**[Bearbeitervermerk:**

**Jede Stelle, die personenbezogene Daten verarbeitet, muss ein Löschkonzept als Teil des Datenschutzkonzeptes vorweisen können. Zur Erstellung des Löschkonzeptes für Ihre Praxis können Sie diese Vorlage verwenden. Zur Vorlage gehören auch die Anlagen 1-3, welche Sie ebenfalls an Ihre Bedürfnisse anpassen und zum Teil Ihres Datenschutzkonzeptes machen sollten.**

**An den gelb markierten Stellen müssen Sie jeweils eigene Angaben machen.**

**Löschintervalle:**

**Sie sollten wenigstens einmal jährlich alle Akten auf Löschungsreife hin überprüfen. Legen Sie einen Zeitraum fest, in welchem Sie dies erledigen.**

**Speicherung von Patientenakten:**

**Da es nicht immer im besten Interesse der Patientinnen und Patienten ist, ihre Daten nach zehn Jahren zu löschen, ist auch eine längere, über den Zeitraum von zehn Jahren hinausgehende Speicherung möglich. Möchten Sie in Ihrer Praxis von der Möglichkeit, Patientenakten auch über zehn Jahre hinaus zu speichern, Gebrauch machen, verwenden Sie bitte den hier vorgeschlagenen Textbaustein. Sofern Sie alle Patientenakten nach Ablauf von zehn Jahren grundsätzlich löschen möchten, verzichten Sie auf den Textbaustein und löschen Sie ihn.**

**Zu guter Letzt sollten Sie festlegen, wer für die Überwachung der Einhaltung der Löschfristen und die Löschung zuständig ist. Im Zweifel fällt diese Aufgabe der Praxisleitung bzw. der Praxisinhaberin/dem Praxisinhaber zu.**

**Beim Löschprotokoll genügt es, wenn Sie jeweils in der ersten Spalte angeben, welche Arten von Daten gelöscht worden sind (z.B. *Patientenakten, Mitarbeiterunterlagen, Rechnungen, etc.*) und das Datum der Löschung notieren. Sollte Ihnen bei der Löschung Besonderheiten aufgefallen sein, können Sie diese in die Spalte „Anmerkungen“ vermerken.**

Falls Sie weitere Aspekte oder Sachverhalte, die in der Vorlage noch nicht abgebildet sind, in die Vorlage aufnehmen möchten, wenden Sie sich gerne an uns.

Sollten Sie Fragen haben, zögern Sie bitte nicht, sich an uns zu wenden.

DATA*privat* GmbH

horbach@dataprivat.de

0241 - 99 77 6 88 3

Entfernen Sie ganz zum Schluss bitte auch diesen Bearbeitungshinweis.

Ihr DATA*privat* Team]

**Datenlöschkonzept der**

**Praxis Mustermann**

**Inhaberin: Petra Mustermann**

**Musterstraße 1, 12345 Musterhausen**

**Datum der Erstellung des Konzepts:** XX.XX.2019

Nach dem in Art. 5 Abs. 1 lit. c DSGVO verankerten Grundsatzes der Speicherbegrenzung dürfen personenbezogene Daten nur solange gespeichert werden, wie es für die Erreichung des Zweckes der Verarbeitung erforderlich ist. Zur Verwirklichung der Grundsätze der Speicherbegrenzung und der Zweckbindung bestimmen wir für unsere Praxis dieses Löschkonzept.

Als Teil unseres Löschkonzeptes legen wir folgendes fest:

**Übergangsfristen:**

Nach Ablauf der Löschfrist bis zur endgültigen Löschung dürfen bei Datenkategorien, welche einer Aufbewahrungsfrist von mindestens sechs Jahren unterliegen, nicht mehr als sechs Monate vergehen. Bei Datenkategorien, deren Löschungsreife früher eintritt, muss die Löschung spätestens drei Wochen nach Ablauf der Löschfrist erfolgen.

**Durchführungsanweisungen zur Löschung:**

Sobald wir Daten nicht mehr benötigen oder die gesetzliche Aufbewahrungsfrist (Auflistung aller Fristen in **Anlage 1**) abgelaufen ist, löschen wir die entsprechenden Daten.

**Löschintervalle und Besonderes Vorgehen bei Patientenakten:**

Alle Patientenakten werden mindestens einmal jährlich und zwar zu Beginn/Ende des 1., 2., 3., 4. Quartals eines jeden Kalenderjahres auf Löschungsreife hin überprüft.

*[Optional, nur wenn Patientendaten länger als zehn Jahre gespeichert werden sollen:*

Wir sind gesetzlich verpflichtet, Patientenakten und die darin enthaltene Behandlungsdokumentation mindestens zehn Jahre nach Abschluss der Behandlung zu speichern (§ 630 f Abs. 3 BGB i.V.m. Art. 9 Abs. 4 DSGVO). Aus unserer Sicht liegt jedoch eine Löschung der Daten nach Ablauf der Zehnjahresfrist in der überwiegenden Zahl der Fälle nicht im Interesse Betroffenen (= der Patientinnen und Patienten). In der Frist kommt ausschließlich die gesetzgeberische Wertung in Bezug auf das Beweiserhaltungsinteresse von Patientinnen und Patienten und Behandlerinnen und Behandler zum Ausdruck. Tatsächlich kann es für die Behandlung jedoch auch nach längeren Zeiträumen als zehn Jahre wichtig sein, nachzuvollziehen, mit welchen Leiden ein/e Patient/in bereits in der Praxis war, welche Behandlungen sie/er empfangen hat und wie die Behandlungen verlaufen sind.

Wir speichern Patientenakten daher auch über die gesetzliche Aufbewahrungsfrist hinaus und machen insoweit von der Möglichkeit Gebrauch, welche der Gesetzgeber in § 35 Abs. 2 BDSG geschaffen hat. Danach können Daten zu fremden Zwecken gespeichert werden, sofern die betroffenen Personen bei Erhebung der Daten darauf hingewiesen worden sind und die Daten nur eingeschränkt verarbeitet werden.

Wir löschen Patientendaten nach Ablauf der gesetzlichen Aufbewahrungsfrist in jedem Fall, wenn die Betroffenen von ihrem Recht auf Löschung Gebrauch machen (Art. 17 DSGVO) oder die Patientinnen und Patienten uns vor Ablauf der Frist darauf hingewiesen haben.

*Ende des optionalen Textes. Bitte den gelbmarkierten Text vor und nach dem Absatz löschen]*

Alle Unterlagen, welche der steuerlichen Aufbewahrungspflicht von zehn Jahren gemäß § 147 AO unterliegen, werden jährlich nach Fristablauf gelöscht.

Je nach Datenträger werden Daten unterschiedlich gelöscht. Wir löschen nach den Vorgaben der DIN-Norm 66399, die die Grundlagen der Datenvernichtung festlegt. Die genaue Form der Vernichtung richtet sich nach der Schutzklasse und der Sicherheitsstufe der jeweiligen Daten (siehe **Anlage 2**).

Dabei gehen wir wie folgt vor:

* **Daten auf Papier** (z.B. Patientenakten, Papierkalender, Personalakten)**:** Diese Daten entsorgen wir über eine spezielle Entsorgungstonne oder löschen sie über geeignete Schredder. Wir nutzen hierfür Aktenvernichter der Sicherheitsstufe P-4 nach DIN 66399.
* **Daten auf digitale Datenträger** (z.B. Festplatten, DVD, USB-Stick, usw.):

Diese Daten löschen wir entweder, indem wir ein "Leasing" durchführen oder aber den gesamten Datenträger vernichten.

**1. Möglichkeit: Überschreiben**

Beim „Leasing“ werden Daten auf einem Datenträger durch ein mehrmaliges Überschreiben mit Zufallszahlen (Nullen und Einsen) unlesbar gemacht. Dies erfolgt mit kommerziellen Tools, die in Versionen für Server, PCs, mobile Endgeräte und Speicher-Systeme zur Verfügung stehen. SSDs, die über den SATA-Bus an einen unserer Rechner angebunden sind, löschen wir mit dem „ATA Secure Erase“-Befehl oder aber mit Hilfe eines Tools, das bereits vom Anbieter der jeweiligen SSD auf dem Flash-Speicher vorhanden ist.

**2. Möglichkeit: Vernichtung des Datenträgers**

Wollen wir Datenträger nicht mehr weiterverwenden, vernichten wir den gesamten Datenträger. Festplatten aus PCs bauen wir vor der Vernichtung aus dem PC aus und vernichten nur die Festplatte, nicht den gesamten PC. Wir schreddern die jeweiligen Datenträger entweder fachgerecht in unserer Praxis oder beauftragen hierfür ein Fachunternehmen.

Für Festplatten nutzen wir einen Schredder der Sicherheitsstufe H-4 nach DIN 66399, für optische Datenträger (CD, DVD) einen Schredder der Sicherheitsstufe O-4 nach DIN 66399, für Halbleiterspeicher (USB-Sticks, SSDs) einen Schredder der Sicherheitsstufe E-4 nach DIN 66399.

* **Drucker, Faxe andere Endgeräte:**

Entsorgen wir Endgeräte wie Drucker, Telefaxgeräte, Mobiltelefone o. ä. aus unserer Praxis, prüfen wir die integrierten Speicher auf persistente Daten. Vor einer Weitergabe oder Verschrottung stellen wir sicher, dass diese Speicher gegebenenfalls gelöscht sind.

**Protokollierungsanweisung:**

Die Löschung und Vernichtung von Daten protokollieren wir unserer Löschliste (siehe **Anlage 3**).

**Verantwortlichkeiten:**

Verantwortlich für das Löschen der Daten und damit für die Einhaltung der Löschfristen und der tatsächlichen Durchführung der Löschung ist \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Praxisinhaber/in).

[Optional]

Die turnusmäßige Überwachung der Akten auf Löschungsreife obliegt: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Anlage 1**

**Einzelaufstellung der Löschfristen**

|  |  |  |
| --- | --- | --- |
| **Art der Daten (Patientendaten, Kundendaten, Mitarbeiterdaten, sonstige Daten)** | **Aufbewahrungs-/Löschpflicht** | **Rechtsgrundlage** |
| **Patientendaten** | | |
| Stammdaten der Patienten | 10 Jahre | Behandlungsvertrag Art. 6 Abs. 1 b DS-GVO, Art. 9 Abs. 2 h i.V.m. Abs. 3 DS-GVO, § 22 BDSG n.F., § 630 f Abs. 3 BGB, § 147 AO |
| Krankheitsdaten | 10 Jahre | Behandlungsvertrag Art. 6 Abs. 1 b DS-GVO, Art. 9 Abs. 2 h i.V.m. Abs. 3 DS-GVO, § 22 BDSG n.F., § 630 f Abs. 3 BGB, § 147 AO |
| Körperliche Daten | 10 Jahre | Behandlungsvertrag Art. 6 Abs. 1 b DS-GVO, Art. 9 Abs. 2 h i.V.m. Abs. 3 DS-GVO, § 22 BDSG n.F., § 630 f Abs. 3 BGB |
| Sozialanamnetische Daten | 10 Jahre | Behandlungsvertrag Art. 6 Abs. 1 b DS-GVO, Art. 9 Abs. 2 h i.V.m. Abs. 3 DS-GVO, § 22 BDSG n.F., § 630 f Abs. 3 BGB |
| Krankheitsdaten | 10 Jahre | Behandlungsvertrag Art. 6 Abs. 1 b DS-GVO, Art. 9 Abs. 2 h i.V.m. Abs. 3 DS-GVO, § 22 BDSG n.F., § 630 f Abs. 3 BGB |
| Rechnungsdaten (Privatpatienten) | 10 Jahre | Behandlungsvertrag Art. 6 Abs. 1 b DS-GVO, Art. 9 Abs. 2 h i.V.m. Abs. 3 DS-GVO, § 22 BDSG n.F., § 630 f Abs. 3 BGB, § 147 AO |
| Behandler | 10 Jahre | Behandlungsvertrag Art. 6 Abs. 1 b DS-GVO, Art. 9 Abs. 2 h i.V.m. Abs. 3 DS-GVO, § 22 BDSG n.F., § 630 f Abs. 3 BGB |
| Zeiterfassungsdaten (Patienten) | 10 Jahre | Behandlungsvertrag Art. 6 Abs. 1 b DS-GVO, Art. 9 Abs. 2 h i.V.m. Abs. 3 DS-GVO, § 22 BDSG n.F., § 630 f Abs. 3 BGB |
| Begleitpersonen und Angehörige von Patienten | 10 Jahre | Behandlungsvertrag Art. 6 Abs. 1 b DS-GVO, Art. 9 Abs. 2 h i.V.m. Abs. 3 DS-GVO, § 22 BDSG n.F., § 630 f Abs. 3 BGB |
| **Kundendaten** | | |
| Stammdaten | 10 Jahre | Art. 6 Abs. 1 b DS-GVO, Art. 9 Abs. 2 h i.V.m. Abs. 3 DS-GVO, § 22 BDSG, § 147 AO |
| Krankheitsdaten | 10 Jahre | Art. 6 Abs. 1 b DS-GVO, Art. 9 Abs. 2 h i.V.m. Abs. 3 DS-GVO, § 22 BDSG, § 147 AO |
| Körperliche Gesundheitsdaten | 10 Jahre | Art. 6 Abs. 1 b DS-GVO, Art. 9 Abs. 2 h i.V.m. Abs. 3 DS-GVO, § 22 BDSG, § 147 AO |
| Rechnungsdaten | 10 Jahre | Art. 6 Abs. 1 b DS-GVO, Art. 9 Abs. 2 h i.V.m. Abs. 3 DS-GVO, § 22 BDSG, § 147 AO |
| Zeiterfassungsdaten | 10 Jahre | Art. 6 Abs. 1 b DS-GVO, Art. 9 Abs. 2 h i.V.m. Abs. 3 DS-GVO, § 22 BDSG, § 147 AO |
| **Allgemeine Praxisdaten** | | |
| Abmahnungen | nicht festgelegt, spätestens beim Ausscheiden des Mitarbeiters aus der Praxis | § 147 AO, § 257 HGB |
| An-, Ab- und Ummeldungen der AOK und Ersatzkassen | 6 Jahre | § 147 AO, § 257 HGB |
| Anträge auf Arbeitnehmersparzulage | 6 Jahre | § 147 AO, § 257 HGB |
| Arbeitsmittelprüfung – Aufzeichnung über Prüfungsergebnisse | Angemessene Zeit (mindestens bis zur nächsten Prüfung) | § 11 BetrSichV |
| Arbeitszeitnachweise, soweit für Lohnbuchhaltung erforderlich | 10 Jahre (ansonsten 2 Jahre) | Art. 6 Abs. 1 f DS-GVO i.V.m. den Arbeitsverträgen, § 16 Abs. 2 ArbZG, § 147 AO |
| Bankauszüge, Bankbelege | 10 Jahre |  |
| Bankdaten der Mitarbeiter | 10 Jahre | Art. 6 Abs. 1 f DS-GVO i.V.m. den Arbeitsverträgen, § 147 AO |
| Beitragsabrechnungen zur Sozialversicherung | 10 Jahre | § 147 AO, § 257 HGB |
| Belege, Beleglisten, Sammelbelege, Buchungsunterlagen | 10 Jahre | § 147 AO, § 257 HGB |
| Bewerbungsunterlagen abgelehnter Bewerber | eine gesetzliche Frist existiert nicht; Empfehlung: 6-9 Monate, bis zum Ablauf der variablen Klagefristen | 15 Abs. 4 AGG, § 61 Abs. 1 ArbGG, Art. 6 Abs. 1 f DS-GVO i.V.m § 21 Abs. 2 S. 1 AGG |
| Bewirtungsunterlagen | 10 Jahre | § 147 AO, § 257 HGB |
| Darlehnsunterlagen | 10 Jahre | § 147 AO, § 257 HGB |
| Dauerauftragsunterlagen | 6 Jahre | § 147 AO, § 257 HGB |
| DEÜV-Bescheinigung über Datenübermittlung | bis zum Ablauf des auf die letzte Prüfung folgenden Kalenderjahres | § 25 DEÜV |
| E-Mails mit steuerrelevantem Inhalt | 10 Jahre | § 147 AO, § 257 HGB |
| Fahrtkostenerstattungsunterlagen | 6 Jahre | § 41 Abs. 1 EstG i.V.m. R 38 der Lohnsteuerrichtline |
| Gehaltslisten | 10 Jahre | § 147 AO, § 257 HGB |
| Geschenknachweise | 10 Jahre | § 147 AO, § 257 HGB |
| Heimarbeit-Entgeltbelege | 3 Jahre | § 13 HAGDV 1 |
| Heimarbeit-Personenlisten | bis zum Ablauf des Kalenderjahres, das auf das Jahr der Anlegung folgt | § 9 Abs. 3 HAGDV 1 |
| Inkassobücher, -Karteien, - Quittungen | 10 Jahre | § 147 AO, § 257 HGB |
| Jahreslohnnachweise für Berufsgenossenschaften | 10 Jahre | § 147 AO, § 257 HGB |
| Kontoauszüge | 10 Jahre | § 147 AO, § 257 HGB |
| Krankschreibungen mit Auswirkung auf den Lohn | 10 Jahre | Art. 6 Abs. 1 f DS-GVO i.V.m. den Arbeitsverträgen, § 16 Abs. 2 ArbZG, § 147 AO |
| Krankschreibungen ohne Auswirkung auf den Lohn, etc.) | 2 Jahre | Art. 6 Abs. 1 f DS-GVO i.V.m. den Arbeitsverträgen, § 16 Abs. 2 ArbZG |
| Lastschriftanzeigen | 10 Jahre | § 147 AO, § 257 HGB |
| Lohnkontenarten | 10 Jahre | § 147 AO, § 257 HGB |
| Lohnlisten | 10 Jahre | § 147 AO, § 257 HGB |
| Lohnsteuer-Jahresausgleichsunterlagen | 10 Jahre | § 147 AO, § 257 HGB |
| Mahnvorgänge | 10 Jahre | § 147 AO, § 257 HGB |
| Mietverträge (nach Vertragsende) | 6 Jahre | § 147 AO, § 257 HGB |
| Mutterschutzunterlagen | 2 Jahre | § 19 Abs. 2 MuSchuG |
| Pensionskassenunterlagen | 10 Jahre | § 147 AO, § 257 HGB |
| Pfändungsunterlagen | 10 Jahre | § 147 AO, § 257 HGB |
| Prämienunterlagen (z.B. Versicherung), soweit Buchungsunterlagen | 10 Jahre | § 147 AO, § 257 HGB |
| Provisionsabrechnung mit Unterlagen | 10 Jahre | § 147 AO, § 257 HGB |
| Quittungen, wenn Buchungsunterlagen | 10 Jahre | § 147 AO, § 257 HGB |
| Personalakte | 6-10 Jahre | Art. 6 Abs. 1 f DS-GVO i.V.m. den Arbeitsverträgen, § 147 AO |
| Rechnungen und Rechnungsunterlagen | 10 Jahre | § 147 AO, § 257 HGB |
| Rechtsstreitfälle mit allen Unterlagen, Klagearten (nach Verfahrensabschluss) | 6 Jahre | § 147 AO, § 257 HGB |
| Reisekostenabrechnung | 10 Jahre | § 147 AO, § 257 HGB |
| Röntgenbilder | 10 Jahre | § 147 AO, § 257 HGB |
| Schriftwechsel (auch innerbetrieblich) | 6 Jahre | § 147 AO, § 257 HGB |
| Sozialversicherungsunterlagen | 6 Jahre | § 147 AO, § 257 HGB |
| Stammdaten der Mitarbeiter | 10 Jahre | Art. 6 Abs. 1 f DS-GVO i.V.m. den Arbeitsverträgen, § 147 AO |
| Telefonkostennachweise | 10 Jahre | § 147 AO, § 257 HGB |
| Überstundenlisten (nicht buchhaltungsrelevant) | 2 Jahre | § 147 AO, § 257 HGB |
| Überstundenlisten (buchhaltungsrelevant) | 10 Jahre | § 147 AO, § 257 HGB |
| Urlaubsanträge | 0 (Vernichtung nach Abschluss des Vorgangs | § 147 AO, § 257 HGB |
| Urlaubsgenehmigung (soweit buchungsrelevant, z.B. wg. Urlaubsgeld) | 10 Jahre | § 147 AO, § 257 HGB |
| Verträge | 6 Jahre nach Vertragsende | § 147 AO, § 257 HGB |

**Anlage 2**

**I. Schutzklassen nach DIN Norm 66399**

|  |  |
| --- | --- |
| **Schutzklasse 1** | **Normaler Schutzbedarf** für interne Daten (z.B. Telefonlisten, Lieferantendateien, Adressdatenbanken, Notizen)  Der Schutz von personenbezogenen Daten muss gewährleistet sein. Andernfalls besteht die Gefahr, dass der Betroffene in seiner Stellung und seinen wirtschaftlichen Verhältnissen beeinträchtigt wird. |
| **Schutzklasse 2** | **Hoher Schutzbedarf** für vertrauliche Daten (z.B. Personal- und Finanzdaten)  Bei diesen Daten besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt wird. Außerdem hätte die unbefugte Kenntnisnahme der Daten erhebliche negative Auswirkungen für die speichernde Stelle. |
| **Schutzklasse 3** | **Sehr hoher Schutzbedarf für besonders geheime und vertrauliche Daten**  Der Schutz personenbezogener Daten muss unbedingt gewährleistet sein. Andernfalls kann es zu einer Gefahr für Leib und Leben oder für die persönliche Freiheit des Betroffenen kommen. Außerdem hätte die unbefugte Kenntnisnahme der Daten ernsthafte (existenzbedrohende) Auswirkungen für die speichernde Stelle und würde gegen Berufsgeheimnisse, Verträge oder Gesetze verstoßen (z. B. Forschungs- und Entwicklungsdokumente, Verschlusssachen, **Gesundheitsdaten**) |

**II. Sicherheitsstufen nach DIN Norm 66399**

|  |  |
| --- | --- |
| **Sicherheitsstufe 1** | **Allgemeine Daten** (z.B. Broschüren und Kataloge)  Der Datenträger wird so vernichtet, dass die Reproduktion der auf ihm gespeicherten Daten mit einfachem Aufwand (= ohne besondere Hilfsmittel und Fachkenntnisse, jedoch nicht ohne besonderen Zeitaufwand) möglich ist.  Papiere und Filme in Originalgröße: Materialteilchenfläche max. 2.000 mm², Streifenbreite max. 12 mm, Streifenlänge unbegrenzt, Toleranz für 10 % der Fläche des Materials: maximal 3800 mm²  Kunststoff wie Identifikationskarte oder Mikrofilm:  Materialteilchenfläche max. 160 mm², Toleranz für 10 % der Fläche des Materials: maximal 480 mm²  Optische Datenträger: Materialteilchenfläche max. 2000 mm², Toleranz für 10 % der Fläche des Materials: maximal 3800 mm²  Magnetische Datenträger:  Medium muss funktionsunfähig sein  Festplatten:  Festplatte muss funktionsunfähig sein  Halbleiterspeicher (z.B. Speichersticks, Chipkarten, mobile Kommunikationsmittel): Datenträger muss funktionsunfähig sein |
| **Sicherheitsstufe 2** | **Interne Daten** (z.B. Aushänge und Formulare)  Der Datenträger wird so vernichtet, dass die Reproduktion der auf ihm gespeicherten Daten mit besonderem Aufwand (= mit Hilfsmitteln und nur mit besonderem Zeitaufwand) möglich ist.  Papiere und Filme in Originalgröße: Materialteilchenfläche max. 800 mm², Streifenbreite bis max. 6 mm, Streifenlänge unbegrenzt, Toleranz für 10 % der Fläche des Materials: maximal 2000 mm²  Kunststoff wie Identifikationskarte oder Mikrofilm:  Materialteilchenfläche max. 30 mm², Toleranz für 10 % der Fläche des Materials: maximal 90 mm²  Optische Datenträger: Materialteilchenfläche max. 800 mm², Toleranz für 10 % der Fläche des Materials: maximal 2000 mm²  Magnetische Datenträger: Medium mehrfach zerteilt und Materialteilchenfläche max. 2000 mm², Toleranz für 10 % der Fläche des Materials: maximal 3800 mm²  Festplatten:  Datenträger beschädigt  Halbleiterspeicher:  Datenträger muss zerteilt sein |
| **Sicherheitsstufe 3** | **Sensible Daten** (Unterlagen mit vertraulichen Daten)  Der Datenträger wird so vernichtet, dass die Reproduktion der auf ihm gespeicherten Daten mit erheblichem Aufwand (= Personen, Hilfsmittel, Zeit) möglich ist.  Papiere und Filme in Originalgröße: Materialteilchenfläche max. 320 mm², Streifenbreite max. 2 mm, Streifenlänge unbegrenzt, Toleranz für 10 % der Fläche des Materials: maximal 480 mm²  Kunststoff wie Identifikationskarte oder Mikrofilm:  Materialteilchenfläche max. 10 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm²  Optische Datenträger: Materialteilchenfläche max. 160 mm², Toleranz für 10 % der Fläche des Materials: maximal 480 mm²  Magnetische Datenträger: Materialteilchenfläche max. 320 mm², Toleranz für 10 % der Fläche des Materials: maximal 800 mm²  Festplatten:  Datenträger verformt  Halbleiterspeicher:  Datenträger muss zerteilt sein und Materialteilchenfläche max. 160 mm², Toleranz für 10 % der Fläche des Materials: maximal 480 mm² |
| **Sicherheitsstufe 4** | **Besonders sensible Daten** (z.B. Gehaltsabrechnungen, Personaldaten/-akten, Arbeitsverträge, medizinische Berichte, Steuerunterlagen)  Der Datenträger wird so vernichtet, dass die Reproduktion der auf ihm gespeicherten Daten mit außergewöhnlichem Aufwand (= Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen, die im Falle kleiner Auflagen sehr aufwändig sind) möglich ist.  Papiere und Filme in Originalgröße: Materialteilchenfläche max. 160 mm² und für gleichförmige Partikel: Streifenbreite max. 6 mm, Toleranz für 10 % der Fläche des Materials: maximal 800 mm²  Kunststoff wie Identifikationskarte oder Mikrofilm:  Materialteilchenfläche max. 2,5 mm², Toleranz für 10 % der Fläche des Materials: maximal 7,5 mm²  Optische Datenträger: Materialteilchenfläche max. 30 mm², Toleranz für 10 % der Fläche des Materials: maximal 90 mm²  Magnetische Datenträger: Materialteilchenfläche max. 160 mm², Toleranz für 10 % der Fläche des Materials: maximal 480 mm²  Festplatten:  Datenträger mehrfach zerteilt und verformt und Materialteilchenfläche max. 2000 mm², Toleranz für 10 % der Fläche des Materials: maximal 3800 mm²  Halbleiterspeicher:  Datenträger muss zerteilt sein und Materialteilchenfläche max. 30 mm², Toleranz für 10 % der Fläche des Materials: maximal 90 mm² |
| **Sicherheitsstufe 5** | **Geheim zu haltende Daten** (Datenträger mit geheim zu haltenden Informationen mit existenzieller Wichtigkeit für eine Person, ein Unternehmen oder eine Einrichtung)  Der Datenträger wird so vernichtet, dass die Reproduktion der auf ihm gespeicherten Daten mit zweifelhaften Methoden möglich ist.  Papiere und Filme in Originalgröße: Materialteilchenfläche max. 30 mm² und für gleichförmige Partikel: Streifenbreite max. 2 mm, Toleranz für 10 % der Fläche des Materials: maximal 90 mm²  Kunststoff wie Identifikationskarte oder Mikrofilm:  Materialteilchenfläche max. 1 mm², Toleranz für 10 % der Fläche des Materials: maximal 3 mm²  Optische Datenträger: Materialteilchenfläche max. 10 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm²  Magnetische Datenträger: Materialteilchenfläche max. 30 mm², Toleranz für 10 % der Fläche des Materials: maximal 90 mm²  Festplatten:  Datenträger mehrfach zerteilt und verformt und Materialteilchenfläche max. 320 mm², Toleranz für 10 % der Fläche des Materials: maximal 800 mm²  Halbleiterspeicher:  Datenträger muss zerteilt sein und Materialteilchenfläche max. 10 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm² |
| **Sicherheitsstufe 6** | **Geheime Hochsicherheitsdaten** (z.B. geheimdienstlicher oder militärischer Bereich)  Der Datenträger wird so vernichtet, dass die Reproduktion der auf ihm gespeicherten Daten technisch nicht möglich ist.  Papiere und Filme in Originalgröße: Materialteilchenfläche max. 10 mm² und für gleichförmige Partikel: Streifenbreite max. 1 mm, Toleranz für 10 % der Fläche des Materials: maximal 30 mm²  Kunststoff wie Identifikationskarte oder Mikrofilm:  Materialteilchenfläche max. 0,5 mm², Toleranz für 10 % der Fläche des Materials: maximal 1,5 mm²  Optische Datenträger: Materialteilchenfläche max. 5 mm², Toleranz für 10 % der Fläche des Materials: maximal 15 mm²  Magnetische Datenträger: Materialteilchenfläche max. 10 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm²  Festplatten:  Datenträger mehrfach zerteilt und verformt und Materialteilchenfläche max. 10 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm²  Halbleiterspeicher:  Datenträger muss mehrfach zerteilt sein und Materialteilchenfläche max. 1 mm², Toleranz für 10 % der Fläche des Materials: maximal 30 mm² |
| **Sicherheitsstufe 7** | **Top Secret Hochsicherheitsdaten** (Datenträger mit strengst geheim zu haltende Daten, bei denen höchste Sicherheitsvorkehrungen einzuhalten sind).  Eine Reproduktion ist ausgeschlossen!  Papiere und Filme in Originalgröße: Materialteilchenfläche max. 5 mm² und für gleichförmige Partikel: Streifenbreite max. 1 mm, Toleranz für 10 % der Fläche des Materials: keine Toleranz zugelassen  Kunststoff wie Identifikationskarte oder Mikrofilm:  Materialteilchenfläche max. 0,2 mm², Toleranz für 10 % der Fläche des Materials: keine Toleranz zugelassen  Optische Datenträger: Materialteilchenfläche max. 0,2 mm², Toleranz für 10 % der Fläche des Materials: maximal 0,6 mm² |

**III. Zuordnung der Sicherheitsstufen zu den gewählten Schutzklassen**

Jeder Schutzklasse können unterschiedliche Sicherheitsstufen zugeordnet werden, möglich sind jedoch nur folgende Kombinationen:

* **Datenträger der Schutzklasse 1** können den Sicherheitsstufen 1, 2 und 3 zugeordnet werden. Ausnahme: Handelt es sich um personenbezogene Daten, ist nur eine Zuordnung zur Sicherheitsstufe 3 erlaubt.
* **Datenträger der Schutzklasse 2** können den Sicherheitsstufen 3, 4 und 5 zugeordnet werden.
* **Datenträger der Schutzklasse 3** können den Sicherheitsstufen 4, 5, 6 und 7 zugeordnet werden.

**IV. Kürzel der Datenträgerart**

Jede Datenträgerart ist durch ein Kürzel beschrieben (PFOTHE), das der jeweiligen Sicherheitsstufe vorangestellt wird:

* **P** - Informationsdarstellung in Originalgröße: *Papier, Film, Druckformen*
* **F** - Informationsdarstellung verkleinert: *Film, Mikrofilm, Folie*
* **O** - Informationsdarstellung auf optischen Datenträgern: *CD, DVD*
* **T** - Informationsdarstellung auf magnetischen Datenträgern: *Disketten, ID-Karten, Magnetbandkassetten*
* **H** - Informationsdarstellung auf Festplatten mit magnetischem Datenträger: *Festplatten*
* **E** - Informationsdarstellung auf elektronischen Datenträgern: *Speicherstick, Chipkarte, Halbleiterfestplatten, mobile Kommunikationsmittel*

**Anlage 3**

**Löschprotokoll**

**Name des Verantwortlichen: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |
| --- | --- | --- |
| **Gelöschte Daten** | **Datum der Löschung** | **Anmerkungen** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |