



Der Landesbeauftragte
für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern



Ermittlung des Schutzbedarfs personenbezogener Daten für den Prozess der Datenträgervernichtung

Stand: 15. September 2014

Inhalt

1	Einleitung.....	3
1.1	Datenschutzrechtliche Anforderungen	3
1.2	DIN 66399	3
1.3	Zu dieser Orientierungshilfe	4
2	Schutzbedarf.....	4
3	Schutzklassen	5
4	Sicherheitsstufen.....	6
5	Zuordnung von Sicherheitsstufen zu Schutzklassen aus Datenschutzsicht	6
6	Aufbewahrungsfristen und Empfehlungen für Schutzklassen	8
6.1	Allgemeine Geschäftsunterlagen mit einer Aufbewahrungsdauer von sechs Jahren	9
6.2	Allgemeine Geschäftsunterlagen mit einer Aufbewahrungsdauer von zehn Jahren.....	10
6.3	Unterlagen des Personalbereichs.....	11
6.3.1	Allgemeine arbeitsrechtliche Regelungen.....	11
6.3.2	Besonderheiten im Beamtenrecht	13
6.3.3	Unterlagen zu Sicherheitsüberprüfungen	15
6.4	Arbeitsschutzunterlagen	16
6.5	Medizinische Unterlagen.....	17

1 Einleitung

1.1 Datenschutzrechtliche Anforderungen

Durch das Vernichten von Datenträgern, auf denen personenbezogene Daten gespeichert sind, können öffentliche und nicht-öffentliche Daten verarbeitende Stellen ihrer Verpflichtung zum Löschen dieser Daten nachkommen. Die Verpflichtung ist sowohl im Bundesdatenschutzgesetz (§ 20 Abs. 2 bzw. § 35 Abs. 2 BDSG) und den Landesdatenschutzgesetzen (z.B. § 13 Abs. 2 DSG M-V, § 19 Abs. 3 DSG NRW, Art. 12 Abs. 1 BayDSG) als auch in spezialgesetzlichen Regelungen (z.B. § 84 Abs. 2 SGB X) verankert. Personenbezogene Daten sind insbesondere dann zu löschen, wenn ihre Speicherung unzulässig oder ihre Kenntnis für die Aufgabenerfüllung bzw. zur Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.

Unter dem Begriff „Löschen“ wird dabei das Unkenntlichmachen gespeicherter personenbezogener Daten verstanden (§ 3 Abs. 4 Nr. 5 BDSG und entsprechende Landes- oder spezialgesetzliche Regelungen). Der Prozess muss dauerhaft und irreversibel dazu führen, dass die betreffenden Informationen nicht mehr aus den gespeicherten Daten gewonnen werden können. Dies gilt sowohl für die Daten verarbeitende Stelle selbst als auch für Dritte.

Das Vernichten von Datenträgern ist gleichzeitig eine technisch-organisatorische Maßnahme zur Gewährleistung der Datensicherheit, insbesondere zur Verhinderung der Kenntnisnahme personenbezogener Daten durch Unbefugte (Sicherung der Vertraulichkeit). Insofern sind die entsprechenden Regelungen des Bundesdatenschutzgesetzes (§ 9 BDSG sowie dessen Anlage), der Landesdatenschutzgesetze (z.B. § 21 DSG M-V, § 10 DSG NRW, Art. 7 BayDSG) sowie spezialgesetzliche Vorschriften (z.B. § 78a SGB X) zu beachten. Danach muss die Maßnahme dem Schutzbedarf der Daten angemessen sein. Ihre Umsetzung hat sich nach den im Einzelfall zu betrachtenden Risiken und dem Stand der Technik zu richten.

1.2 DIN 66399

Im Oktober 2012 wurde die neue DIN 66399 „Büro- und Datentechnik - Vernichten von Datenträgern“ veröffentlicht. Der zuständige DIN-Ausschuss hat damit einen Standard erarbeitet, der den heutigen Stand der Technik in der Datenträgervernichtung abbildet und die veraltete Norm DIN 32757 ablöst. Die DIN 66399 verfolgt einen ganzheitlichen Ansatz, benennt Grundlagen und Begriffe (Teil 1) sowie Anforderungen an Maschinen zur Vernichtung von Datenträgern (Teil 2) und beschreibt einen sicheren Prozess der Datenträgervernichtung (Teil 3).

Die DIN 66399 empfiehlt jeder verantwortlichen Daten verarbeitenden Stelle, alle im Geschäftsverkehr vorkommenden oder anfallenden Informationen (Daten) bzw. die sie speichernden Datenträger zunächst hinsichtlich des Schutzbedarfs zu klassifizieren und definiert hierfür drei Schutzklassen. Darüber hinaus beschreiben sieben Sicherheitsstufen Anforderungen an die Wirksamkeit der Vernichtung, d.h. die Höhe des Aufwands für Angreifer, vernichtete Datenträger bzw. darauf gespeicherte Daten wiederherzustellen und Information zur Kenntnis nehmen zu können.

Anschließend empfiehlt die DIN, Datenträger bestimmter Schutzklassen nur nach bestimmten Sicherheitsstufen zu vernichten und trägt so o.g. dem Prinzip der Angemessenheit Rechnung. Die

Norm bestimmt für diverse Materialklassen (wie Papier, Mikrofilm, magnetische Festplatten, optische Datenträger, Halbleiterspeicher) Grenzwerte für Teilchengrößen, die bei der Vernichtung eines Datenträgers eingehalten werden müssen, um die Wiederherstellung von Informationen aus dem nach der Vernichtung vorliegenden Restmaterial zu verhindern oder zumindest zu erschweren.

1.3 Zu dieser Orientierungshilfe

Mit dieser Orientierungshilfe werden die datenschutzrechtlichen Anforderungen zum Löschen und Vernichten von personenbezogenen Daten mit den in der DIN 66399 beschriebenen Empfehlungen zur Datenträgervernichtung in Verbindung gesetzt. Ziel ist es, für die Praxis konkrete Anregungen zu geben, welche Überlegungen bei der Vernichtung von Datenträgern mit Daten unterschiedlicher Sensitivität anzustellen sind. Im Mittelpunkt stehen hierbei Ausführungen zur Ermittlung des Schutzbedarfs von Daten und Datenträgern (Abschnitt 2), zur Zuordnung von Schutzklassen (Abschnitt 3) und zu den Eigenschaften der Sicherheitsstufen gem. DIN 66399 (Abschnitt 4) sowie zur Auswahl geeigneter und angemessener Sicherheitsstufen für die datenschutzgerechte Vernichtung von Datenträgern mit personenbezogenen Daten (Abschnitt 5). Weiterhin werden für eine Reihe konkreter Arten von Daten bzw. Unterlagen die vorgeschriebenen Aufbewahrungsfristen sowie Empfehlungen zur Einstufung in Schutzklassen gegeben (Abschnitt 6).

Anmerkung: Diese Orientierungshilfe beinhaltet mit Zustimmung der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) Teile des GDD-Ratgebers „Datenschutzgerechte Datenträgervernichtung - nach dem Stand der Technik“, 3. Aufl., 2014.

2 Schutzbedarf

Ziel der Ermittlung des Schutzbedarfs ist eine qualitative Aussage zum Bedarf an Schutz in Bezug auf definierte Schutzziele. Im Kontext des Löschens und Vernichtens geht es um den Schutz der Vertraulichkeit der Daten, d.h. die Verhinderung ihrer unbefugten Kenntnisnahme. In der Praxis bewährt hat sich eine mindestens dreistufige Schutzbedarfsskala (Schutzbedarf normal, hoch, sehr hoch). Diese wird auch vom Bundesamt für Sicherheit in der Informationstechnik zur Gewährleistung der Informationssicherheit in IT-Systemen empfohlen (s. BSI-Standard 100-2) und lässt sich direkt auf Schutzklassen der DIN 66399 abbilden (s. Abschnitt 3).

Bei der Schutzbedarfsermittlung ist folgendes zu berücksichtigen:

- Verantwortlich für die Bestimmung des Schutzbedarfs ist stets die Daten verarbeitende Stelle selbst. Sie muss eine Klassifikation der anfallenden Daten, insbesondere der personenbezogenen Daten, vornehmen. Die Einstufung von Daten in eine Schutzbedarfsklasse vererbt sich auf den Datenträger, auf dem die Daten gespeichert sind.
- Die Gesamtverantwortung der verantwortlichen Daten verarbeitenden Stelle besteht auch, wenn sie sich im Verlauf des Prozesses der Vernichtung von Datenträgern eines externen Dienstleisters im Rahmen einer Auftragsdatenverarbeitung gem. § 11 BDSG oder der entsprechenden landes- bzw. spezialgesetzlichen Vorschriften bedient.
- Bei der Bestimmung des Schutzbedarfs personenbezogener Daten ist der Grundrechtscharakter des Rechts auf informationelle Selbstbestimmung mit einzubeziehen. Rein wirtschaftliche Erwägungen zur Einstufung von Daten und Datenträgern sind beim Löschen und Vernichten personenbezogener Daten nicht zielführend. Es ist daher ein Schutzbedarf

anzustreben, dessen Aufwand für die Maßnahmen in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stellt (§ 9 Satz 2 BDSG).

- Zu beachten sind sowohl das Maximumprinzip als auch Kumulationseffekte: Ersteres besagt, dass der Schutzbedarf einer Menge von Daten (z.B. auf einem Datenträger) mindestens so hoch ist wie der höchste Schutzbedarf eines Einzeldatums. Letzteres kann dazu führen, dass für eine Anhäufung einer großen Anzahl von Daten als Gesamtheit ein höherer Schutzbedarf festgestellt wird als für einzelne Daten, da potentielle Schäden sich summieren können.
- Durch die Einteilung der Daten bzw. Datenträger entsprechend ihrem Schutzbedarf in Schutzklassen kann dem Grundsatz der Verhältnismäßigkeit aus § 9 BDSG bzw. den entsprechenden landes- oder spezialgesetzlichen Regelungen Rechnung getragen werden: Die Trennung der zu vernichtenden Datenträger nach ihrer Schutzklasse ermöglicht es, ausschließlich diejenigen Datenträger mit einer höheren Schutzklasse entsprechend den DIN-Vorgaben für den aufwändigeren Prozess und den höheren Grad an Vernichtung/Zerkleinerung zu behandeln, die dieses Schutzes auch wirklich bedürfen.

3 Schutzklassen

Ausgehend von den Ergebnissen der Schutzbedarfsermittlung sind zu löschende Daten bzw. zu vernichtende Datenträger adäquaten Schutzklassen zuzuordnen. Die Festlegung der Schutzklasse hat sowohl Auswirkung auf die anwendbaren Sicherheitsstufen als auch auf die Prozesse der Datenträgervernichtung.

Die DIN 66399 definiert drei Schutzklassen, die mit der in der Praxis bewährten dreistufigen Schutzbedarfsskala korrespondieren. Für die Einstufung personenbezogener Daten bzw. entsprechender Datenträger lassen sich die Schutzklassen wie folgt abgrenzen:

- Schutzklasse 1 (Normaler Schutzbedarf): Es handelt sich um personenbezogene Daten, bei deren unrechtmäßiger Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann. Schadensauswirkungen sind begrenzt und überschaubar und etwaig eingetretene Schäden für Betroffene relativ leicht durch eigene Aktivitäten zu heilen.
- Schutzklasse 2 (Hoher Schutzbedarf): Es handelt sich um personenbezogene Daten, bei deren unrechtmäßiger Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann. Die Schadensauswirkungen werden für Betroffene als beträchtlich eingeschätzt.
- Schutzklasse 3 (Sehr hoher Schutzbedarf): Es handelt sich um personenbezogene Daten, bei deren unrechtmäßiger Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist. Die Schadensauswirkungen nehmen ein unmittelbar existenziell bedrohliches, katastrophales Ausmaß für Betroffene an.

Neben der reinen Bewertung des Schutzbedarfs der Daten/Datenträger können ggf. weitere Aspekte in die Bestimmung der Schutzklassen einfließen. So können etwa Anforderungen des Geheimschutzes sowie Vorgaben zum Umgang mit Geschäfts-, Betriebs-, Berufs- oder Amtsgeheimnissen dazu führen, dass für die Datenträgervernichtung insgesamt eine höhere Schutzklasse festgelegt wird als diejenige, die sich aus der Schutzbedarfsermittlung unmittelbar ergibt. Gerade im Hinblick auf die Strafbarkeit der unbefugten Offenbarung von Privatgeheimnissen (§ 203 StGB) ist eine Organisation des Vernichtungsprozesses gemäß Einstufung entsprechender Daten und Datenträger in die Schutzklasse 3 angezeigt.

4 Sicherheitsstufen

Die DIN 66399 sieht sechs Materialklassen und für jede Materialklasse sieben Sicherheitsstufen vor. Mit einer höheren Sicherheitsstufe steigen sowohl der Grad an Vernichtung/Zerstörung der Datenträger als auch der Aufwand für die Vernichtung. Die Verwendung einer höheren Sicherheitsstufe wird notwendig, wenn ein höherer Schutzbedarf erkannt bzw. eine höhere Schutzklasse festgelegt wurde und somit ein höherer Schutz gegen die Wiederherstellung der Daten erforderlich ist.

Die Sicherheitsstufen sind in der DIN 66399 unabhängig von der Materialklasse wie folgt definiert:

Sicherheitsstufe	Geeignet für
1	Allgemeine Daten – Eine Reproduktion ist ohne besondere Hilfsmittel und Fachkenntnisse, jedoch nicht ohne besonderen Zeitaufwand möglich.
2	Interne Daten – Eine Reproduktion ist nur mit Hilfsmitteln und besonderem Aufwand möglich.
3	Sensible und vertrauliche Daten – Eine Reproduktion ist nur mit erheblichem Aufwand möglich (Hilfsmittel, Zeit, Personal).
4	Besonders sensible und vertrauliche Daten – Eine Reproduktion ist nur mit außergewöhnlich hohem Aufwand möglich (Hilfsmittel, Zeit, Personal).
5	Geheim zu haltende Daten – Eine Reproduktion ist nur unter Verwendung gewerbeüblicher Einrichtungen bzw. Sonderkonstruktionen sowie forensischen Methoden möglich.
6	Geheim zu haltende Daten, wenn außergewöhnlich hohe Sicherheitsvorkehrungen einzuhalten sind – Eine Reproduktion ist nach dem Stand der Technik nicht möglich.
7	Streng geheim zu haltende Daten, wenn höchste Sicherheitsvorkehrungen einzuhalten sind – Eine Reproduktion ist nach dem Stand von Wissenschaft und Technik nicht möglich.

5 Zuordnung von Sicherheitsstufen zu Schutzklassen aus Datenschutzsicht

Die DIN 66399 ermöglicht die Anwendung verschiedener Sicherheitsstufen der Vernichtung innerhalb einer Schutzklasse. Die Entscheidung für eine konkrete Stufe muss die verantwortliche Daten verarbeitende Stelle u.a. unter Berücksichtigung des Einzelfalls und nach Analyse evtl. bestehender Risiken treffen. Die folgende Tabelle gibt die Kombinationsmöglichkeiten der DIN-Norm wieder, wurde jedoch im Hinblick auf datenschutzrechtliche Anforderungen – also im Hinblick auf die Vernichtung von Datenträgern mit personenbezogenen Daten – angepasst.

Schutzklasse	Sicherheitsstufe				
	3	4	5	6	7
1	x*	x	x		
2		x	x	x	
3			x	x	x

Zur Erläuterung nachfolgend einige Anmerkungen:

- Die Sicherheitsstufen 1 und 2 wurden in der Tabelle weggelassen, da sie auch nach der DIN 66399 nicht für die Vernichtung von Datenträgern mit personenbezogenen Daten der Schutzklassen 1, 2 oder 3 anwendbar sind.
- *) Aus der Definition des § 3 Abs. 5 BDSG ergibt sich, dass Löschen das Unkenntlichmachen gespeicherter Daten ist. Die einschlägigen Kommentare¹ verdeutlichen, dass dieses Unkenntlichmachen ein **irreversibler Vorgang** sein muss. Die Reproduktion der Daten darf demnach allenfalls mit „unverhältnismäßig hohem Aufwand“ möglich sein. Da gemäß der Definition der Sicherheitsstufe 3 eine Reproduktion der Daten bereits „mit erheblichem Aufwand“ möglich sein soll, ist nicht auszuschließen, dass eine Vernichtung von Datenträgern mit personenbezogenen Daten beliebiger Schutzklasse nach der Sicherheitsstufe 3 die datenschutzrechtlichen Anforderungen zum Löschen von Daten nicht erfüllt. In diesen Fällen sind weitere technische und organisatorische Maßnahmen erforderlich, die in der DIN bereits beschrieben sind.
- Datenträger mit personenbezogenen Daten der Schutzklasse 2 sind grundsätzlich mindestens nach der Sicherheitsstufe 4 zu vernichten, für Datenträger mit personenbezogenen Daten der Schutzklasse 3 ist grundsätzlich mindestens Sicherheitsstufe 5 vorzusehen.
- Die gewählten Sicherheitsstufen zur Vernichtung von Datenträgern mit personenbezogenen Daten berücksichtigen neben datenschutzrechtlichen Anforderungen auch die rasche Entwicklung von Wissenschaft und Technik im Bereich der Reproduktion von Informationen selbst auf kleinsten Partikeln sowie bei der Computer Forensik.

In begründeten Fällen kann die verantwortliche Daten verarbeitende Stelle für die Vernichtung von Datenträgern mit personenbezogenen Daten auch von den Empfehlungen in der obigen Tabelle abweichen. Hierzu sind eine Betrachtung der sicherheitsrelevanten Rahmenbedingungen des Vernichtungsprozesses und eine Einschätzung des Gesamtrisikos für die Wiederherstellung von Daten erforderlich. Zwei Beispiele sollen dies verdeutlichen:

1. Mit Büroaktenvernichtern, insbesondere mit Cross-Cut-Geräten, die Papierunterlagen nach der Sicherheitsstufe 4 zerschneiden, werden die Anforderungen an ein datenschutzgerechtes Vernichten von papiernen Datenträgern der Schutzklasse 2 in der Regel nicht erfüllt, da sich aufgrund der Größe der Partikel die Informationen leicht wiederherstellen lassen. Die verantwortliche Daten verarbeitende Stelle sollte Cross-Cut-Geräte der Stufe P-5 für die

¹ Zitate, z.B.

Dammann in Simitis: BDSG § 3 Rn. 174 + 176:

Der Begriff des Unkenntlichmachens trifft auf jede Handlung zu, die irreversibel bewirkt, dass eine Information nicht länger aus gespeicherten Daten gewonnen werden kann.

Die verantwortliche Stelle muss zur Erfüllung des Lösungsgebotes einen Zustand herstellen, in dem sie die betreffende Information nicht mehr aus von ihr gespeicherten Daten gewinnen kann.

Schild in Wolff/Brink: BDSG § 3 Rn 86:

Das Unkenntlichmachen ist jede Handlung, die dazu führt, dass Daten nicht mehr zur Kenntnis genommen und Informationen nicht länger aus gespeicherten Daten gewonnen werden können. Durch den Begriff des Unkenntlichmachens wird klargestellt, dass nur eine Handlung, die nicht mehr reversibel ist, dazu führt, dass Daten nicht mehr verarbeitet oder genutzt werden können, da sie nicht mehr vorhanden sind.

BfD 33.3, 16. TB

Das BDSG und die meisten Landesdatenschutzgesetze definieren das Löschen als "Unkenntlichmachen der Daten". Unkenntlich gemacht sind Daten dann, wenn die Informationen nicht länger aus den ursprünglich gespeicherten Daten gewonnen werden können.

Vernichtung solcher Datenträger einsetzen, um das Risiko der Datenrekonstruktion zu minimieren.

2. Neben der maximalen Partikelgröße, die beim Vernichten erreicht wird, wird der Aufwand für die Rekonstruierbarkeit der Informationen auch durch weitere sicherheitstechnische Rahmenbedingungen des Vernichtungsprozesses beeinflusst. Hierzu zählen etwa Verwirbeln, Verpressen oder Verbrennen von Vernichtungsrückständen. Für die Materialklassen Papier und Film kann so durch Vermischen und Verpressen die Sicherheitsstufe 3 auf die Sicherheitsstufe 4 angehoben werden, wenn eine Mindestmenge von 100 kg an Datenträgern in einem Durchgang ununterbrochen in der Maschine oder Einrichtung vernichtet wird. Die verantwortliche Daten verarbeitende Stelle kann in diesem Fall die Sicherheitsstufe anheben, wenn aufgrund der sicherheitsrelevanten Rahmenbedingungen des Vernichtungsprozesses das Gesamtrisiko für die Wiederherstellung von Daten tolerierbar ist. Die ergänzenden sicherheitstechnischen Maßnahmen sind in diesen Fällen detailliert zu dokumentieren und sollten vertraglich festgeschrieben werden, wenn für die Aktenvernichtung ein Dienstleister beauftragt wird.

Abschließend wird darauf hingewiesen, dass die Tabelle keine Aussage zu Anforderungen für die Vernichtung von Datenträgern mit allgemein zugänglichen personenbezogenen Daten, deren Schutzbedarf unterhalb der Schutzklasse 1 liegt, trifft (z.B. für Telefonbücher, Adressbücher, Vorschlagslisten für öffentliche Wahlen).

6 Aufbewahrungsfristen und Empfehlungen für Schutzklassen

Die nachfolgenden Tabellen geben für ausgewählte Kategorien von Unterlagen einen Überblick über wesentliche gesetzliche Aufbewahrungsvorschriften, die einer Vernichtung von Daten bzw. Datenträgern entgegenstehen. Dabei wurden neben den Regelungen des Handels- und Steuerrechts vor allem Aufbewahrungsnormen im Personal- sowie im medizinischen Bereich berücksichtigt. Die Tabellen enthalten darüber hinaus Empfehlungen zur Festlegung von Schutzklassen gem. DIN 66399 im Vorfeld einer Vernichtung der Daten bzw. Datenträger.

Die Übersichten erheben keinen Anspruch auf Vollständigkeit. Insbesondere ist zu beachten, dass für bestimmte Arten von Daten bzw. Unterlagen (z.B. im Personalbereich für öffentliche Daten verarbeitende Stellen) ggf. spezifische landesrechtliche Regelungen für Aufbewahrungsfristen zu berücksichtigen sind.

Weiterhin ist darauf hinzuweisen, dass Stellen, die unter den Geltungsbereich der Archivgesetze des Bundes bzw. der Länder fallen, vor der Vernichtung von Unterlagen diese - falls keine anderen Regelungen greifen - den jeweils zuständigen Archiven anzubieten haben.

6.1 Allgemeine Geschäftsunterlagen mit einer Aufbewahrungsdauer von sechs Jahren

Art der Unterlage	Aufbewahrungsdauer	Rechtsgrundlage	Empfehlung Schutzklasse
Angebote	6 Jahre	§ 257 Abs. 1 Nr. 2, Abs. 4 HGB; § 147 Abs. 1 Nr. 2, Abs. 3 AO	1/2
Auftragsbestätigungen	6 Jahre	§ 257 Abs. 1 Nr. 2, Abs. 4 HGB; § 147 Abs. 1 Nr. 2, Abs. 3 AO	1/2
Bruttolohnlisten	6 Jahre	§ 257 Abs. 1 Nr. 2, Abs. 4 HGB; § 147 Abs. 1 Nr. 2, Abs. 3 AO	2
Bauakten	6 Jahre	§ 257 Abs. 1 Nr. 2, Abs. 4 HGB; § 147 Abs. 1 Nr. 2, Abs. 3 AO	1/2
Handels- oder Geschäftsbriefe - empfangene Schreiben ²	6 Jahre ³	§ 257 Abs. 1 Nr. 2, Abs. 4 HGB; § 147 Abs. 1 Nr. 2, Abs. 3 AO, § 6 KHBV	1/2
Handels- oder Geschäftsbriefe - Wiedergabe der abgesendeten Schreiben	6 Jahre ⁴	§ 257 Abs. 1 Nr. 3, Abs. 4 HGB; § 147 Abs. 1 Nr. 3, Abs. 3 AO, § 6 KHBV	1/2
Kommissionslisten	6 Jahre	§ 257 Abs. 1 Nr. 2, Abs. 4 HGB; § 147 Abs. 1 Nr. 2, Abs. 3 AO	1
Kreditunterlagen	6 Jahre	§ 257 Abs. 1 Nr. 2, Abs. 4 HGB; § 147 Abs. 1 Nr. 2, Abs. 3 AO	2
Sonstige steuerrelevante Unterlagen	6 Jahre	§ 257 Abs. 1 Nr. 2, Abs. 4 HGB; § 147 Abs. 1 Nr. 2, Abs. 3 AO	1/2/3
Versicherungspolicen	6 Jahre	§ 257 Abs. 1 Nr. 2, Abs. 4 HGB; § 147 Abs. 1 Nr. 2, Abs. 3 AO	2

² Als Geschäftsbrief (Handelsbrief) gilt jegliche Korrespondenz, die der Vorbereitung, der Durchführung oder der Rückgängigmachung eines Geschäftes dient.

³ Soweit es sich zugleich um einen Buchungsbeleg handelt, gilt die höhere Frist von zehn Jahren.

⁴ Vgl. vorhergehende Fußnote

6.2 Allgemeine Geschäftsunterlagen mit einer Aufbewahrungsdauer von zehn Jahren

Art der Unterlage	Aufbewahrungsdauer	Rechtsgrundlage	Empfehlung Schutzklasse
Abrechnungsunterlagen	10 Jahre	§ 257 Abs. 1 Nr. 1, Abs. 4 HGB; § 147 Abs. 1 Nr. 1, Abs. 3 AO	2
Änderungsnachweis der EDV-Buchführung	10 Jahre	§ 257 Abs. 1 Nr. 1, Abs. 4 HGB; § 147 Abs. 1 Nr. 1, Abs. 3 AO	2
Bankbelege	10 Jahre	§ 257 Abs. 1 Nr. 1, Abs. 4 HGB; § 147 Abs. 1 Nr. 1, Abs. 3 AO	2
Eingangsrechnungen	10 Jahre	§ 257 Abs. 1 Nr. 1, Abs. 4 HGB; § 147 Abs. 1 Nr. 1, Abs. 3 AO	1/2
Fehlerprotokoll bei EDV-Buchführung	10 Jahre	§ 257 Abs. 1 Nr. 1, Abs. 4 HGB; § 147 Abs. 1 Nr. 1, Abs. 3 AO	1
Gehaltslisten	10 Jahre	§ 257 Abs. 1 Nr. 1, Abs. 4 HGB; § 147 Abs. 1 Nr. 1, Abs. 3 AO	2
Handelsbücher	10 Jahre	§ 257 Abs. 1 Nr. 1, Abs. 4 HGB; § 147 Abs. 1 Nr. 1, Abs. 3 AO	1/2
Inventare (einschließlich Forderungsverzeichnisse)	10 Jahre	§ 257 Abs. 1 Nr. 1, Abs. 4 HGB; § 147 Abs. 1 Nr. 1, Abs. 3 AO, § 6 KHBV	1/2
Lieferscheine	10 Jahre	§ 257 Abs. 1 Nr. 1, Abs. 4 HGB; § 147 Abs. 1 Nr. 1, Abs. 3 AO	1/2
Verträge	10 Jahre	§ 147 Abs. 1 Nr. 5, Abs. 3 AO	2
Wareneingangs- und Zahlungsausgangsbücher	10 Jahre	§ 147 Abs. 1 Nr. 5, Abs. 3 AO	2
Zahlungsanweisungen	10 Jahre	§ 147 Abs. 1 Nr. 5, Abs. 3 AO	2

6.3 Unterlagen des Personalbereichs

6.3.1 Allgemeine arbeitsrechtliche Regelungen

Art der Unterlage	Aufbewahrungsdauer	Rechtsgrundlage	Empfehlung Schutzklasse
Arbeitnehmerüberlassung - Geschäftsunterlagen des Verleihers	3 Jahre	§ 7 Abs. 2 Arbeitnehmerüberlassungsgesetz (AÜG)	2
Arbeitszeitnachweise (allgemein)	2 Jahre	§ 16 Abs. 2 Arbeitszeitgesetz (ArbZG)	1
DEÜV-Bescheinigung über Datenübermittlungen	bis zum Ablauf des auf die letzte Prüfung folgenden Kalenderjahres ⁵	§ 25 Datenerfassungs- und -übermittlungsverordnung (DEÜV)	1/2
Doppelbesteuerungsbescheinigung	6 Jahre	§ 39b Abs. 6 i.V.m. § 41 Abs. 1 Einkommensteuergesetz (EStG)	2
Fahrtenschreiber-Schaublätter	1 Jahr	§ 57a Abs. 2 Straßenverkehrszulassungsordnung (StvZO)	2
Fahrtkostenerstattung	6 Jahre	§ 41 Abs. 1 EStG i.V.m. R 38 der Lohnsteuerrichtlinien	1/2
Heimarbeit-Entgeltbelege	3 Jahre	§ 13 Erste Verordnung zur Durchführung des Heimarbeitgesetzes (HAGDV 1)	2
Heimarbeit-Personenlisten	bis zum Ablauf des Kalenderjahres, das auf das Jahr der Anlegung folgt	§ 9 Abs. 3 HAGDV 1	1/2
Infektionsschutzgesetz-Gesundheitszeugnis und letzte Dokumentation der Belehrung	bis zum Ausscheiden des Arbeitnehmers	§ 43 Abs. 5 Infektionsschutzgesetz (IfSG)	2/3
Jugendarbeitsschutz-Unterlagen	2 Jahre	§ 50 Abs. 2 Jugendarbeitsschutzgesetz (JArbSchG)	1
Ladenschlussgesetz-Verzeichnisse und Unterlagen	1 Jahr	§ 22 Abs. 3 Nr. 2 Gesetz über den Ladenschluss (LadSchIG)	1

⁵ Prüfungen erfolgen mindestens alle 4 Jahre (§ 28p Abs. 1 S. 1 Sozialgesetzbuch - Viertes Buch).

Lohnkonto (Steuer)	6 Jahre	§ 41 Abs. 1 EStG	2
Lohnsteuerkarte	aktuelle Lohnsteuerkarte; Aushändigung bei Beendigung des Dienstverhältnisses; nach Ablauf des Kalenderjahres: Aushändigung bzw. Vernichtung ⁶	§§ 39b Abs. 1, 41b Abs. 1 S. 4 bis 6 EStG	2
Lohnsteuerpauschalierung	6 Jahre	§ 4 Abs. 2 Nr. 8 Lohnsteuer-Durchführungsverordnung (LStDV) i.V.m. § 41 Abs. 1 EStG	1
Lohnunterlagen ⁷ (Sozialversicherung)	bis zum Ablauf des auf die letzte Prüfung folgenden Kalenderjahres	§ 28f Abs. 1 S. 1 Sozialgesetzbuch - Viertes Buch (SGB IV)	2
Mutterschutz-Unterlagen	2 Jahre	§ 19 Abs. 2 Mutterschutzgesetz (MuSchG)	2

⁶ § 41b Abs. 1 S. 5 und 6 Einkommensteuergesetz: „Nach Ablauf des Kalenderjahres darf der Arbeitgeber die Lohnsteuerkarte nur aushändigen, wenn sie eine Lohnsteuerbescheinigung enthält und der Arbeitnehmer zur Einkommensteuer veranlagt wird. Dem Arbeitnehmer nicht ausgehändigte Lohnsteuerkarten ohne Lohnsteuerbescheinigungen kann der Arbeitgeber vernichten; nicht ausgehändigte Lohnsteuerkarten mit Lohnsteuerbescheinigungen hat er dem Betriebsstättenfinanzamt einzureichen.“

⁷ Der notwendige Inhalt der Lohnunterlagen ist in § 2 der Verordnung über die Durchführung der Beitragsüberwachung und die Auskunfts- und Vorlagepflichten geregelt.

6.3.2 Besonderheiten im Beamtenrecht

Für Bundesbeamte gilt das Bundesbeamtengesetz. Für Landesbeamte sind neben bundeseinheitlichen Regelungen (z.B. im Beamtenstatusgesetz) in jedem Fall die jeweils geltenden Landesbeamtengesetze sowie ggf. die zugehörigen Verordnungen und Verwaltungsvorschriften anzuwenden. Darüber hinaus können abweichende Regelungen für Aufbewahrungsfristen für einzelne öffentliche Stellen z.B. in Dienstvereinbarungen festgelegt sein.

Art der Unterlage	Aufbewahrungsdauer	Rechtsgrundlage (beispielhaft)	Empfehlung Schutzklasse
Personalakte	5 Jahre nach Abschluss der Akte	§ 113 Abs. 1 Bundesbeamtengesetz (BBG), Art. 110 Abs. 1 Bayerisches Beamtengesetz (BayBG), § 100 Abs.1 Landesbeamtengesetz Brandenburg (LGB Bbg), § 90 Abs. 1 Landesbeamtengesetz Meckl.-Vorp. (LGB M-V), § 94 Abs. 1 Niedersächsisches Beamtengesetz (NBG)	2
Unterlagen über Beihilfe, Heilfürsorge, Heilverfahren, Unterstützungen, Erkrankungen, Umzugs- und Reisekosten	falls zahlungsbegründend: 6 Jahre nach Ablauf des Jahres, in dem Vorgangsbearbeitung endete	§ 113 Abs. 2 BBG, § 90 Abs. 2 LGB M-V	2
	5 Jahre nach Ablauf des Jahres, in dem Vorgangsbearbeitung endete	§ 113 Abs. 2 BBG, Art. 110 Abs. 2 BayBG, § 100 Abs.2 LGB Bbg, § 94 Abs. 2 NBG	
Unterlagen über Erholungsurlaub	5 Jahre nach Ablauf des Jahres, in dem Vorgangsbearbeitung endete	Art. 110 Abs. 2 BayBG, § 100 Abs. 2 LGB Bbg	1
	3 Jahre nach Ablauf des Jahres, in dem Vorgangsbearbeitung endete	§ 113 Abs. 2 BBG, § 90 Abs. 2 LGB M-V, § 94 Abs. 2 NBG	

Versorgungsakten	5 Jahre nach Ablauf des Jahres der letzten Versorgungszahlung	§ 90 Abs. 3 LBG M-V, § 94 Abs. 3 NBG	2
	10 Jahre nach Ablauf des Jahres der letzten Versorgungszahlung	§ 113 Abs. 3 BBG, Art. 110 Abs. 3 BayBG, § 100 Abs. 3 LBG Bbg	
Unterlagen über Beschwerden, Behauptungen, Bewertungen, die für Beamten/Beamtin ungünstig sind oder nachteilig werden können	mindestens 2 Jahre (auf Antrag zu löschen)	§ 112 Abs. 2 BBG, Art. 109 Abs. 1 BayBG, § 99 Abs. 1 LBG Bbg, § 89 Abs. 1 LBG M-V, § 93 Abs. 1 NBG	2
	mindestens 3 Jahre (auf Antrag zu löschen)	§ 90 Abs. 1 LBG SH	
Mitteilungen in Strafsachen (soweit nicht Teil einer Disziplinarakte), Auskünfte aus dem Bundeszentralregister	2 Jahre (mit Zustimmung zu löschen)	§ 112 Abs. 2 BBG	2
	3 Jahre (mit Zustimmung zu löschen)	Art 109 Abs. 2 BayBG, § 99 Abs. 2 LBG Bbg, § 89 Abs. 2 LBG M-V, § 93 Abs. 2 NBG	
Arbeitszeitnachweise bei gleitender Arbeitszeit	mindestens 3 Monate, höchstens 13 Monate nach Monatsende der Erhebung	§ 7 Abs. 7 Arbeitszeitverordnung (AZV) für Bundesbeamte	1
	höchstens 6 Monate nach Ablauf des für die Aufgabenerfüllung festgelegten Zeitraums	§ 14 Abs. 7 AZVO Nordrhein-Westfalen	
	2 Jahre	§ 12 Abs. 7 ArbZVO Rheinland-Pfalz	

6.3.3 Unterlagen zu Sicherheitsüberprüfungen

Personen, die mit sicherheitsempfindlichen Tätigkeiten betraut werden sollen (z.B. mit Zugang zu als VS-Vertraulich, Geheim oder Streng Geheim eingestuften Verschlusssachen), sowie ggf. auch deren Ehegatten oder Lebenspartner müssen sich zuvor einer Sicherheitsprüfung unterziehen. Näheres regeln die Sicherheitsüberprüfungsgesetze (SÜG) des Bundes bzw. der Länder. Bezüglich der Vernichtung von Unterlagen bzw. der Löschung von Daten enthalten sie weitgehend ähnliche Vorschriften.

Art der Unterlage	Aufbewahrungsdauer	Rechtsgrundlage (beispielhaft)	Empfehlung Schutzklasse
Sicherheitsakte bei der zuständigen Stelle	höchstens 1 Jahr, falls Betroffener keine sicherheitsempfindliche Tätigkeit aufnimmt	§ 19 Abs. 2 SÜG Bund, § 21 Abs. 6 BlnSÜG, § 20 Abs. 2 SÜG NRW, § 23 Abs. 2 ThürSÜG, § 19 Abs. 2 SÜG M-V, §20 Abs. 2 LSÜG SH (länger bei Einwilligung)	2/3
	5 Jahre nach dem Ausscheiden aus sicherheitsempfindlicher Tätigkeit	§ 19 Abs. 2 SÜG Bund, § 21 Abs. 6 BlnSÜG, § 20 Abs. 2 SÜG NRW, §23 Abs. 2 ThürSÜG, § 19 Abs. 2 SÜG M-V, §20 Abs. 2 LSÜG SH (länger bei Einwilligung)	
Sicherheitsüberprüfungsakte bei der mitwirkenden Stelle (i.d.R. die zuständige Verfassungsschutzbehörde): für einfache Sicherheitsüberprüfungen (Ü1)	5 Jahre nach Ausscheiden aus der sicherheitsempfindlichen Tätigkeit	§ 22 Abs. 2 SÜG Bund, § 21 Abs. 6 BlnSÜG, §23 Abs. 2 SÜG NRW, § 23 Abs. 2 ThürSÜG	2
	Fristen wie bei der zuständigen Stelle	§ 22 Abs. 2 SÜG M-V, §20 Abs. 3 Nr. 1 LSÜG SH	
Sicherheitsüberprüfungsakte bei der mitwirkenden Stelle (i.d.R. die zuständige Verfassungsschutzbehörde): für erweiterte Sicherheitsüberprüfungen (Ü2, Ü3)	10 Jahre nach Ausscheiden aus der sicherheitsempfindlichen Tätigkeit	§ 23 Abs. 2 ThürSÜG	2/3
	10 Jahre nach Ablauf der Aufbewahrungsfristen bei zuständiger Stelle	§ 22 Abs. 2 SÜG Bund, § 21 Abs. 6 BlnSÜG, §23 Abs. 2 SÜG NRW, § 22 Abs. 2 SÜG M-V	
	nach Ablauf von 10 Jahren	§20 Abs. 3 Nr. 2 LSÜG SH	

6.4 Arbeitsschutzunterlagen

Art der Unterlage	Aufbewahrungsdauer	Rechtsgrundlage	Empfehlung Schutzklasse
Unterweisungsaufzeichnungen für bestimmte Beschäftigte im Sperrbereich und außerhalb des Kontrollbereichs	5 Jahre	§ 36 Abs. 4 RöV, § 38 Abs. 4 StrlSchV	2
Unterweisungsaufzeichnungen für andere Personen im Kontrollbereich	1 Jahr	§ 36 Abs. 4 RöV, § 38 Abs. 4 StrlSchV	2
Kartei über Vorsorgeuntersuchungen, Ärztliche Bescheinigungen	Bis zum Ausscheiden des Mitarbeiters	z.B. § 11 Abs. 4 Unfallverhütungsvorschrift (UVV), BGV A4 Arbeitsmedizinische Vorsorge	2
Chemikalien (Prüfpläne, vorgenommene Inspektionen, Einweisungen, u.a.m.)	15 Jahre	Anhang 1 zu § 19a Abs. 1 Chemikaliengesetz (ChemG)	1
Gefährliche Arbeitsstoffe	30 Jahre ⁸	früher: § 18 Gefahrstoffverordnung (GefStoffV)	1
Kartei über arbeitsmedizinische Vorsorgeuntersuchungen im Gefahrstoffbereich	Bis Beendigung des Arbeitsverhältnisses (danach Aufbewahrung eines Auszuges entsprechend Personalunterlagen)	§ 14 Abs. 4, § 15 Abs. 5, 6 GefStoffV	3

⁸ Empfehlung aus Beweissicherungsgründen, da Aufbewahrungsfrist bei Novellierung 2005 abgeschafft wurde

6.5 Medizinische Unterlagen

Art der Unterlage	Aufbewahrungsdauer	Rechtsgrundlage	Empfehlung Schutzklasse
Behandlungsunterlagen (Anamnese, Aufnahme- und Aufklärungsbögen, Befunde, Medikation, Pflegeanordnungen, Arztbriefe, EKG, EEG, CTG, histologische Berichte, OP-Berichte usw.)	10 Jahre ⁹	§ 10 Abs. 3 MBO (Stand 2011), § 630f BGB	2/3
Aufzeichnungen über Untersuchungen mit radioaktiven oder ionisierenden Strahlen, Röntgenbilder, szintigrafische Aufnahmen u. ä.	10 Jahre	§ 85 Abs. 3 StrlSchV, § 28 Abs. 3 RöV	2/3
Aufzeichnungen über Behandlungen mit radioaktiven oder ionisierenden Strahlen	30 Jahre	§ 85 Abs. 3 StrlSchV, § 28 Abs. 3 RöV	2/3
Aufzeichnungen im Rahmen der klinischen Forschung im Zusammenhang mit Röntgen und Bestrahlung	30 Jahre	§ 87 Abs. 5 StrlSchV, § 28c Abs. 5 RöV	2
Unterlagen über Verbleib und Bestand von Betäubungsmitteln	3 Jahre von der letzten Eintragung an gerechnet	§ 13 Abs. 3 Betäubungsmittelverschreibungsverordnung (BtMVV)	2
Aufzeichnungen über Herstellung, Prüfung, Lagerung, Einfuhr, Rückruf usw. von Arzneimitteln	mindestens 1 Jahr nach Ablauf des Verfallsdatums, jedoch nicht weniger als 5 Jahre	§ 22 Abs. 1 Apothekenbetriebsordnung (ApBetrO)	2
Aufzeichnungen über Rückverfolgung zum Unterzeichner bei Verschreibung in elektr. Form	3 Jahre nach der letzten Eintragung	§ 22 Abs. 1b ApBetrO	3
Aufzeichnungen zur Rückverfolgung hinsichtlich Erwerbs und Abgabe von Blutzubereitungen, Sera, Plasmaproteinen usw.	mindestens 30 Jahre	§ 22 Abs. 4 ApBetrO	2/3
Aufzeichnungen über Blutspendenentnahme	mindestens 15 Jahre	§ 11 Abs. 1 Transfusionsgesetz (TFG)	2/3

⁹ Bei besonderen Risiken, schutzwürdigen Belangen Betroffener oder aus speziellen Beweissicherungsgründen können Einzelakten ggf. auch länger als 10 Jahre aufzubewahren sein. Zu beachten sind darüber hinaus ggf. existierende landes- oder spezialgesetzliche Regelungen z.B. § 37 Abs. 1 Landeskrankenhausgesetz Mecklenburg-Vorpommern (Sperrung der Daten nach Abschluss der Behandlung, Aufbewahrung i. d. R. 10 Jahre, jedoch höchstens 30 Jahre) oder § 43 Abs. 6 Psychischkrankengesetz Mecklenburg-Vorpommern (für Daten psychisch Kranker höchstens 2 Jahre nach Ende der Unterbringung, wenn nicht in Krankenakten enthalten).

Immunisierungsprotokolle und Aufzeichnungen im Zusammenhang mit der Vorbehandlung zur Blutstammzellseparation	mindestens 20 Jahre	§ 11 Abs. 1 TFG	3
Angaben zur Spenderdokumentation, die für die Rückverfolgung benötigt wird	mindestens 30 Jahre	§ 11 Abs. 1 TFG	3
Aufzeichnungen über die Anwendung von Blutprodukten	mindestens 30 Jahre	§ 14 Abs. 3 TFG	1/2
Aufzeichnungen im Zusammenhang mit der Anwendung von Blutprodukten (Aufklärung, Einwilligungserklärungen usw.)	mindestens 15 Jahre	§ 14 Abs. 3 TFG	3
Transplantationsunterlagen	mindestens 30 Jahre	§ 15 TPG	3
Berufsgenossenschaftliche Verletzungsverfahren	mindestens 15 Jahre	Anforderungen nach § 34 SGB VII	3