**Löschkonzept mit Muster und Reaktionsplan[[1]](#footnote-1)**

## Löschkonzept

Das Löschkonzept setzt die gesetzliche Pflicht aus der DSGVO um, dass Daten mit Personenbezug nach Erreichung des Zwecks zu löschen sind (vgl. Ziffer 13.2 in den „Hinweisen für den Umgang mit personenbezogenen Daten durch Steuerberater und steuerberatende Berufsausübungsgesellschaften“).

Daneben kann auch durch die Geltendmachung eines Betroffenenrechts ein Löschvorgang initiiert werden.

Daher empfiehlt es sich für beide Szenarien ein Löschkonzept zu erstellen.

Standardisierte (*Regel*)löschung

## Schritt 1: Verantwortlichkeiten festlegen

Die Gesamtverantwortung für ein Löschkonzept und deren Durchführung trägt die Kanzleileitung.

Für die jeweilige Umsetzung können andere Personen beauftragt werden. Gleiches gilt für die Kontroll- bzw. Prüftätigkeiten hinsichtlich der Umsetzung.

## Schritt 2: Datenarten clustern

Daten können zusammengefasst werden, um für vergleichbare Datenarten standardisierte Vorgänge zu definieren. Hierzu ist zunächst erforderlich zu erfassen, welche Daten in welchen IT-Systemen vorhanden sind. Dies kann über das Verzeichnis der Verarbeitungstätigkeit erfolgen (Art. 30 Abs. 1 DSGVO, vgl. auch Ziffer 10.3.4 der „Hinweise für den Umgang mit personenbezogenen Daten durch Steuerberater und steuerberatende Berufsausübungsgesellschaften“.

Datenarten könnten z. B. Adressdaten, Lohndaten oder Zahlungsdaten sein.

Besonderheit Protokolldaten – Daten mit besonderer Zweckbindung

Auch technische Daten mit Personenbezug (z. B. Protokolldaten über Systeman- und -abmeldungen) unterliegen einer strengen Zweckbindung. Für diese Daten ist ebenfalls ein Löschkonzept erforderlich.

## Schritt 3: Löschfristen bestimmen

Für vergleichbare Daten können gleiche Löschfristen festgelegt werden. Diese Löschfristen umfassen den Zeitraum gesetzlicher Aufbewahrungsfristen (z. B. gem. HGB oder AO) und die innerbetriebliche Bearbeitungszeiten bzw. die technische Umsetzungszeiten.

[Ein Beispiel ist unter 13.1 der „Hinweise für den Umgang mit personenbezogenen Daten durch Steuerberater und steuerberatende Berufsausübungsgesellschaften“ aufgezeigt.]

## Schritt 4: Löschregeln erstellen

Nachdem für jede Datenart Löschfristen definiert sind, sind Vorgaben und Regeln
(Löschregeln) für die konkrete Umsetzung der Löschung jeder Datenart zu entwickeln, bei denen technische Abhängigkeiten der betroffenen Systeme berücksichtigt werden können.

Diese Löschregeln bestehen aus:

* Datenobjekte (z. B. Dateien, Dokumente, Datensätze oder Attribute)
* Datenart(en)
* Aufbewahrungsfrist mit Startzeitpunkt für den Fristbeginn
* Zeitraum nach Ablauf der Frist, in dem die Löschung zu erfolgen hat

Empfehlenswert ist ein Hinweis auf die Technik des Löschvorgangs sowie die Festlegung, wer für den Prozess verantwortlich ist und wie eine angemessene Dokumentation des Löschvorgangs erfolgt. Es kann erforderlich sein, für jedes Datenobjekt oder gar jede Datenart eigene Löschregeln zu definieren.

Dabei muss ein Startereignis für den Zeitpunkt des Beginns der Löschfrist einer Datenart festgelegt werden. Das Startereignis kann dann z. B. die Beendigung des Mandats, wenn dann die gesetzliche Aufbewahrungsfrist beginnt oder der Zeitpunkt einer Protokollierung für den Zeitraum einer Nachweispflicht sein.

Zusätzlich können noch erforderliche Karenzzeiten für die technische und/oder organisatorische Umsetzung berücksichtigt werden, beispielsweise (abhängig von der Sensibilität der Daten) noch bis zu 6 Monaten.

## Schritt 5: Löschregeln technisch umsetzen

Nach der Definition von Löschregeln (wann welche Datenarten zu löschen sind) muss eine technische Löschung für alle relevanten IT-Systeme und Anwendungen festgelegt werden.

Sofern für Datenarten die Aufbewahrungszeiträume zeitgleich enden, ist eine zentrale Löschroutine empfehlenswert. Werden Informationen dezentral verarbeitet, sind dezentrale Vorgaben zu erstellen. Bei individueller Ablage (z. B. bei E-Mails durch Mitarbeiter) muss für eine individuelle Löschung nach Ablauf des Aufbewahrungszeitraums gesorgt werden.

Für die technische Umsetzung der Löschung bei Papierunterlagen und Datenträgern sollten die Vorgaben der DIN 66399/ISO IEC 21964 (Vernichtung von Datenträgern) berücksichtigt werden. Nach ihr werden die Informationen nach Schutzklassen und Sicherheitsstufen geclustert und Festlegungen zu einer angemessenen Entsorgung definiert. Berufsrechtlich geschützte Informationen sind z. B. der Schutzklasse 3 und mindestens Sicherheitsstufe 4 zugeordnet.

Mit der Löschung (Entsorgung) von digitalen Datenträgern oder von Papierunterlagen können auch Dienstleister beauftragt werden. Diese Beauftragung stellt im Regelfall eine Auftragsverarbeitung gemäß Art. 28 DSGVO dar (vgl. Ziffer 7.1 der „Hinweise für den Umgang mit personenbezogenen Daten durch Steuerberater und steuerberatende Berufsausübungsgesellschaften“.)

## Schritt 6: Nachweisfähigkeit gewährleisten

Über die Löschvorgänge sind geeignete Protokolle zu führen. Dabei ist zu unterscheiden, ob die Löschung aufgrund einer Routinemaßnahme erfolgt oder auf Verlangen einer betroffenen Person erfolgt ist. In die Dokumentation gehören in der Regel folgende Punkte:

Routineprozess (Beispiel an Lohndaten eines Mandanten):

|  |  |
| --- | --- |
| **Prozessschritte:** | **Beispiel** |
| * Prozess, aus dem heraus Daten gelöscht werden
 | Lohnbuchhaltung |
| * Herkunft der Daten (zentrale Ablage, individuelle Ablage, Archiv usw.)
 | Mandant Muster GmbHMandanten Nr. 1234567 Alternativ: alle Mandanten mit Mandatierung zur LohnbuchhaltungVeranlagungszeitraum 2005🞎 Rechenzentrum 🞎 On-Premise |
| * Betroffenengruppen
 | Beschäftigte/Mandanten |
| * Datenart
 | Lohnbuchhaltungsdaten/Zahlungsdaten |
| * Zeitpunkt der Löschung
 | Tag/Monat/Jahr |
| * Löschung bei /durch Dienstleistern (Auftragsverarbeitung)
 | 🞎 Durch Vertrag geregelt🞎 Weisung erteilt am: ………… |

**Zusätzlich** bei Löschung aufgrund der Geltendmachung eines Rechtes durch die betroffene Person:

* Prüfung der Identität der betroffenen Person
* Dokumentation der Antragstellung
* Dokumentation über Berechtigung des Löschanspruchs
* ggf. Verweigerung der Löschung

(Beispiel an Lohndaten der Kanzlei)[[2]](#footnote-2)

|  |  |
| --- | --- |
| **Prozessschritte:** | **Beispiel** |
| * Prüfung der Identität der betroffenen Person
 | 🞎 persönlich bekannt 🞎 Identitätsfeststellung auf andere Weise: 🞎 Verwendung bestehender Kontaktdaten🞎 Einsichtnahme Personalausweis |
| * Dokumentation der Antragstellung
 | Antrag eingegangen am: ………………… |
| * Dokumentation über Berechtigung des Löschanspruchs
 | Löschanspruch geprüft am…………………Durch …………………………**Ergebnis**: Löschanspruch bejaht, Grund: 🞎 keine Rechtsgrundlage zur Verarbeitung, Art. 17 Abs. 3 DS-GVO: 🞎 sonstiges:…………………………………………… Löschanspruch abgelehnt, Grund: 🞎 bestehende Verpflichtung, zB Art. 17 Abs. 3 lit. b DSGVO iVm § 147 AO, 257 HGB🞎 sonstiges:……………………………………………  |
| * ggf. Verweigerung der Löschung
 | Information an betroffene Person mit Angabe Grund |
| * Prozess, aus dem heraus Daten gelöscht werden
 | Lohnbuchhaltung |
| * Herkunft der Daten (zentrale Ablage, individuelle Ablage, Archiv usw.)
 | Kanzlei MustermannVeranlagungszeitraum 2005🞎 Rechenzentrum 🞎 On-Premise |
| * Betroffenengruppen
 | Beschäftigte/Mandanten |
| * Datenart
 | Lohnbuchhaltungsdaten/Zahlungsdaten |
| * Zeitpunkt der Löschung
 | Tag/Monat/Jahr |
| * Löschung bei/durch Dienstleistern (Auftragsverarbeitung)
 | 🞎 Durch Vertrag geregelt🞎 Weisung erteilt am: ………… |

## Schritt 7: regelmäßige Überprüfungen

Im Rahmen eines PDCA-Zyklus (Plan-Do Check-Act) sind regelmäßig Überprüfungen durchzuführen, ob die festgelegten Maßnahmen des Löschkonzeptes eingehalten werden. Diese Überprüfungen können sowohl durch andere interne Bereiche aber auch durch den DSB, die eigene Revision oder externe Auditoren erfolgen. Die Ergebnisse dieser Audits sind zu dokumentieren.

## Schritt 8: Dienstleister nicht vergessen!

Vom Löschkonzept umfasst sein müssen auch Daten, die durch Dienstleister im Auftrag gemäß Art. 28 DSGVO verarbeitet werden. Diese sind dann als Auftragsverarbeiter im Vertrag zu verpflichten wie mit den Daten nach Zweckerfüllung umzugehen ist, z. B. also Rückgabe oder Löschung. Dabei können dann auch die Vorgaben der DIN 66399 vereinbart werden.

**Anlagen:**

Anlage 1: Reaktionsplan bei Löschanfragen betroffener Personen

Anlage 2: Muster Löschkonzept

Anlage 1

**Reaktionsplan bei Löschanfragen**

Betroffene Personen haben gem. Art 17 DSGVO das Recht, mit formlosem Antrag und ohne Begründung von der Kanzlei die Löschung der dort gespeicherten personenbezogenen Daten zu verlangen, sofern keine vorrangigen Zwecke wie z. B. gesetzliche Aufbewahrungsfristen und Beweissicherungsinteressen des Verantwortlichen vorliegen.

Mit einer entsprechenden Dokumentation ist es der Kanzleileitung möglich, den rechtskonformen Umgang mit diesen Löschbegehren nachzuweisen.

Zuständig für die Bearbeitung von Auskunftsersuchen in der Kanzlei ist

[*Name Mitarbeiter/in einfügen*]

1. **Ist die Identität des Anfragenden feststellbar, wenn ja, anhand welcher Kriterien?**

|  |
| --- |
| *Name:**Geburtsdatum:**Anschrift:**Ggf. Mandantennummer:** *Legitimation anhand gültiger Ausweispapiere: ………………………(vermerken, welches Dokument vorgelegt wurde, eine Kopie zur Aufbewahrung ist nicht erforderlich)*
* *Persönlich bekannt, bestätigt durch: ………………………..*
 |

1. **Wie erfolgte die Antragstellung?**

|  |
| --- |
| * per E-Mail
* E-Mailadresse ist die intern bereits hinterlegte
* E-Mailadresse ist bisher noch nicht bekannt
* Fax
* Telefon/Briefpost gestellt
* Weiteres:
* Datum der Anfrage:
* Uhrzeit der Anfrage:
 |

1. **Welche konkreten Daten sollen gelöscht werden?**

|  |
| --- |
|  |

1. **Der Löschantrag ist nach Art. 17 Abs. 1 DSGVO aus dem folgenden Grund unverzüglich nachzukommen:**

|  |
| --- |
| * Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig
* Die betroffene Person widerruft ihre Einwilligung und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung
* Die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor
* Die personenbezogenen Daten wurden unrechtmäßig verarbeitet
* Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich
* Die personenbezogenen Daten eines Kindes in Bezug auf angebotene Dienste der Informationsgesellschaft, d. d. Internetangebote wie Medien, Webshops oder Online-Spiele wurden erhoben
 |

1. **Eine Löschpflicht liegt nach Art. 17 Abs. 3 DSGVO aus folgendem Grund nicht vor:**

|  |
| --- |
| * Ausübung des Rechts auf freie Meinungsäußerung und Information
* Erfüllung einer Rechtspflicht (gesetzliche Aufbewahrungsfristen z. B. nach HGB, AO, SGB) oder öffentlichen Aufgaben
* Begründung im öffentlichen Interesse
* Für im öffentlichen Interesse liegende Archivzwecke, Forschungszwecke oder statistische Zwecke
* Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
 |

1. **Eine Löschpflicht liegt vor, die Löschung des betroffenen Datensatzes wurde veranlasst:**

|  |
| --- |
| * Durchführende Stelle:
 |

1. **Eine Löschpflicht liegt nicht vor, eine Zugangsbeschränkung (Einschränkung) des betroffenen Datensatzes wurde veranlasst:**

|  |
| --- |
| * Durchführende Stelle:
 |

1. **Welche Daten wurden von der betroffenen Person verarbeitet?**

|  |
| --- |
| * Name
* Anschrift
* E-Mail-Adresse
* Telefonnummer
* Fax-Nummer
* Mandatierung
* Korrespondenz (E-Mail, Fax etc.)
* Weitere:
 |

1. **Welche Speicherorte im Unternehmen sind von der Löschpflicht betroffen?**

|  |
| --- |
| * Software
* Akten bzw. Unterlagen in Papierform
* Externe Festplatten
* USB-Sticks
* Mobile Endgeräte
* Internet
* Datensicherung
* Weitere:
 |

1. **Wurden die personenbezogenen Daten an Vertragspartner weitergegeben?**

|  |
| --- |
| * Ja, an folgende Vertragspartner:

Die Löschanfrage wurde weitergeleitet (Datum, Empfänger):* Nein
 |

1. **Zustellung des Antwortschreibens an:**

|  |
| --- |
| * Bekannte und durch betroffene Person mitgeteilte E-Mail-Adresse:
* Fax-Nr:
* Adresse:
* Datum des Antwortschreibens:
 |

1. **Weitere Hinweise:**

|  |
| --- |
|  |

1. **Wo finde ich hierzu im Unternehmen Informationen?**

|  |
| --- |
|  |

**Hinweise:**

1. Über sämtliche Anfragen, die durch betroffene Personen hinsichtlich der Wahrnehmung Ihrer Rechte an die Kanzlei gestellt werden, ist unverzüglich die Kanzleileitung zu informieren.
2. Übt eine betroffene Person ein Betroffenenrecht aus, so muss die Kanzlei die Identität der betroffenen Person feststellen. Kann die Identität der betroffenen Person nicht festgestellt werden, so muss die Ausübung eines Betroffenenrechts aus den Artikeln 15 – 20 DSGVO verweigert, die anfragende Person unterrichtet und der Vorgang dokumentiert werden. Die Prüfung der Plausibilität der Identität ist hierbei ausreichend. Verwendet die betroffene Person eine Adresse, mit der sie zuvor mit dem Verantwortlichen korrespondiert hat, darf eine Auskunft an diese Adresse versendet werden. Sofern dies per E-Mail erfolgt, ist in der Regel auf eine Inhaltsverschlüsselung zu achten.
3. Die Kanzlei muss gemäß Art. 12 DSGVO sicherstellen, dass ein Betroffenenrecht **spätestens innerhalb eines Monats** gewährt wird.

Eine Fristverlängerung um weitere 2 Monate ist zulässig, wenn dies unter der Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Eine Information über die Fristverlängerung zusammen mit der Begründung für die Verzögerung muss innerhalb eines Monats nach Eingang des Antrags erfolgen.

Sofern dem Löschantrag nicht nachgekommen werden kann, ist der Betroffene innerhalb eines Monats über die Gründe und das Recht bei der zuständigen Aufsichtsbehörde Beschwerde einzulegen, zu informieren.

1. Die betroffene Person kann eine Bestätigung darüber verlangen, ob in der Kanzlei sie betreffende personenbezogene Daten verarbeitet werden. Somit ist auch eine Negativauskunft erforderlich, wenn der Verantwortliche entweder keine Daten zu dieser Person verarbeitet oder personenbezogene Daten unumkehrbar anonymisiert hat.
2. **Auskünfte an Behörden dürfen grundsätzlich nur von hierzu autorisierten Personen der Kanzlei erteilt werden. Fragen Sie hierzu die Kanzleileitung!**

Anlage 2

**Muster Löschkonzept**

1. **Verantwortlichkeiten**

Variante 1:

Die Einhaltung der Löschfristen wird durch die Kanzleileitung bzw. eine durch die Kanzleileitung beauftragte Person einmal jährlich überprüft. Das Ergebnis dieser Überprüfung wird dokumentiert.

Variante 2:

Die Einhaltung der Löschfristen wird durch folgende Personen einmal jährlich überprüft. Das Ergebnis dieser Überprüfungen ist zu dokumentieren.

Mandantendaten: XXX

Beschäftigen- und Bewerberdaten, sowie Daten in Zusammenhang mit Mandanten-/Interessentenveranstaltungen: XXX

Protokolldaten: XXX

Videoüberwachung: XXX

**Datenarten und Löschfristen**

*Folgende Datenkategorien, Datenarten, Aufbewahrungsfristen und Bemerkungen sind beispielhaft zu verstehen und müssen in der Kanzlei individuell angepasst und erarbeitet werden.*

| **Datenkategorie** | **Datenart** | **Aufbewahrungsfrist** | **Löschzeitraum** | **Bemerkung** |
| --- | --- | --- | --- | --- |
| **Mandantendaten** | Steuerberatungsvertrag und Vollmachten | 15 Jahre nach Beendigung des Mandatsverhältnisses | innerhalb von 6 Monaten nach Ablauf der Aufbewahrungsfrist  | Die Aufbewahrungsfrist beginnt jeweils mit dem Schluss des Kalenderjahrs in dem das Mandatsverhältnis endete. |
|  | Lohn- und Gehaltsabrechnung Mandanten | 15 Jahre nach Beendigung des Mandatsverhältnisses | innerhalb von 6 Monaten nach Ablauf der Aufbewahrungsfrist  | Die Aufbewahrungsfrist beginnt jeweils mit dem Schluss des Kalenderjahrs in dem das Mandatsverhältnis endete. |
|  | Rechnungswesen und Deklarationswesen | 15 Jahre nach Beendigung des Mandatsverhältnisses | innerhalb von 6 Monaten nach Ablauf der Aufbewahrungsfrist  | Die Aufbewahrungsfrist beginnt jeweils mit dem Schluss des Kalenderjahrs in dem das Mandatsverhältnis endete. |
|  | etc. |  |  |  |
|  |
| **Beschäftigten-daten** | Bewerbungsunterlagen (bei abgelehnten Bewerbern) | 6 Monate nach Bewerbung | innerhalb von 4 Wochen nach Fristende |  |
|  | Bewerbungsunterlagen bei Mitarbeitern | 10 Jahre nach Beendigung des Arbeitsverhältnisses | innerhalb von 6 Monaten nach Ablauf der Aufbewahrungsfrist  | Die Aufbewahrungsfrist beginnt jeweils mit dem Schluss des Kalenderjahrs in dem das Arbeitsverhältnis endete. |
|  | Reisekostenabrechnung |  |  |  |
|  | Mitarbeiterdarlehen |  |  |  |
|  | Arbeitszeiterfassung |  |  |  |
|  | Mitarbeiterfotos auf der Homepage | Keine Aufbewahrungsfrist | Innerhalb von 14 Tagen nach Beendigung des Arbeitsverhältnisses oder nach Widerruf | Die Dateien sind sowohl von der Homepage zu entfernen als auch in der Mediathek des CMS zu löschen.  |
|  | Verbandbuch |  |  |  |
|  | etc. |  |  |  |
|  |
| **EDV** | Protokolle Firewall  | 6 Monate | Unmittelbar | Die Löschung sollte technisch sichergestellt werden. |
|  | Protokolle Windows (Mitarbeiter) |  |  |  |
|  | Protokolle Gäste-WLAN |  |  |  |
|  | Protokolle Steuerberatersoftware |  |  |  |
|  | Protokolle Lohnsoftware |  |  |  |
|  | Protokolle asp |  |  |  |
|  | etc. |  |  |  |
|  |
| **Videoüberwachung** | Videoüberwachung des Kanzleieingangs | 72 Stunden | Unmittelbar | Die Löschung nach 72 Stunden ist technisch sicher zu stellen! |

1. Das Löschkonzept soll die Praxisarbeit unterstützen. Verfahren und Fristen sind individuell und eigenverant-

 wortlich anzupassen. [↑](#footnote-ref-1)
2. Zu beachten: direkte Geltendmachung von Betroffenenrechten durch Arbeitnehmer eines Mandanten sind rechtlich möglich, aber Einbeziehung des Mandanten erforderlich. [↑](#footnote-ref-2)