GEFAK

Vorgehen der GEFAK zur Vernichtung von Datenträgern und Papier

Stand: 15.11.2022

GEFAK Gesellschaft für angewandte Kommunalforschung mbH
Ockershäuser Allee 40b · 35037 Marburg
Tel.: +49 6421 1728-0 · Fax: +49 6421 1728-28
www.gefak.de · info@gefak.de
Amtsgericht Marburg HR B 1699
Geschäftsführer Dr. Ulrich Dewald, Christian Worm

Nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die datenschutzgerechte Verarbeitung der Daten sicherzustellen.

Soweit es sich um personenbezogene Daten handelt, sind die gesetzlichen Regelungen über den Zeitpunkt und die Art und Weise der Löschung zu beachten.

Als gelöscht gelten Daten, wenn sie unkenntlich gemacht wurden. Konkrete Aussagen über eine gesicherte Vernichtung von Informationsträgern enthält die DIN 66399 Teile 1, 2, 3. Diese Norm unterscheidet fünf Sicherheitsstufen bei der Vernichtung und berücksichtigt bei der Festlegung den Grad der Schutzwürdigkeit von Informationen, die physikalischen Eigenschaften von Informationsträgern und die zur Anwendung kommenden technischen Verfahren.

Datenträger

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gibt in diesem Zusammenhang die folgenden Empfehlungen:

1. Der Problemkreis des sicheren Löschens von Daten erfordert die Sensibilisierung der verantwortlichen Entscheidungsträger, Administratoren, Sicherheits- und Datenschutzbeauftragten sowie jedes einzelnen Nutzers. Dies ist durch geeignete Information und Schulung zu erreichen.

2. Im jeweiligen Verantwortungsbereich sind technisch-organisatorische Maßnahmen festzulegen, die eine sichere Löschung von Daten gewährleisten. Sie sind in das übergreifende Datenschutz- bzw. Sicherheitskonzept zu integrieren. Insbesondere sind Maßnahmen vor der Veräußerung, Vermietung, Aussonderung, Rückgabe, Reparatur und Wartung von Datenträgern zu bestimmen.

3. Die Maßnahmen sind durch konkrete Handlungsanweisungen für das sichere Löschen zu untersetzen. Diese Anweisungen müssen den Schutzbedarf der zu löschenden Daten ebenso berücksichtigen wie den Aufwand und die Kosten für eine mögliche Datenwiederherstellung.

4. Schutzwürdige Daten sind (soweit möglich) bereits in verschlüsselter Form auf dem Datenträger zu speichern. Hierzu sollten verschlüsselte Dateisysteme verwendet werden. Auch für temporäre und Auslagerungsdateien sowie für Sicherheitskopien sollten verschlüsselte Dateisysteme verwendet werden, da diese ebenfalls schutzwürdige Daten enthalten können.

5. Daten auf intakten Datenträgern sind durch das ein- oder mehrmalige, komplette Überschreiben mit Zufallszahlen zu löschen. Hierbei können spezielle Softwarewerkzeuge zum Einsatz

kommen. Die Verwendung gleichförmiger Überschreibmuster beim Löschen ist nicht zu empfehlen, da so kein Schutz gegen ausführliche Laboranalysen besteht.

6. Das einmalige, komplette Überschreiben mit Zufallszahlen sollte beim Löschen von Daten jeder Art praktiziert werden. Beim Löschen personenbezogener Daten niedriger oder mittlerer Schutzstufe sollten mindestens 7 Überschreibzyklen ausgeführt werden. Personenbezogene Daten hoher Schutzstufe sollten mit mindestens 33 Überschreibzyklen gelöscht werden.

7. Soll ein noch intakter Datenträger verkauft, vermietet, ausgesondert, zurückgegeben oder einer neuen Nutzung zugeführt werden, ist zuvor der gesamte Datenträger mehrmals komplett mit Zufallszahlen zu überschreiben. Diese Form der Wiederaufbereitung gestattet anschließend die weitere Nutzung des Datenträgers (z.B. die Neuinstallation eines Betriebssystems).

8. Das selektive Löschen einzelner Dateien durch Überschreiben ist meist problematisch. Es eignet sich nur dann, wenn sichergestellt ist, dass keine Kopien der in diesen Dateien enthaltenen Daten an anderen Orten abgelegt wurden (z.B. in temporären Dateien, Auslagerungsdateien oder Sicherungskopien) oder diese Orte eindeutig bestimmt und auch die Kopien sicher gelöscht werden können. Weiter ist zu gewährleisten, dass die Metadaten der gelöschten Dateien überschrieben werden, falls sie sensible Informationen enthalten.

9. Bei der Festlegung von technisch-organisatorischen Maßnahmen sowie von Handlungsanweisungen für das Löschen durch Überschreiben sind geeignete Softwarewerkzeuge anhand eines Kriterienkatalogs auszuwählen, zu bewerten und für die betreffenden Nutzer bereitzustellen. Die Anwendung der Werkzeuge ist stichprobenartig zu kontrollieren.

10. Defekte Datenträger, deren Daten nicht mehr mit Softwarewerkzeugen überschrieben werden können, sind durch mechanische oder thermische Zerstörung (Disketten, Festplatten) bzw. durch magnetische Durchflutung (Disketten) unbrauchbar zu machen. Um die Zuverlässigkeit der Verfahren zu sichern, ist eine korrekte Anwendung zu gewährleisten.

11. Müssen Datenträger ohne sicheres Löschen der Daten aus der Hand gegeben werden (z.B. Reparatur, Rückgabe an den Hersteller in der Garantiezeit), ist in Abhängigkeit von der Sensibilität der Daten durch vertragliche Regelungen und evtl. mit Schadensersatzansprüchen zu verhindern, dass unerwünschte Informationsflüsse stattfinden oder von Angreifern ausgenutzt werden. Ggf. ist auf Garantieansprüche zu verzichten.

Papier

Bei der Unkenntlichmachung von auf Papier gespeicherten Daten ist darauf zu achten, dass ein der Sicherheitsstufe entsprechender Schredder eingesetzt wird.

Ist kein der Sicherheitsstufe entsprechender Schredder vorhanden, so weist das BSI darauf hin, dass die Sicherheit auch durch eine größere Durchsatzmenge des vernichteten Materials erhöht werden kann. Diese erreicht man durch gezieltes Vermischen schutzbedürftiger und „offener“ Daten direkt vor dem Vorgang des Schredderns.

Durchstreichen einzelner Datensätze ist keine Methode zur sicheren Unkenntlichmachung von auf Papier gespeicherten Daten. Gleiches gilt für Überkleben, Weißen, Schwärzen und ähnliche Vorgänge.