****

**Vorlage für eine Richtlinie zur Aufbewahrung und Vernichtung von Daten**

*Von Paul Kirvan, FBCI, CISA*

|  |
| --- |
| **Titel:** Richtlinie zur Aufbewahrung und Vernichtung von Daten  |
| **Abteilung** | **Version:** Original |
| **Genehmigt durch:** | **Datum der Genehmigung:**  |
| **Genehmigung der Geschäftsleitung:** |
| **Datum des Inkrafttretens:** | **Zuletzt aktualisiert:** |
| **Autor:** |
| **Umfang**Diese Richtlinie gilt für den <Standort angeben>> von <Firmenname>. <Adresse eingeben> |
| **Behörde** Diese Policy wird hiermit gebilligt und genehmigt.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Unterschrift Titel Datum \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Unterschrift Titel Datum \_\_\_\_\_\_\_\_\_\_\_\_ |
| **Zweck** Zweck dieser Richtlinie ist es, die Aktivitäten im Zusammenhang mit der Entwicklung, Aktualisierung und Einführung von Plänen und Verfahren zur Datenaufbewahrung und -vernichtung festzulegen, die <Name des Unternehmens> Informationssysteme, Netzwerke, Daten, Datenbanken und andere Informationswerte schützen. Zusätzliche Richtlinien, die die Datenverwaltung regeln, werden separat behandelt. Zu den weiteren Zwecken dieses Plans gehören die Einhaltung der geltenden Normen und Vorschriften zur Datenaufbewahrung und -vernichtung sowie die Einhaltung von Umwelt-, Nachhaltigkeits- und ähnlichen Vorschriften.  |
| **Umfang**Der Geltungsbereich dieser Richtlinie zur Datenaufbewahrung und -vernichtung umfasst alle informationstechnischen Systeme, Software, Datenbanken, Anwendungen und Netzwerkressourcen, die das Unternehmen zur Ausübung seiner Geschäftstätigkeit benötigt. Die Richtlinie gilt für alle Mitarbeiter des Unternehmens, Auftragnehmer und andere autorisierte Drittorganisationen. |
| **Erklärung zur Einhaltung der Vorschriften**Diese Richtlinie ist so konzipiert, dass sie mit dem U.S. Data Protection Act von 1998, dem Freedom of Information Act von 2000, dem Fair and Accurate Credit Transactions Act von 2003 (FACTA), dem Personal Information Protection and Electronic Documents Act (PIPEDA) in Kanada, dem Gramm-Leach-Bliley Act (GLBA), der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union, ISO 27040: Information Technology -- Security techniques -- Storage security und NIST SP 800-209 -- Security Guidelines for Storage Infrastructure übereinstimmt.Die Einhaltung der Richtlinien zur Datenaufbewahrung und -vernichtung wird von der IT-Abteilung mit Unterstützung der Abteilungsleitung und der Fachexperten von <Name des Unternehmens> verwaltet. Um die Einhaltung der Richtlinien zu gewährleisten, müssen die Programme zur Datenaufbewahrung und -vernichtung geeignete Verfahren umfassen und die personellen und technischen Ressourcen zur Erfüllung der Richtlinienanforderungen festlegen. Die Überprüfung der Einhaltung (insbesondere der Datenvernichtung) wird monatlich von der IT-Abteilung, der Innenrevision oder einer anderen geeigneten Stelle durchgeführt.  |
| **Policy**Die Abteilung Informationstechnologie (IT) ist für die Verwaltung aller Datenaufbewahrungs- und Vernichtungsaktivitäten des Unternehmens zuständig. Andere Abteilungen, wie Finanz- und Rechnungswesen, Betrieb und Personalwesen, sind ebenfalls dafür verantwortlich, der IT-Abteilung ihre Anforderungen an die Datenaufbewahrung und -vernichtung mitzuteilen. Die IT-Abteilung ist für die Entwicklung, Ausführung und regelmäßige Prüfung der Verfahren zur Datenaufbewahrung und -vernichtung verantwortlich. Die IT-Abteilung erkennt außerdem an, dass sie bei ihren Tätigkeiten die entsprechenden Industriestandards für die Datenaufbewahrung und -vernichtung einhalten wird. 1. Das Unternehmen entwickelt umfassende Pläne für die Aufbewahrung und Vernichtung von Daten im Einklang mit bewährten Datenverwaltungspraktiken, wie sie in festgelegten Standards definiert sind.
2. Die Aufbewahrung und Vernichtung von Daten erfolgt im Rahmen des Datenverwaltungsprogramms des Unternehmens, das das gesamte Programm zur Verwaltung von Technologiedaten verwaltet und leitet.
	* Planung und Gestaltung von Maßnahmen zur Datenaufbewahrung und -vernichtung.
	* Ermittlung von Teams für die Datenaufbewahrung und -vernichtung, Festlegung ihrer Aufgaben und Zuständigkeiten und Sicherstellung, dass sie ordnungsgemäß geschult und auf die Erfüllung ihrer Aufgaben vorbereitet sind.
	* Planung, Gestaltung und Dokumentation von Plänen zur Aufbewahrung und Vernichtung von Daten.
	* Planung von Aktualisierungen der Risikoanalysen zur Datenaufbewahrung und -vernichtung
	* Planung und Durchführung von Sensibilisierungs- und Schulungsmaßnahmen für Mitarbeiter und Mitglieder des Teams für Datenaufbewahrung und -vernichtung.
	* Planung und Durchführung von Übungen zur Datenaufbewahrung und -vernichtung.
	* Entwurf und Umsetzung von Maßnahmen zur Pflege der Datenaufbewahrung und -vernichtung, um sicherzustellen, dass die Pläne auf dem neuesten Stand und einsatzbereit sind.
	* Sicherstellung, dass die Verfahren zur Datenaufbewahrung und -vernichtung mit den Umwelt- und Nachhaltigkeitsmanagementprogrammen des Unternehmens vereinbar sind.
	* Vorbereitung der Überprüfung und des Audits der Pläne zur Datenaufbewahrung und -vernichtung durch das Management.
	* Planung und Durchführung von Maßnahmen zur kontinuierlichen Verbesserung der Aktivitäten und Pläne zur Datenaufbewahrung und -vernichtung.
3. Formelle Risikobewertungen (Risk Assessment, RA) und Analysen der Auswirkungen auf den Geschäftsbetrieb (Business Impact Analysis, BIA) müssen Anforderungen an die Datenaufbewahrung und -vernichtung enthalten; RAs und BIAs müssen mindestens jährlich aktualisiert werden, um sicherzustellen, dass sie mit den Anforderungen des Geschäftsbetriebs und seiner Technologie übereinstimmen.
4. Die Pläne und Zeitpläne für die Datenaufbewahrung und -vernichtung beziehen sich auf elektronische Daten, die auf elektronischen Medien wie CDs, Festplattenlaufwerken, Solid-State-Laufwerken, Magnetbändern und anderen zugelassenen Medien gespeichert sind.
5. Die Pläne und Zeitpläne für die Datenaufbewahrung und -vernichtung beziehen sich auf Daten, die auf nichtelektronischen Datenträgern (zum Beispiel Papierakten, Mikrofiche) gespeichert sind.
6. Die Pläne und Zeitpläne für die Datenaufbewahrung und -vernichtung beziehen sich auf elektronische Informationssysteme (zum Beispiel Server, Router, Switches) und Komponenten (zum Beispiel Verkabelung und Anschlüsse, Netzteile, Speicherschränke) sowie auf andere Vermögenswerte, die derzeit nicht mehr produziert werden oder deren Ausmusterung aus Produktionsumgebungen geplant ist.
7. In den Plänen und Zeitplänen für die Datenaufbewahrung werden die Aufbewahrungsanforderungen und die zugehörigen Metriken (zum Beispiel Dauer der Aufbewahrung, Art der Speichermedien) für elektronische und nichtelektronische Informationen sowie für die Systeme zur Unterstützung der IT-Infrastruktur festgelegt.
8. In den Plänen und Zeitplänen für die Datenvernichtung sind die Parameter für die Vernichtung elektronischer Daten (zum Beispiel Überschreiben, Neuformatierung, Degaussing, Löschen mit Hilfe von Firmware, Vernichtung physischer Datenträger), nichtelektronischer Daten (zum Beispiel Schreddern von Ausdrucken) sowie von Systemen und Komponenten (zum Beispiel Vernichtungsdienste Dritter) festzulegen.
9. Die Pläne und Zeitpläne für die Datenaufbewahrung und -vernichtung sind regelmäßig zu überprüfen und in einer geeigneten Umgebung zu testen, um sicherzustellen, dass Daten, Datenbanken, Medien, Systeme und andere relevante Elemente aufbewahrt oder vernichtet werden können und dass die Leitung und die Mitarbeiter von <Name des Unternehmens> verstehen, wie die Pläne und Zeitpläne auszuführen sind und welche Aufgaben und Verantwortlichkeiten sie haben.
10. Die Pläne und Zeitpläne für die Datenaufbewahrung und -vernichtung stehen im Einklang mit den Umwelt- und Nachhaltigkeitsprogrammen, die das Unternehmen eingeführt hat
11. Alle Mitarbeiter müssen über das Programm zur Aufbewahrung und Vernichtung von Daten sowie über ihre eigenen Aufgaben und Verantwortlichkeiten informiert werden.
12. Die Pläne für die Aufbewahrung und Vernichtung von Daten und andere Dokumente sind auf dem neuesten Stand zu halten und spiegeln bestehende und sich ändernde Umstände wider.
 |
| **Spezifikationen zur Datenaufbewahrung und -vernichtung** Nachfolgend sind die spezifischen technischen Anforderungen für die Aufbewahrung und Vernichtung von Daten aufgeführt:**Allgemein**1. Geben Sie die Häufigkeit und die Art der durchzuführenden Daten-/Systemaufbewahrungsaktivitäten an.
2. Geben Sie die Häufigkeit und Art der durchzuführenden Daten-/Systemvernichtungsmaßnahmen an.
3. Geben Sie den Zeitplan für die Aufbewahrung und Vernichtung von Daten an.
4. Geben Sie an, wer (zum Beispiel internes Personal, externe Dritte) für die Aufbewahrung und Vernichtung der Daten verantwortlich ist.
5. Geben Sie an, wer zu benachrichtigen ist, wenn ein Problem mit den Aufbewahrungs- und Vernichtungsaktivitäten festgestellt wird.

**Verfahren zur Aufbewahrung von Daten/Systemen** 1. Geben Sie an, wie die Daten (zum Beispiel elektronisch und nicht-elektronisch) gespeichert und aufbewahrt werden
2. Geben Sie an, wie die Systeme gespeichert und aufbewahrt werden.
3. Geben Sie den Zeitplan für die Datenaufbewahrung an.
4. Geben Sie an, wo die Daten/Systeme gespeichert und aufbewahrt werden.
5. Angabe des Verfahrens, mit dem sichergestellt wird, dass die Aufbewahrungsverfahren ordnungsgemäß funktionieren.
6. Angabe des Verfahrens zur Validierung der Speicherung von Daten/Medien.
7. Angabe des Verfahrens zur Einhaltung der Umwelt- und Nachhaltigkeitsprogramme des Unternehmens.

**Verfahren zur Daten-/Systemvernichtung**1. Angabe von Datenvernichtungsmetriken und Zeitrahmen
2. Angabe des Verfahrens für die Vernichtung von Daten/Systemen
3. Angabe des Verfahrens zur Validierung der Daten-/Medienvernichtung.
4. Geben Sie den Zeitplan für die Datenvernichtungsaktivitäten an.
5. Angabe des Verfahrens zur Einhaltung der Umwelt- und Nachhaltigkeitsprogramme des Unternehmens.

**Anträge auf Aufbewahrung und Vernichtung**1. Angabe des Verfahrens zur Bearbeitung von Anträgen auf Wiederherstellung und Vernichtung von Daten
 |
| **Politische Führung** **<Titel der Führungskraft>** ist der Verantwortliche für die Aufbewahrung und Vernichtung von Daten/Systemen für das Unternehmen. Die Lösung von Problemen bei der Unterstützung von Daten-/Systemaufbewahrungs- und -vernichtungsaktivitäten sollte mit der IT-Leitung und anderen nach Bedarf koordiniert werden.  |
| **Zuständigkeiten für die Policy*** Genehmigung der Richtlinie - Der **<Titel der Führungskraft>** ist für die Genehmigung dieser Richtlinie zuständig.
* Umsetzung der Richtlinie - Die <Name der Abteilung oder Person> ist verantwortlich für die Planung, Organisation und Umsetzung aller Aktivitäten, die diese Richtlinie erfüllen.
* Pflege und Aktualisierung der Richtlinien - Die <Name der Abteilung oder Person> ist für alle Aktivitäten im Zusammenhang mit der Pflege und Aktualisierung dieser Richtlinien verantwortlich.
* Einhaltung der Richtlinien - Die <Name der Abteilung oder Person> ist dafür verantwortlich, dass die einschlägigen Normen, Vorschriften und bewährten Verfahren für die Aufbewahrung und Vernichtung von Daten eingehalten werden.
* Richtlinie Einhaltung von Umweltmanagementprogrammen - Die <Name der Abteilung oder Person> ist dafür verantwortlich, die Einhaltung der Unternehmensrichtlinien und -programme für Umwelt- und Nachhaltigkeitsmanagement sicherzustellen.
* Überwachung, Überprüfung und Prüfung der Richtlinie - Die <Name der Abteilung oder Person> ist für die Überwachung und Überprüfung dieser Richtlinie und die Unterstützung bei geplanten Prüfungen - sowohl intern als auch extern durchgeführt - von Datenaufbewahrungs- und -vernichtungsaktivitäten verantwortlich.
* Verbesserung der Policy - Die <Name der Abteilung oder Person> ist für die Festlegung und Durchführung von Maßnahmen zur Verbesserung dieser Richtlinie verantwortlich.
 |
| **Management Review**<Name der Abteilung oder Person> wird diese Richtlinie zur Datenaufbewahrung und -vernichtung jährlich überprüfen und aktualisieren. Wenn sich im Geschäftsverlauf Änderungen an dieser Richtlinie ergeben, kann <Name der Abteilung oder Person> einen Änderungsmanagementprozess zur Aktualisierung dieser Richtlinie einleiten.  |
| **Durchsetzung der Richtlinie**Der **<Titel der Führungskraft>** wird diese Policy durchsetzen.  |
| **Sanktionen bei Nichteinhaltung der Vorschriften** In Situationen, in denen festgestellt wird, dass die Datenaufbewahrung und -vernichtung nicht mit dieser Richtlinie übereinstimmt, erstellt das für diese Tätigkeit zuständige Team der IT-Abteilung einen Bericht, in dem die Gründe für die Nichteinhaltung dargelegt werden, und legt ihn der IT-Leitung zur Lösung vor. Die Nichteinhaltung dieser Richtlinie zur Datenaufbewahrung und -vernichtung innerhalb der vorgegebenen Frist kann zu mündlichen Verwarnungen, Vermerken in den Personalakten, Kündigungen und anderen Maßnahmen führen, die als angemessen erachtet werden.  |
| **Standort der Richtlinie**Die Richtlinie wird unterzeichnet, in eine elektronische Datei eingescannt und an folgendem Ort im Netz veröffentlicht: <Speicherort der Richtlinie> |