DATENSCHUTZ

So funktioniert die DS-GVO-konforme Aktenvernichtung in der Kanzlei

von RAin Heike Mareck, externe Datenschutzbeauftragte, Dortmund

| Wann werden in Unternehmen Unterlagen, Dokumente, Papiere entsorgt? Wenn der Keller voll ist! Wie werden diese Unterlagen entsorgt? Unterschiedlich: Vertrauliche Unterlagen kommen in den versiegelten Container, der im Papierraum oder Keller steht. Bei als unbedenklich eingestuften Unterlagen, die personenbedingte Daten enthalten, ist das Entsorgen teilweise „unkomplizierter". Mit der DS-GVO sollten Kanzleien Akten datenschutzkonform entsorgen. AK Anwalt und Kanzlei gibt hierzu Tipps. |

1. Allgemeines

Problem: Einsichtbare Altunterlagen!

Das Entsorgen von weniger vertraulichen Unterlagen erfolgt in vielen Kanzleien unterschiedlich: Mal trifft sich ein Team spontan, weil der Keller voll ist. Mal werden die Unterlagen der Reinigungskraft an die Bürotür gestellt, damit diese sie abends zum versiegelten Container vor der Kanzlei bringt. Manchmal bleiben die Unterlagen auch bereitgelegt tagelang irgendwo zum Abholen – einsehbar für viele. So zuletzt beim LG Dortmund, wo alte Akten zum Entsorgen durch den Dienstleister kurzerhand einige Tage auf dem Gerichtsflur standen.

Papierakten sind ein ernsthaftes Risiko

Es verwundert daher nicht, dass Papierakten für zwei Drittel (63 Prozent) der mittelständischen, deutschen Unternehmer ein ernsthaftes Risiko für die Informationssicherheit darstellen. Zu diesem Ergebnis kamen PwC und Iron Mountain in ihrer 2014 durchgeführten Studie über den „Reifeindex zum Informationsrisiko". Fakt: Das sind mehr als doppelt so viele Befragte, als die, die externe Bedrohungen, wie Schadsoftware oder Hacker fürchten.

Zwar verfügen laut Studie fast alle deutschen Unternehmen (92 Prozent) über Richtlinien, die regeln, wie digitale Dokumente gespeichert und bereitgestellt werden. Aber nur 35 Prozent haben entsprechende Regelungen für Papierakten. Lediglich 41 Prozent legen Zugangsbeschränkungen zu Bereichen fest, in denen vertrauliche Informationen gelagert werden.

Team in der Kanzlei für umfangreiche Maßnahmen bestimmen

PRAXISTIPP | Legen Sie in Ihrer Kanzlei fest, wer für das Management sowohl von Papierdokumenten, als auch digitalen Daten verantwortlich ist. Übertragen Sie es nie nur auf eine Einzelperson – mindestens zwei Personen müssen hierfür zuständig sein. Bestimmen Sie feste Regeln zum Umgang mit der Datenvernichtung. Schulen Sie zumindest einmal Ihre Mitarbeiter. Ihr Team sollte festlegen, wann einmal im Jahr die Papierakten in der Kanzlei durchgesehen und geordnet werden, das heißt, welche im Büro bleiben, welche vernichtet und welche in ein sicheres, externes Archiv verlagert werden müssen.

2. Entscheidende Unterschiede beim Aktenvernichter

Orientieren Sie sich an der DIN-Norm 66399

Nach der im Oktober 2012 eingeführten DIN-Norm 66399 erfolgt die Vernichtung von Papierdokumenten in drei Schutzklassen und sieben Sicherheitsstufen. Sie sollten sich an diese Norm halten, da sie DS-GVO konformer ist. Die DIN 66399 spezifiziert drei Schutzklassen, nach denen die Datenträger hinsichtlich ihrer Schutzbedürftigkeit einzuordnen sind:

■ **Schutzklassen nach DIN 66399**

Schutzklassen	Beschreibung	Beispiele
Klasse 1 Normaler Bedarf für interne Daten	Der Schutz von personenbezogenen Daten muss gewährleistet sein. Andernfalls besteht die Gefahr, dass der Betroffene in seiner Stellung und seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.	Nicht Knowhow-relevante Korrespondenz, personalisierte Werbung, Kataloge, Wurfsendungen, Notizen
Klasse 2 Hoher Bedarf für vertrauliche Daten	Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt wird.	Knowhow-relevante Korrespondenz wie Angebote, Anfragen, Memos, Aushänge, Personaldaten
Klasse 3 Sehr hoher Bedarf für besonders geheime 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.	Verschlusssachen, Mandanteninformationen, Unterlagen der Geschäftsleitung

Sieben Sicherheitsstufen und ihre Beispiele

Zusätzlich gibt es sieben Sicherheitsstufen, die der TÜV Süd wie folgt aufführt:

1. **Allgemeine Daten** – Reproduktion mit einfachem Aufwand. Für Datenträger mit allgemeinen Daten, die unlesbar gemacht werden sollen, zum Beispiel Kataloge oder Prospekte etc.
2. **Interne Daten** – Reproduktion mit besonderem Aufwand. Für Datenträger mit internen Daten, die unlesbar gemacht werden sollen, zum Beispiel allgemeine interne Arbeitsanweisungen, Reiserichtlinien, Formulare.
3. **Sensible Daten** – Reproduktion mit erheblichem Aufwand. Für Datenträger mit sensiblen und vertraulichen Daten, zum Beispiel Angebote, Bestellungen mit Adressdaten von Personen.
4. **Besonders sensible Daten** – Reproduktion mit außergewöhnlichem Aufwand. Für Datenträger mit besonders sensiblen und vertraulichen Daten, zum Beispiel Personaldaten, Arbeitsverträge, Steuerunterlagen.
5. **Geheim zu haltende Daten** – Reproduktion mit zweifelhaften Methoden. Beispiel: für Datenträger mit geheim zu haltenden Daten, zum Beispiel medizinische Berichte, Konstruktionspläne, Strategiepapiere.
6. **Geheime Hochsicherheitsdaten** – Reproduktion technisch nicht möglich. Für Datenträger mit geheim zu haltenden Daten, wenn außergewöhnlich hohe Sicherheitsvorkehrungen einzuhalten sind, zum Beispiel Entwicklungsunterlagen.
7. **Top Secret Hochsicherheitsdaten** – Reproduktion ausgeschlossen. Für Datenträger mit streng geheim zu haltenden Daten, wenn höchste Sicherheitsvorkehrungen einzuhalten sind, zum Beispiel Daten aus geheimdienstlichen oder militärischen Bereichen.

PRAXISTIPP | Viele Aktenvernichter sind eher auf die geringeren Stufen 1 und 2 ausgelegt (Streifen und große Partikel). Diese genügen für die Aktenvernichtung nicht, wenn personenbezogene Daten betroffen sind. Nur Aktenvernichter mit Partikelschnitt und der Sicherheitsstufe 4 oder höher erfüllen die Kriterien der DS-GVO zur Vernichtung personenbezogener Daten. Einen guten Überblick gibt auch die Broschüre des TÜV Süd unter https://www.tuev-sued.de.

Nur Sicherheitsstufe 4 und höher ausreichend

3. Dienstleister übernimmt Vernichtung? Nur mit AV!

Vernichtet ein Dienstleister die Akten, muss bei zu vernichtenden Dokumenten mit personenbezogenen Daten stets beachtet werden, dass es sich hierbei um eine Auftragsverarbeitung (AV) handelt. Dies gilt unabhängig davon, ob der Dienstleister die Unterlagen vor Ort vernichtet oder sie zur Entsorgung abholt und an einem anderen Ort endgültig entsorgt.

Inhalte der Vertragsvereinbarung

Daher muss der Auftraggeber (Verantwortliche) nach Art. 28 Abs. 3 DS-GVO mit dem Auftragnehmer (Auftragsverarbeiter) einen Vertrag schließen. Der Vertrag muss die folgenden Mindestanforderungen regeln. Zudem sollte er einzelfallbezogen vertraglich ausgestaltet bzw. auf den jeweiligen Dienstleister und seine Tätigkeiten angepasst werden:

- Gegenstand und Dauer der Verarbeitung,
- Art und Zweck der Verarbeitung,
- Art der personenbezogenen Daten, Kreis betroffener Personen,
- Umfang der Weisungsbefugnisse,
- Pflichten und Rechte des Verantwortlichen,
- Pflichten des Auftragsverarbeiters:
  - Verarbeitung nach dokumentierter Weisung,
  - Wahrung der Vertraulichkeit bzw. Verschwiegenheit,
  - Ergreifung geeigneter Maßnahmen für die eigene Sicherheit der Verarbeitung,
  - Rechtmäßige Hinzuziehung von Subunternehmen,
  - Unterstützung des Verantwortlichen bei der Beantwortung von Anträgen betroffener Personen,
  - Unterstützung des Verantwortlichen bei der Einhaltung von dessen Pflichten aus Art. 32 bis 36 DS-GVO (Ergreifung geeigneter Maßnahmen für die Sicherheit der Verarbeitung, Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Durchführung einer Datenschutz-Folgenabschätzung, Konsultierung der Aufsichtsbehörde bei Verarbeitung mit hohen Risiken,
  - Löschung oder Rückgabe nach Beendigung des Auftrags,
  - Zurverfügungstellung von Informationen und Ermöglichung von Überprüfungen.

Wichtig ist auch eine Anlage zu den technischen und organisatorischen Maßnahmen (TOM), mit denen der Auftragnehmer Datenschutz und Datensicherheit der ihm überlassenen Daten gewährleistet.

4. Wer ist für was bei einer AV verantwortlich?

Auftraggeber behält Verantwortung für die Vernichtung

Auch nach Abschluss des Vertrags über die Auftragsverarbeitung behält der Auftraggeber die Verantwortung bei der Aktenvernichtung. Nach Art. 24 DS-GVO hat er dafür Sorge zu tragen, dass die Verarbeitung rechtmäßig erfolgt. Zudem muss er auch Art, Umfang, Umstände und Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Entsprechend muss er hierfür geeignete technische und organisatorische Maßnahmen umsetzen.

5. Auswahl und Kontrolle des Dienstleisters

Auftraggeber muss sich von den TOM des Auftragnehmers ein Bild machen

Der Auftraggeber trägt auch die Verantwortung für die Auswahl des Dienstleisters bzw. Verarbeiters. Er muss sich davon überzeugen, dass der Auftragnehmer ausreichende TOM getroffen hat, um den Schutz der ihm zugänglich gemachten Daten zu gewährleisten. Damit sichergestellt ist, dass die datenschutzrechtlichen Vorgaben auch tatsächlich vom Dienstleister erfüllt werden, muss der Auftragsverarbeiter nach Art. 28 DS-GVO hinreichende Garantien bieten.

■ Wo lauern weitere „datenschutzrelevante“ Gefahren?

Geräte/Umstände	Beschreibung
Kopierer und Faxgerät	Vergessene Papiere werden in den nebenstehenden Mülleimer geworfen oder vertrauliche Dokumente werden neben die Geräte gelegt, da der Bearbeiter nicht sofort erkennbar ist.
Festplatten	Werden häufig nicht fachgemäß überschrieben.
Auslagern der Aktenvernichtung an Entsorgungsunternehmen	Es erfolgt keine datenschutzgerechte Auswahl, das heißt, es wird der Erstbeste aus dem Telefonbuch genommen.
Mobiltelefon	Datenspeicher werden nicht überschrieben und formatiert. Bei Verlust des Mobiltelefons sofort sperren unter: 116 116. Hierunter erreichen Sie die zentrale Anlaufstelle zur Sperrung elektronischer Berechtigungen, die von der Bundesnetzagentur zur Sperrung elektronischer Medien wie Kredit- und EC-Karten, digitaler Signaturen, Krankenversicherungskarten, Mitarbeiter-Ausweisen, Kundenkarten oder sensibler Online-Berechtigungen eingerichtet wurde. Beim letzten Arbeitstag des Mitarbeiters wird häufig vergessen, das Gerät auf Werkseinstellungen zurückzustellen.
Navigationsgerät im Dienstwagen	Bei Privatnutzung: Private Routenplanungen oder Adressen, evtl. vorhandene SMS-Nachrichten und Anrufverläufe im Bordcomputer werden nicht gelöscht.