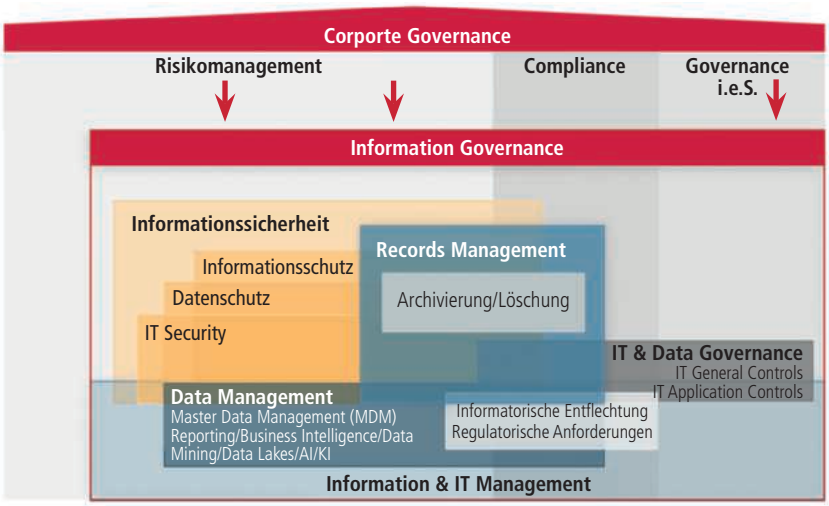
Die Themen Informationssicherheit, Records Management und Archivierung sind ebenso Bestandteil der Information Governance. Damit sollen die mit der Erstellung, Nutzung und Weitergabe von Unternehmensdaten verbundenen Risiken reduziert und Massnahmen zum Schutz der Informationen definiert, aufeinander abgestimmt, überprüft und laufend optimiert werden.

Die Informationssicherheit soll eine angemessene Vertraulichkeit, Verfügbarkeit und Integrität der bearbeiteten Informationen und der zu deren Bearbeitung eingesetzten Funktionen, Systeme und Prozesse erreichen und aufrechterhalten. Insbesondere öffentliche Verwaltungen, so beispielsweise der Bund, ergänzen die Schutzziele der Informationssicherheit um den Begriff «Nachvollziehbarkeit». Die sich überschneidenden Bereiche Datenschutz (Bearbeitung Personendaten), IT-Sicherheit (digitale Bearbeitung bzw. digitale Instrumente) und Informationsschutz (Vertraulichkeit unternehmenseigener Informationen) bilden gemäss Lehre und Praxis Teil der Informationssicherheit.

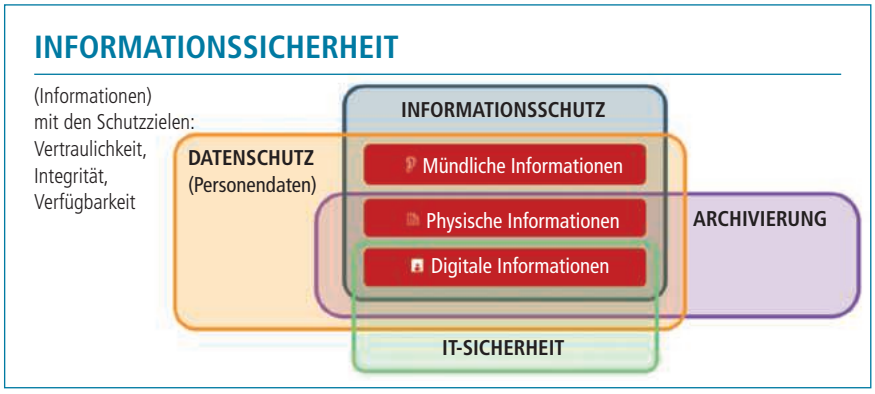
Archivierung, verstanden als rechtskonforme Aufbewahrung von Informationsobjekten gemäss internen und externen Vorgaben, wird häufig dem Thema Informationssicherheit zugeordnet. Dies unter anderem deshalb, weil die Mechanismen zur Erreichung der gesetzlich geforderten Fälschungssicherheit des Archivguts im Bereich der IT-Sicherheit bestens bekannt sind. Die Archivierung bildet aber «nur» den zweitletzten Schritt (vor der Löschung) im übergeordneten Records Management-Prozess.

Unter Records Management (bzw. Aktenverwaltung oder Aktenführung) versteht man gemäss ISO 15489 die effiziente und systematische Erstellung, Entgegennahme, Pflege, Nutzung und Aussonderung von Aufzeichnungen einschliesslich der Erfassung und Aufbe-

INFORMATION GOVERNANCE IM UNTERNEHMEN



Themen innerhalb der Information Governance und Nahtstellen. Quelle: Swiss Infosec



Bei digitalen Informationen überschneiden sich Informationsschutz, Datenschutz, Archivierung und Cybersecurity. Quelle: Swiss Infosec

wahrung von Nachweisen und Informationen über Geschäftsabläufe und Transaktionen in Form von Akten.

Die Löschung bildet den letzten Schritt im Records-Management-Prozess. Gerade aber diese Löschung wird aktuell aufgrund der Datenschutzanforderungen leider allzu oft unabhängig von einem bestehenden Records Management umgesetzt. Zur Erreichung von zuverlässigen und nutzenstiftenden Löschvorgängen ist es aus Sicht des Autors dringend angezeigt, entsprechende Records-Management-Prozesse aufzubauen und umzusetzen. Löschkonzepte dürfen nicht Datenschutzinseln bleiben.

Anforderungen an Records Management und Archivierung

Für das Records Management relevante rechtliche Vorgaben ergeben sich insbesondere aus den Bestimmungen der Art. 957 ff. des schweizerischen Obligationenrechts (OR; SR 220), der Geschäftsbücherverordnung (GeBüV; SR 221.431), dem Mehrwertsteuergesetz (MWSTG; SR 641.20), der dazugehörigen Verordnung (MWSTV; SR 641.201) und den Prozessordnungen der Rechtspflegeorgane.

Einerseits müssen Informationen archiviert werden, die Ansprüche der Organisation begründen oder unberechtigte Ansprüche abwehren können (Beweiszweck). Die Organisation hat mit Hilfe entsprechender Aufzeichnungen den Nachweis einer ordnungsgemässen Geschäftsführung gegenüber Aufsichtsorganen und Gerichten zu erbringen.

Andererseits müssen gemäss OR die Geschäftsbücher, Buchungsbelege und die Geschäftskorrespondenz mit Belegcharakter archiviert werden, die nach Art und Umfang des jeweiligen Geschäfts nötig sind, um die Vermögenslage des Unternehmens und die mit dem Geschäftsbetrieb zusammenhängenden Schuld- und Forderungsverhältnisse sowie die Ergebnisse der einzelnen Geschäftsjahre festzustellen.

Geschäftsbücherverordnung und Verfahrensdokumentation

Die Geschäftsbücherverordnung (GeBüV) beschreibt in den Art. 2 bis 4 die allgemeinen Voraussetzungen betreffend Führung und Aufbewahrung der Bücher.

Neben einem Verweis auf die allgemeinen Grundsätze der ordnungsgemässen Buchführung, die in jedem Falle eingehalten werden müssen, bestimmt Art. 2 Abs. 2, dass bei der elektronischen Führung der Bücher die Grundsätze der ordnungsgemässen Datenverarbeitung zu beachten sind. Die Ordnungsmässigkeit richtet sich gemäss Abs. 3 nach den anerkannten Standards zur Rechnungslegung, sofern die Gesetzgebung nichts anderes vorsieht (ordnungsgemässe Datenverarbeitung).

Gemäss Art. 3 müssen die archivierten Informationen so erfasst und aufbewahrt werden, dass sie nicht geändert werden können, ohne dass sich dies feststellen lässt (Schutz Integrität). Geschäftsunterlagen müssen unveränderlich erfasst und aufbewahrt werden.

Gemäss Art. 4 sind die Organisation, die Zuständigkeiten, die Abläufe und Verfahren und die Infrastruktur (Maschinen und Programme), die bei der Archivierung zur Anwendung kommen, in Arbeitsanweisungen so zu dokumentieren, dass die Geschäftsbücher und die Buchungsbelege verstanden werden können. Die Arbeitsanweisungen sind zu aktualisieren und nach den gleichen Grundsätzen und gleich lang aufzubewahren wie die Geschäftsbücher, die danach geführt wurden (Arbeitsanweisungen).

Gemäss Art. 5 sind die archivierten Informationen sorgfältig, geordnet und vor schädlichen Einwirkungen geschützt aufzubewahren (Schutz). Für die elektronische Verwaltung reicht somit die blosse Aufbewahrung auf einem «sicheren» Medium allein nicht aus, sondern es sind weitere Vorkehrungen zu treffen.

Gemäss Art. 6 müssen die aufbewahrten Unterlagen ausserdem jederzeit innert angemessener Frist eingesehen und geprüft werden können (Verfügbarkeit). Soweit es für die Einsicht und die Prüfung erforderlich ist, sind das entsprechende Personal sowie die Geräte oder Hilfsmittel verfügbar zu halten. Im Rahmen des Einsichtsrechts muss die Möglichkeit bestehen, die Informationen auf Begehren einer berechtigten Person auch ohne Hilfsmittel lesbar zu machen.

Gemäss Art. 7 sind archivierte Informationen von den aktuellen Informationen zu trennen beziehungsweise so zu kennzeichnen, dass eine Unterscheidung möglich ist. Die Verantwortung für die archivierten Informationen ist klar zu regeln und zu dokumentieren (Trennung, Verantwortung).

Gemäss Art. 8 sind die Informationen systematisch zu inventarisieren und vor unbefugtem Zugriff zu schützen. Zugriffe und Zutritte sind aufzuzeichnen. Diese Aufzeichnungen unterliegen derselben Aufbewahrungspflicht wie die Datenträger (Inventarisierung, Zugriff, Zutritt).

Gemäss Art. 9 sind zur Aufbewahrung von Unterlagen folgende Informationsträger zulässig:

a) unveränderbare Informationsträger, namentlich Papier, Bildträger und unveränderbare Datenträger und/oder
b) veränderbare Informationsträger, wenn:
   1. technische Verfahren zur Anwendung kommen, welche die Integrität der gespeicherten Informationen gewährleisten (z.B. digitale Signaturverfahren);
   2. der Zeitpunkt der Speicherung der Information unverfälschbar nachweisbar ist (z.B. durch Zeitstempel);
   3. die zum Zeitpunkt der Speicherung bestehenden weiteren Vorschriften über den Einsatz der betreffenden technischen Verfahren eingehalten werden; und
   4. die Abläufe und Verfahren zu deren

Einsatz festgelegt und dokumentiert sowie die entsprechenden Hilfsinformationen (wie Protokolle und Log Files) ebenfalls aufbewahrt werden.

Informationsträger gelten als veränderbar, wenn die auf ihnen gespeicherten Informationen geändert oder gelöscht werden können, ohne dass die Änderung oder Löschung auf dem Datenträger nachweisbar ist.

Gemäss Art. 10 sind Informationsträger periodisch auf Integrität und Lesbarkeit zu prüfen. Daten dürfen in andere Formate umgewandelt oder auf andere Informationsträger übertragen werden (Datenmigration), falls ihre Vollständigkeit, Richtigkeit, Verfügbarkeit und Lesbarkeit dabei gewährleistet bleibt und die Verfügbarkeit und die Lesbarkeit den gesetzlichen Anforderungen weiterhin genügen. Datenmigrationen sind zu protokollieren und die Protokolle mit den Informationen aufzubewahren.

Die Abläufe, die Verfahren und die Infrastruktur (Systeme, Software), die bei der Archivierung zur Anwendung kommen, müssen so dokumentiert werden, dass sie und die damit verbundenen Verantwortlichkeiten nachvollzogen und verstanden werden können. Die Verfahrensdokumentation muss einem sachverständigen Dritten in angemessener Zeit einen Überblick über sämtliche Aspekte des Verfahrens ermöglichen.

Die Verfahrensdokumentation dokumentiert den organisatorischen und technischen Gesamtprozess von der Entstehung der Informationen über die Indizierung und Speicherung, dem eindeutigen Wiederfinden, der Absicherung gegen Verlust und Verfälschung und der Reproduktion am Bildschirm und auf dem Drucker. Die Verfahrensdokumentation ist entsprechend der Änderungen am System fortzuschreiben.

Datenschutz

Das seit dem 1. September 2023 geltende Datenschutzgesetz auf Stufe Bund (verbindlich für die Privatwirtschaft und den Bund) verlangt, dass Personendaten durch angemessene technische und organisatorische Massnahmen geschützt werden müssen (vgl. Art. 8 DSG). Die Mindestanforderungen an die Datensicherheit werden in allgemeiner Weise in der Datenschutzverordnung (DSV) vom 31. August 2022 erläutert. Dabei wurde bewusst auf die Nennung konkreter Sicherheitsanforderungen verzichtet (mit Ausnahme der Protokollierung und der Erstellung von Bearbeitungsreglementen in Fällen, in denen besonders schützenswerte Personendaten in grosser Anzahl automatisiert bearbeitet werden), da eine Formulierung allgemeingültiger Mindestanforderungen an die Datensicherheit für alle Branchen kaum möglich ist.

Hinsichtlich der Datensicherheit verfolgt das Datenschutzgesetz einen risikobasierten Ansatz. Das heisst, je sensibler die bearbeiteten Daten sind, desto höher sind die Anforderungen an die Datensicherheit. Die Konkretisierung der notwendigen technischen und organisatorischen Massnahmen erfolgt innerhalb der Organisation und projektbezogen.

Archivierungsfristen

Bei der Aufbewahrung von Geschäftsdokumenten, die Personendaten enthalten, stellt sich vorab die Frage, ob eine gesetzliche Aufbewahrungsfrist anwendbar ist. Ist das der Fall, müssen und dürfen Dokumente während dieser Dauer nicht gelöscht werden. Beispielsweise müssen Buchungsbelege 10 Jahre aufbewahrt werden (Art. 958f OR).

Für die Zeit nach Ablauf dieser Dauer oder falls keine gesetzliche Aufbewahrungsfrist besteht, können Dokumente in datenschutzrechtlicher Hinsicht zunächst so lange verwendet und aufbewahrt werden, wie die darin enthaltenen Personendaten zum Zweck, zu dem sie erhoben wurden, noch gebraucht werden. Beispielsweise können Unterlagen, die für das Verfassen eines Arbeitszeugnisses benötigt werden, solange behalten werden, wie das Anstellungsverhältnis dauert. Grundlagendokumente des Unternehmens, wie etwa dessen Statuten oder Organisationsreglemente, sollten während der ganzen Lebensdauer des Unternehmens aufbewahrt werden.

Werden Personendaten nicht mehr gebraucht, kann im Allgemeinen angenommen werden, dass Unterlagen zu legitimen Beweiszwecken noch so lange aufbewahrt werden dürfen (aber nicht müssen), als die Verjährungsfrist der zugrundeliegenden Forderung noch nicht abgelaufen ist, ausser Datenschutzaspekte geben den Ausschlag für eine frühere Vernichtung/Löschung von Personendaten (was nicht das gesamte Dokument erfassen muss). Die Verjährung spricht den Zeitpunkt an, ab dem eine Forderung nicht mehr (gerichtlich) durchgesetzt werden kann. Bei der Frage, welche Unterlagen während laufender Verjährungsfrist noch zu behalten sind, geht es im Wesentlichen um die Einschätzung, wie das Unternehmen im Hinblick auf potenzielle rechtliche Auseinandersetzungen aufgestellt sein will.

Zusammengefasst lässt sich die Aufbewahrungsdauer von Dokumenten mit Personendaten anhand von drei Fragen nachvollziehen (in dieser Reihenfolge):

a) Besteht eine gesetzliche Aufbewahrungsfrist?
b) Werden die Personendaten noch gebraucht?
c) Wenn nicht: ist eine weitere Aufbewahrung zu (legitimen) Beweiszwecken erforderlich (Verjährungsfristen), die im Einklang mit dem Datenschutz steht?

Wenn alle drei Fragen mit nein beantwortet werden, verlangt der Datenschutz, dass Personendaten, die nicht mehr gebraucht werden, gelöscht (oder anonymisiert) werden oder der Zugriff darauf und die Verwendung zumindest stark eingeschränkt wird. Daneben können auch von einer Datenbearbeitung Betroffene entsprechende Rechte geltend machen.

Da die gesetzliche Aufbewahrungspflicht für Geschäftsbücher, Geschäftsbericht und Buchungsbelege 10 Jahre beträgt und auch die meisten Forderungen nach 10 Jahren verjähren, haben sich für die Aufbewahrungsfrist als genereller Richtwert 10 Jahre eingebürgert (vom Zeitpunkt an, an dem die Personendaten nicht mehr regelmässig benötigt werden). Überwiegende Interessen einer von einer

DER AUTOR

Rechtsanwalt **Reto Zbinden,** Gründer und Inhaber von Swiss Infosec, beschäftigt sich neben seiner Führungstätigkeit als Berater und Ausbildner. Seine Fachgebiete sind Sicherheit und Organisation, Zertifizierung im Bereich der Informationssicherheit und die rechtlichen Aspekte der Informationssicherheit, so unter anderem Archivierung, Datenschutz und Vertragsrecht im Bereich IT und Informationssicherheit.

Datenbearbeitung betroffenen Person können aber im Sinne des Datenschutzes eine frühere Vernichtung, Löschung beziehungsweise Anonymisierung von Personendaten verlangen.

Im Einzelnen ist darauf zu achten, ob gesetzliche Aufbewahrungsfristen anwendbar sind, Personendaten für den bestimmungsgemässen Zweck (noch) benötigt werden und sich allenfalls unter Berücksichtigung der jeweils relevanten Verjährungsfrist eine ausgedehntere Aufbewahrung zu Beweiszwecken aufdrängt.

Anpassung Verjährungsrecht

Seit anfangs 2020 verjähren Forderungen aus Personenschäden spätestens 20 Jahre nachdem das schädigende Verhalten erfolgte oder aufhörte (absolute Frist). Sieht sich ein Unternehmen also mit einer gewissen Wahrscheinlichkeit dem Risiko ausgesetzt, entsprechende Forderungen in der Zukunft bestreiten zu müssen, sollten entsprechende Dokumente genügend lange aufbewahrt werden (wenn nicht zwingende Datenschutzgründe dagegensprechen).

Geschäftskorrespondenz: Gesetzesänderung 2013/2015

Gemäss Art. 958f OR bezieht sich die gesetzliche Aufbewahrungsfrist lediglich auf Korrespondenz, die den Charakter von Buchungsbelegen hat. Seit dem 1. Januar 2015 ist im Gesetz keine ausdrückliche Pflicht zur Aufbewahrung von Geschäftskorrespondenz mehr vorgesehen. Während zehn Jahren aufbewahrungspflichtig sind grundsätzlich die Geschäftsbücher, der Geschäftsbericht, der Revisionsbericht und die Buchungsbelege (Art. 958f OR). Legitime Aufbewahrungsinteressen können darüber hinaus eine ebenso lange Archivierung rechtfertigen. Es ist aber nicht davon auszugehen, dass dies auf sämtliche in einem Unternehmen ausgetauschten E-Mails zutrifft.

Mehrwertsteuer: Gesetzesänderung

Im Mehrwertsteuergesetz ist seit dem 1. Januar 2018 der Grundsatz der Beweismittelfreiheit festgehalten, so dass grundsätzlich bei Einhaltung der handelsrechtlichen Bestimmungen zur ordnungsgemässen Buchführung nach Artikel 957a OR der mehrwertsteuerliche Nachweis des Ursprungs und der Unveränderbarkeit eines Beleges gegeben ist. Die Mehrwertsteuerverordnung (MWSTV) hält im Abschnitt über die papierlosen Belege nur fest, dass für die volle Beweiskraft von elektronischen Buchungsbelegen die Artikel 957– 958f des Obligationenrechts (Grundsätze ordnungsmässiger Buchführung) sowie die Bestimmungen der GeBüV massgebend sind.

Anforderungen an die Archivierung

Mit folgenden Schritten lassen sich die gesetzlichen Anforderungen an die Archivierung umsetzen:

1. Erstellen einer Archivierungsweisung.
2. Erstellen eines Aktenplanes (Hierarchisch strukturierte Auflistung der Akten/Records/Informationen). Enthält eine inhaltliche Beschreibung der Akten, klassifiziert und typisiert diese und regelt deren Aufbewahrungsdauer sowie den Beginn der Aufbewahrungsfrist.
3. Erstellen einer Verfahrensdokumentation für das Archivsystem. ■

dun & bradstreet

Weg mit Duplikaten. Weg mit veralteten Daten.

Bringen Sie Ihre Stammdaten auf Vordermann!

6´000 Unternehmen wechseln in jeder Stunde ihre Adresse

https://www.dnb.com/de-ch/stammdaten