DATENSCHUTZ

So funktioniert die DSGVO-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, muss der Mülleimer herhalten. Nach Inkrafttreten der DSGVO müssen Kanzleien bei der Aktenvernichtung jedoch sehr viel mehr beachten als bisher. BBP gibt hierzu wertvolle Tipps. |

1. Management von Papierdokumenten und digitalen Daten

Problem: einsehbare Altunterlagen

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

Papierakten sind ein ernsthaftes Risiko

Dies ist sicherlich kein Einzelfall. Daher verwundert das Ergebnis einer von PwC und Iron Mountain in 2014 durchgeführten Studie über den „Reifeindex zum Informationsrisiko" wenig: Papierakten stellen für zwei Drittel (63 %) der mittelständischen deutschen Unternehmer ein ernsthaftes Risiko für die Informationssicherheit dar. Fakt ist: 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 %) über Richtlinien, die regeln, wie digitale Dokumente gespeichert und bereitgestellt werden, aber nur 35 % haben entsprechende Regelungen für Papierakten. Lediglich 41 % legen Zugangsbeschränkungen zu Bereichen fest, in denen vertrauliche Informationen gelagert werden.

Team in der Kanzlei für umfangreiche Maßnahmen bestimmen

PRAXISTIPPS |

- 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 für den Umgang mit der Datenvernichtung.
- Schulen Sie zumindest einmal Ihre Mitarbeiter.
- Ihr Team sollte festlegen, wann die Papierakten in der Kanzlei durchgesehen und geordnet werden, d. h., welche im Büro bleiben, welche vernichtet und welche in ein sicheres externes Archiv verlagert werden müssen. Dies sollte mindestens einmal im Jahr passieren.

2. Entscheidende Unterschiede beim Aktenvernichter

Nach der im Oktober 2012 eingeführten DIN-Norm 66399 erfolgt die Vernichtung von Papierdokumenten in 3 Schutzklassen. Sie sollten sich an diese Norm halten, da sie DSGVO-konform ist. Die 3 Schutzklassen ordnen die Datenträger hinsichtlich ihrer Schutzbedürftigkeit ein.

Orientieren Sie sich an der DIN-Norm 66399

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 Know-how-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.	Know-how-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

Zusätzlich gibt es 7 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, z. B. Kataloge oder Prospekte

2. **Interne Daten** – Reproduktion mit besonderem Aufwand. Für Datenträger mit internen Daten, die unlesbar gemacht werden sollen, z. B. allgemeine interne Arbeitsanweisungen, Reiserichtlinien, Formulare

Reproduktion mit besonderem Aufwand

3. **Sensible Daten** – Reproduktion mit erheblichem Aufwand. Für Datenträger mit sensiblen und vertraulichen Daten, z. B. Angebote, Bestellungen mit Adressdaten von Personen

4. **Besonders sensible Daten** – Reproduktion mit außergewöhnlichem Aufwand. Für Datenträger mit besonders sensiblen und vertraulichen Daten, z. B. Personaldaten, Arbeitsverträge, Steuerunterlagen

5. **Geheim zu haltende Daten** – Reproduktion mit zweifelhaften Methoden. Beispiel: für Datenträger mit geheim zu haltenden Daten wie medizinischen Berichten, Konstruktionsplänen, Strategiepapieren

Reproduktion mit zweifelhaften Methoden

6. **Geheime Hochsicherheitsdaten** – Reproduktion technisch nicht möglich. Für Datenträger mit geheim zu haltenden Daten, wenn außergewöhnlich hohe Sicherheitsvorkehrungen einzuhalten sind, z. B. Entwicklungsunterlagen

7. **Topsecret Hochsicherheitsdaten** – Reproduktion ausgeschlossen. Für Datenträger mit streng geheim zu haltenden Daten, wenn höchste Sicherheitsvorkehrungen einzuhalten sind, z. B. Daten aus geheimdienstlichen oder militärischen Bereichen

Reproduktion ausgeschlossen

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 DSGVO zur Vernichtung personenbezogener Daten. Einen guten Überblick erhalten Sie unter www.tuev-sued.de/fokus-themen/it-security/din-66399/din-66399-schutzklassen-und-sicherheitsstufen.

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. Daher muss der Auftraggeber (Verantwortliche) nach Art. 28 Abs. 3 DSGVO mit dem Auftragnehmer (Auftragsverarbeiter) einen Vertrag schließen.

Inhalt der Vertragsvereinbarung

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 den Art. 32 bis 36 DSGVO (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

Unterstützung des Verantwortlichen bei der Einhaltung von dessen Pflichten

MERKE | 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 AV behält der Auftraggeber die Verantwortung bei der Aktenvernichtung. Nach Art. 24 DSGVO hat er dafür Sorge zu tragen, dass die Verarbeitung rechtmäßig erfolgt. Zudem muss er auch Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedliche 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 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 DSGVO hinreichende Garantien bieten.

6. Weitere datenschutzrelevante Gefahren

Achten Sie auch auf die folgenden Gefahrenquellen für den Datenschutz:

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	Festplatten werden nicht fachgemäß überschrieben
Auslagern der Aktenvernichtung an Entsorgungsunternehmen	Es erfolgt keine datenschutzgerechte Auswahl, d. h., 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 ■ Am letzten Arbeitstag des Mitarbeiters wird häufig vergessen, das Gerät auf Werkseinstellungen zurückzusetzen
Navigationsgerät im Dienstwagen	Bei Privatnutzung: private Routenplanungen oder Adressen, eventuell vorhandene SMS-Nachrichten und Anrufverläufe im Bordcomputer werden nicht gelöscht

Keine datenschutzgerechte Auswahl

Private Daten werden nicht gelöscht