*Bitte beachten Sie, dass es sich bei den hier veröffentlichten Mustertexten lediglich um allgemeine und beispielhafte Formulierungen handelt, die auf den jeweiligen Einzelfall noch individuell anzupassen sind. Wir können keine Haftung dafür übernehmen, dass der jeweilige Mustertext für den jeweils individuellen Sachverhalt uneingeschränkt verwendbar ist. Die unkritische Übernahme der Formulierungen erfolgt auf eigenes Risiko und ersetzt keineswegs die individuelle rechtliche Beratung.*

# Löschkonzept

Inhalt

1. Vorbemerkung
2. Datenspeicherung und Löschpflicht
3. Verantwortung für die Verarbeitung und Löschung
4. Rechtsgrundlagen für die Verarbeitung und Speicherung von personenbezogenen Daten
5. Sammlung und Lagerung des Vernichtungsgutes
6. Verantwortung für und Anordnung der Löschung/Vernichtung von personenbezogenen Daten
7. Durchführung der Löschung bzw. Vernichtung
8. Protokollierung und Dokumentation der Löschung/Vernichtung
9. Löschtabelle
10. Prozessbeschreibung

1. Vorbemerkung

Grundsatz

Je nach dem Zweck der Verarbeitung und der Rechtsnatur der Daten bestehen unterschiedliche Anforderungen an die Dauer der Aufbewahrung bzw. Speicherung und ggf. gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen und hinsichtlich der Löschung unterschiedliche Sicherheits- und Vertraulichkeitsanforderungen. Für die rechtlich relevanten und die sonstigen für die betrieblichen Zwecke erforderlichen Daten müssen deshalb die Aufbewahrungsfirsten und Lösch- bzw. Vernichtungsverfahren festgelegt werden.

Soweit Kopien und Sekundärdatenbestände oder aus verarbeitungstechnischen Gründen temporäre Dateien erzeugt worden sind, z. B. wenn von einem Datenbestand Kopien oder aus einem Datenbestand Auszüge erstellt und/oder auf einem mobilen Datenträger, auf einem Notebook oder auf einem sonstigen mobilen Gerät oder in Cloud-Strukturen zur mobilen Nutzung kopiert und vorgehalten werden, ist auch für diese Daten die Rechtsnatur festzulegen und die Verwaltung dieser Daten einschließlich einer Löschung zu regeln. Für den Fall der Rücksicherung von Daten aus Back-up-Beständen sind geeignete Überwachungsmaßnahmen einzurichten, um eine Rücksicherung von bereits gelöschten Daten in den Produktivbestand zu verhindern.

Protokolldaten

Auch Protokolldaten (Protokolldateien, Logfiles und Logdateien) zur Systemüberwachung und zur Dokumentation der Systemverwaltung durch die Administratoren sowie der Systembenutzung durch die Anwender sind regelmäßig personenbezogene Daten und unterliegen sowohl einer Zweckbindung als auch Sicherheitsanforderungen und Aufbewahrungs- bzw. Löschvorschriften. Die Protokolldateien dienen der Kontrolle und Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsverfahren und des ordnungsgemäßen IT-Betriebs. Die Aufbewahrungsfrist für diese Dateien muss ebenfalls nach den bestehenden Sicherheitsanforderungen an den IT-Betrieb geregelt werden. Eine Aufbewahrungsfrist von sechs bis zwölf Monaten wird als angemessen betrachtet, daneben können sich aber weitere Anforderungen ergeben, die eventuell eine längere Speicherdauer rechtfertigen können.

Löschung

Die Regelung der Aufbewahrung und der Löschverfahren sowie eine regelmäßige Löschung/Vernichtung der Daten nach Ablauf der Aufbewahrungsfristen leisten einen wesentlichen Beitrag zur Reduzierung von Risiken im Zusammenhang mit der Verarbeitung von personenbezogenen Daten. Die Überwachung der Speicherung der Daten und deren regelmäßige Löschung ist deshalb eine Regelaufgabe und vom Informationsverantwortlichen regelmäßig wahrzunehmen.

Für die Löschung von Magnetdatenträgern steht die Löschung über Löschkommandos, durch Formatieren, Überschreiben oder spezielle Löschprogramme zur Verfügung. Diese einfachen Löschbefehle reichen für eine sichere Löschung der Datenträger nicht aus. Eine Löschung mit einem Löschkommando führt nur zu einer Löschung der Dateieinträge im Inhaltsverzeichnis des Datenträgers. Die Dateiinformationen bleiben erhalten und können wieder rekonstruiert werden. Löschkommandos dürfen deshalb nur für die interne Verwaltung des Speicherplatzes eingesetzt werden, aber nicht, wenn eine endgültige Löschung der Daten unter Gesichtspunkten des Schutzes der Vertraulichkeit der Daten gefordert ist.

Die Zuverlässigkeit einer Löschung durch Formatieren ist von dem zugrunde liegenden Betriebssystem abhängig. Auch bei formatierten Datenträgern ist häufig eine weitgehende Rekonstruktion der Daten möglich. Zum Einsatz der Formatierung zu Löschzwecken gelten deshalb die gleichen Grundsätze wie für Löschkommandos.

Bei einer Löschung durch Überschreiben werden die Datenträger mit einem bestimmten Muster überschrieben. Es sollen aber kein gleichförmiges Muster wie „000“ oder „111“ verwendet werden. Es sollen mindestens zwei komplementäre Muster (z. B. C1 (hexadezimal 11000001) und 3E (hexadezimal 00111110)) benutzt werden, damit jedes Bit einmal geändert wird. Dieses Löschverfahren ist bei einer mehrfachen Wiederholung für mittlere Sicherheitsanforderungen ausreichend.

Die zuverlässigste Löschung bieten spezielle Löschprogramme, die den Datenträger mehrfach mit einer aufeinander abgestimmten Zeichenfolge überschreiben und so eine Rekonstruktion der Daten unmöglich machen. Für die Löschung von vertraulichen personenbezogenen Daten sind sichere Löschprogramme einzusetzen.

Scheidet aufgrund einer fehlenden Zugriffsmöglichkeit, z. B. durch einen Defekt des Datenträgers, oder der Art des Datenträgers eine Löschung nach den o. g. Verfahren aus, bleiben nur eine mechanische oder thermische Zerstörung.

CD-ROMs, DVDs, optische Platten, Magnetbänder etc. werden durch Schreddern vernichtet.

Werden Geräte, z. B. Server, Multifunktionsgeräte etc., die über einen eigenen Datenträger verfügen, ausgesondert oder im Rahmen eines Leasingvertrags zurückgegeben, werden die enthaltenen Datenträger vor der Rückgabe sicher gelöscht. Die Löschung ist zu protokollieren.

2. Datenspeicherung und Löschpflicht

Personenbezogene Daten dürfen nur so lange gespeichert und verarbeitet werden, wie sie für festgelegte Zwecke des Unternehmens erforderlich sind und dafür eine Rechtsgrundlage vorhanden ist. Wenn der Verarbeitungszweck entfallen ist oder die Daten für den jeweiligen Verarbeitungszweck nicht mehr erforderlich sind oder für die Verarbeitung keine Rechtsgrundlage mehr existiert, müssen die Daten grundsätzlich gelöscht bzw. die Datenträger vernichtet werden.

Personenbezogene Daten sind zu löschen

1. nach Wegfall der Rechtsgrundlage der Verarbeitung
2. nach Ablauf von Aufbewahrungsfristen
3. nach Wegfall der Erforderlichkeit der Daten für die Zweckerreichung
4. bei unrechtmäßiger Speicherung und Verarbeitung
5. nach Rücknahme einer Einwilligung (Art. 7 Abs. 3 DSGVO)
6. nach einem berechtigten Widerspruch gegen eine weitere Verarbeitung auf der Grundlage eines berechtigten Interesses gem. Art. 6 Abs. 1 lit. f DSGVO (Art. 21 Abs. 1 DSGVO)
7. nach einem Widerspruch gegen eine Nutzung der Daten für Zwecke der Werbung einschließlich Werbeprofiling

Über den Zeitraum der Erforderlichkeit der Daten für den jeweiligen Unternehmenszweck hinaus können gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen oder Verjährungsfristen bestehen. Diese Fristen müssen bei der Bemessung der Dauer der Speicherung der Daten berücksichtigt werden. Daneben können in Einzelfällen besondere Umstände vorliegen, die trotz Wegfall der grundsätzlichen Erforderlichkeit der Daten eine weitere Speicherung verlangen.

Keine Löschpflicht besteht gem. § 35 BDSG für nicht automatisiert verarbeitete Daten, z. B. für Papierakten oder Mikrofiches, Mikrofilm-Jackets oder COM-Fiches, wenn die Löschung nur mit einem unverhältnismäßig hohen Aufwand möglich wäre und das Löschinteresse der betroffenen Personen als gering anzusehen ist. Dies gilt

Das gesamte, frei veränderbare Dokument erhalten Sie
im Online-Fachportal **zum Sofort-Download**.
Füllen Sie dazu jetzt das Formular auf der Webseite
aus ([am Seitenende](https://fachportal-datenschutzbeauftragter.de/testen.php#testen)).

Bereits in der kostenlosen 4-Wochen-Testphase
können Sie es **vollständig einsehen**
und prüfen.

Um es uneingeschränkt zu nutzen,
**wechseln** Sie **einfach** in einen
kostenpflichtigen Account.
[Hier Test-Zugang einrichten](https://fachportal-datenschutzbeauftragter.de/testen.php#testen)