DATEN- UND AKTENVERNICHTUNG IN DER ANWALTSKANZLEI

MARIA WINKLER
mag. iur., Rechtskonsulentin, IT & Law Consulting GmbH, Zug

Stichworte: Berufsgeheimnis, Datensicherheit, Vernichtung von physischen Datenträgern, Löschung von elektronischen Daten, Outsourcing

Anwaltskanzleien müssen aufgrund des Berufsgeheimnisses sowie aufgrund von datenschutzrechtlichen Vorgaben bei der Bearbeitung der Daten und Akten ihrer Mandanten mit besonderer Sorgfalt vorgehen und durch geeignete Massnahmen sicherstellen, dass deren Vertraulichkeit gewährleistet wird. Dies gilt auch bei deren Vernichtung und unabhängig davon, ob sie in physischer oder in elektronischer Form vorhanden sind. Der vorliegende Artikel soll eine Übersicht vermitteln, welche Risiken bei der Aktenvernichtung zu beachten sind und welche Lösungsansätze in der Praxis verfügbar sind.

I. Einführung

Die anwaltliche Tätigkeit bringt aufgrund von diversen gesetzlichen Vorgaben und den daraus fliessenden Dokumentationspflichten eine grosse Menge an Akten von Mandanten aber auch von Mitarbeitenden, externen Dienstleistern etc. mit sich, die während ihres gesamten Lebenszyklus gemäss den gesetzlichen Vorgaben verwaltet werden müssen. Das Interesse, Dokumente zu vernichten, wenn sie nicht mehr aufbewahrt werden müssen, ist daher gross.

Die Vernichtung von physischen und elektronischen Dokumenten muss unter Beachtung der gesetzlichen Vorgaben erfolgen. So muss sichergestellt werden, dass die Dokumente erst nach Ablauf der anwendbaren gesetzlichen Aufbewahrungsfristen vernichtet werden,[1] und es muss gewährleistet werden, dass es bei der Vernichtung selbst nicht zu einer Verletzung des Berufsgeheimnisses oder von datenschutzrechtlichen Vorschriften kommt.

Im Folgenden wird zunächst kurz auf die Frage der zu beachtenden Aufbewahrungsfristen eingegangen und anschliessend werden praktische Empfehlungen für die Vernichtung von physischen und elektronischen Dokumenten gegeben.

II. Die Dauer der Aktenaufbewahrung

Neben den Akten von Mandanten bearbeitet eine Anwaltskanzlei in der Regel auch Personaldossiers sowie Verträge und Korrespondenzen mit externen Dienstleistern. Diese Dokumente müssen aufgrund verschiedener gesetzlicher Vorgaben für eine gewisse Zeit integritätssicher aufbewahrt werden. Erst danach dürfen diese Dokumente vernichtet werden.

Im Rahmen der Buchführungs- und Rechnungslegungspflicht[2] sind die Bücher und Buchungsbelege sowie der Geschäftsbericht und der Revisionsbericht zehn Jahre aufzubewahren, wobei die Aufbewahrungsfrist mit dem Ende des Geschäftsjahres zu laufen beginnt.[3] Die anwendbaren steuerrechtlichen Vorgaben kennen ebenfalls eine zehnjährige Aufbewahrungspflicht, die allerdings mit dem Ende des Kalenderjahres beginnt.[4] Zusätzlich zu beachten sind Verjährungsfristen, die bei mehrjährigen Mandaten oder langfristigen Vertragsverhältnissen mit Dritten wie beispielsweise Vermietern, IT-Dienstleistern etc. dazu führen können, dass die betreffenden Vertragsdokumente erst nach dem Ablauf von deren Gültigkeitsdauer in die zehnjährige Aufbewahrung übergehen.

Akten von Mandanten müssen gemäss der herrschenden Lehrmeinung ebenfalls zehn Jahre aufbewahrt werden.[5] Die Aufbewahrungsfrist für Mandantenakten beginnt allerdings erst mit der Beendigung des Mandats zu laufen. Befinden sich in den Akten noch Originaldokumente von Mandanten, dann dürfen diese nicht vernichtet werden. Sie sollten daher bereits bei Beendigung des Mandats

1 Siehe dazu die Ausführungen im nachfolgenden Kapitel II.
2 Seit dem Inkrafttreten der revidierten Buchführungs- und Rechnungslegungsvorschriften am 1. 1. 2013 unterliegen nicht nur juristische Personen sondern auch Personengesellschaften und Einzelunternehmen mit einem Jahresumsatz von mehr als CHF 500 000.– der Buchführungspflicht gemäss Art. 957 ff. OR.
3 Art. 958 f Abs. 1 OR.
4 Art. 70 i. V. m. Art. 42 MWStG sowie Art. 126 Abs. 3 DBG.
5 WOLFGANG STRAUB, Aufbewahrung und Archivierung in der Anwaltskanzlei, AJP 2010, S. 552, abrufbar auf www.swisslex.ch.

dem Mandanten zurückgegeben und nicht mit den übrigen Akten archiviert werden.

Aufgrund der datenschutzrechtlichen Bearbeitungsgrundsätze der Zweckbindung und der Verhältnismässigkeit[6] müssen Dokumente, die Personendaten enthalten, nach Ablauf der gesetzlichen Aufbewahrungsfrist vernichtet werden, sofern kein Rechtfertigungsgrund für eine längere Aufbewahrung geltend gemacht werden kann.[7] Bei Akten von Mandanten kommt als Rechtfertigungsgrund in erster Linie die Einwilligung der betroffenen Person infrage sowie ein überwiegendes eigenes Interesse der betroffenen Anwältin/des betroffenen Anwalts, wenn diese den Zugriff auf die Akten beispielsweise aus Beweisgründen oder für die Klärung von Interessenkonflikten bei späteren Mandaten noch weiter benötigen.[8] Bei der Beurteilung, ob das eigene Interesse an der Aufbewahrung der Akten tatsächlich das Interesse des Mandanten an einer Vernichtung seiner Akten überwiegt, muss eine Interessenabwägung vorgenommen werden. Beinhalten die Akten beispielsweise belastende Informationen, die den Mandanten schädigen könnten, dann wird sein Interesse an der Vernichtung schwerer wiegen als das Interesse der Anwältin/des Anwalts an einer weiteren Aufbewahrung, und die Akten müssen vernichtet werden. Dies insbesondere dann, wenn das Ziel, genügend Informationen für die Klärung von allfälligen Interessenkonflikten mit späteren Mandaten auch mit der Aufbewahrung von wenigen Informationen erreicht werden kann. Sollten die Akten länger als gesetzlich vorgesehen aufbewahrt werden, dann müssen zudem die Zugriffsberechtigungen auf die Personen eingeschränkt werden, die diese zur Abklärung von Interessenkonflikten benötigen.

III. Die Vernichtung von Akten

1. Anforderungen an die Vernichtung von Akten

Beim Vernichtungsvorgang selbst müssen die Akten durch *angemessene technische und organisatorische Massnahmen* vor einer unbefugten Bearbeitung geschützt werden.[9] Bei der Vernichtung darf es zudem nicht zu einer Verfälschung oder zu einer ungeplanten Vernichtung von noch aufbewahrungspflichtigen Akten kommen.[10]

Bei der Bestimmung, ob die geplanten oder ergriffenen Massnahmen angemessen im Sinn der datenschutzrechtlichen Vorgaben sind, müssen insbesondere die *Risiken für die betroffenen Personen,* der *Stand der Technik* sowie der mögliche *Nutzen eines Missbrauchs der Daten* für einen Dritten mit berücksichtigt werden. Ist Letzterer gross und stehen grundsätzlich technische Möglichkeiten einer Wiederherstellung von bereits vernichteten Akten bzw. Daten zur Verfügung, dann ist davon auszugehen, dass sich ein Dritter auch die Mühe machen wird, die Daten zu rekonstruieren. Die gewählte Vernichtungsmethode muss daher die Rekonstruktion entweder generell verhindern oder nur mit einem so grossen Aufwand ermöglichen, dass die Kosten den potenziellen Nutzen eines Missbrauchs übersteigen.[11]

Eine Anwaltskanzlei muss aufgrund des anwaltlichen Berufsgeheimnisses bei der Aktenvernichtung mit *besonderer Sorgfalt* vorgehen, da das Berufsgeheimnis nicht nur durch eine aktive Bekanntgabe, sondern bereits durch die blosse Möglichkeit der Kenntnisnahme der geschützten Information durch Unberechtigte verletzt werden kann.[12] Es muss daher gewährleistet werden, dass es während des Vernichtungsvorgangs sowie danach nicht zu einer Offenlegung von Akten an unberechtigte Dritte kommen kann.

Die Vernichtung von Akten muss daher so erfolgen, dass diese weder als Ganzes noch in Teilen rekonstruiert werden können.[13] Elektronische Akten müssen unwiderruflich und unumkehrbar gelöscht werden.[14] In den folgenden Abschnitten wird erläutert, welche Möglichkeiten für die Vernichtung von elektronischen und physischen Akten in der Praxis zur Verfügung stehen.

2. Die Vernichtung von Papierakten und von Datenträgern

Es kann heute davon ausgegangen werden, dass Papierakten und Datenträger, die Daten von Mandanten enthalten, in Anwaltskanzleien nicht mit dem normalen Abfall entsorgt werden. Häufig werden die Papierakten sowie CD und ähnliche Datenträger in der Anwaltskanzlei selbst geschreddert. Auf dem Markt werden dazu zahlreiche verschiedene Modelle von *Aktenvernichtern* angeboten, die aber nicht alle zur Vernichtung von vertraulichen Akten und Datenträgern geeignet sind. Werden Papierakten oder Datenträger nicht fachgerecht geschreddert, dann können die darin enthaltenen Informationen mit mehr oder weniger Aufwand wiederhergestellt werden.

Zur Bestimmung, ob ein Aktenvernichter für die vertrauliche Vernichtung von Papierakten und Datenträgern geeignet ist, kann die *Norm DIN 66399:2012 «Vernichtung von Datenträgern»* konsultiert werden.[15] Diese Norm definiert drei Schutzklassen und sieben Sicherheitsstufen. Je nach Schutzbedarf der zu vernichtenden Daten erfolgt die Zuordnung zu einer der drei Schutzklassen. Akten von Anwaltskanzleien werden der höchsten Schutzklasse (Schutzklasse 3) zuzuordnen sein. Für jede Schutzklasse

6 Art. 4 Abs. 2 und 3 DSG.
7 Art. 13 DSG.
8 Siehe dazu auch STRAUB, S. 547 ff.
9 Art. 7 DSG i. V. m. Art. 8 ff. VDSG.
10 Art. 8 Abs. 1 VDSG.
11 EDÖB, Datenvernichtung.
12 STEFAN TRECHSEL/HANS VEST, Schweizerisches Strafgesetzbuch, Praxiskommentar, Kommentar zu Art. 321 StGB, Rz. 23.
13 Erläuterungen des EDÖB zur Datenvernichtung, abrufbar auf www.edoeb.admin.ch/datenschutz/00683/00803/00818/index.html?lang=de, besucht am 3. 6. 2016.
14 Bundesamt für Sicherheit in der Informationstechnologie (BSI), IT-Grundschutzhandbuch, M 2.515 Datenschutzgerechte Löschung/Vernichtung, abrufbar auf https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02515.html, besucht am 3. 6. 2016.
15 Die Norm kann auf der Website des Deutschen Instituts für Normung e. V. auf www.din.de bezogen werden.

benennt die Norm wiederum die zugehörigen Sicherheitsstufen und damit die Grösse der von den Aktenvernichtern erzeugten Partikeln.[16]

In der *Norm DIN 66399:2012 Teil 2 «Anforderungen an Maschinen zur Vernichtung von Datenträgern»* werden abhängig von der Sicherheitsstufe und der Art des Datenträgers die Anforderungen an die Geräte festgelegt. Grundsätzlich kann gesagt werden, dass die Sicherheit der Vernichtung umso grösser ist, je kleiner die Partikelgrösse ist, wobei aber nicht alle Geräte für die Vernichtung aller Datenträger gleich geeignet sind. Für die Vernichtung von vertraulichen Papierakten sollte mindestens ein Aktenvernichter mit einer Schutzstufe P-5 verwendet werden.

Bei einer grossen Menge von zu vernichtenden Akten werden diese häufig an ein externes Unternehmen zur Vernichtung weitergegeben. Die Papierakten werden dem externen Dienstleister in verschlossenen Behältern übergeben, die dieser in der Regel selbst zur Verfügung stellt. Die Behälter werden in vertraglich vereinbarten Zeitabständen abgeholt und durch das externe Unternehmen vernichtet.[17]

Auch einige Müllverbrennungsanlagen bieten die Möglichkeit, die Papierakten persönlich zur Müllverbrennung zu bringen und die Vernichtung zu überwachen. Dieses Vorgehen dürfte für die Vernichtung vertraulicher Akten grundsätzlich tauglich sein, sofern die Mitarbeitenden, die die Akten entsorgen, ausreichend geschult sind.

3. Die Vernichtung von elektronischen Akten

Viele Anwaltskanzleien führen ihre Akten heute nur mehr elektronisch oder es werden sogenannte hybride Dossiers geführt, was bedeutet, dass Akten zu einem Dossier sowohl in physischer als auch in elektronischer Form vorliegen. Zudem liegen elektronische Kopien von Akten in der Regel auf verschiedenen mobilen Geräten wie beispielsweise auf Laptops oder auf anderen Datenträgern wie CD, DVD, Festplatten etc.

Die Vernichtung elektronischer Akten muss so erfolgen, dass eine Rekonstruktion unmöglich ist oder zumindest mit hoher Wahrscheinlichkeit ausgeschlossen werden kann. Das einfache Löschen der Daten sowie die Formatierung der Datenträger reichen nicht aus, um vertrauliche Daten sicher zu löschen. Das BSI empfiehlt, die Daten mehrmals unter Verwendung von zufälligen Datenmustern zu überschreiben.[18]

Ist eine definitive Löschung von Daten nicht möglich, dann müssen andere Massnahmen ergriffen werden. So werden beispielsweise bei einer rein elektronischen Aktenführung häufig sogenannte unveränderbare Datenträger wie beispielsweise WORM-Datenträger verwendet. Der Vorteil von WORM-Speichern liegt in der erhöhten Integrität der darauf gespeicherten Daten, die dadurch im Streitfall eine hohe Beweiskraft haben. Allerdings hat diese Art der Datenspeicherung den Nachteil, dass die Daten nicht mehr selektiv gelöscht werden können. Eine Löschung der Daten kann in der Regel nur durch eine Vernichtung des ganzen Datenträgers erfolgen. Der Datenschutzbeauftragte des Kantons Zürich empfiehlt daher, nur Daten mit ähnlichen Aufbewahrungsfristen auf demselben WORM-Datenträger zu speichern.[19]

Eine Vernichtung eines Datenträgers erfolgt durch physikalisches Zerstören, beispielsweise indem dieser mechanisch oder thermisch zerstört wird. Dies ist immer dann zu empfehlen, wenn der Datenträger mit den Daten mit entsorgt werden soll oder, wie im Fall der auf einem WORM-Datenträger gespeicherten Daten, mit entsorgt werden muss. Auch dabei muss beachtet werden, dass die Informationen bei einer Zerkleinerung des Datenträgers je nach Partikelgrösse wiederhergestellt werden können. Für die Auswahl eines geeigneten Verfahrens kann wiederum auf die Empfehlung des BSI verwiesen werden, das für verschiedene Datenträger, abhängig von der Sensibilität und vom Schutzbedarf der darauf gespeicherten Daten, geeignete Vernichtungsmethoden vorschlägt.[20]

Können die Daten nicht sofort sicher gelöscht werden, muss das Risiko eines unbefugten Zugriffs auf diese Daten bis zur Vernichtung durch angemessene technische und organisatorische Massnahmen soweit als möglich reduziert werden. Dies wäre beispielsweise der Fall, wenn sich auf einem WORM-Datenträger zu vernichtende Daten befinden, dieser aber noch weiter verwendet wird.

Der Datenschutzbeauftragte des Kantons Zürich empfiehlt verschiedene Massnahmen, die sich zur Reduktion der entsprechenden Risiken eignen. Dazu zählen die Anonymisierung, die Vernichtung der Entschlüsselungsschlüssel, die Sperrung von Zugriffen, die Pseudonymisierung von Daten sowie die Löschung von Referenzen.[21] Sollen Daten *anonymisiert* werden, muss ein Vorgehen gewählt werden, das den Personenbezug unumkehrbar und unwiderruflich entfernt. Im Zeitalter von Big Data und einer ständig wachsenden Rechnerleistung stellt die korrekte Anonymisierung allerdings eine zunehmende Herausforderung dar, da ein erhebliches Risiko besteht, dass diese durch das Zusammenführen mehrerer an sich anonymer

---

16 Ausführlichere Informationen sind auf der Website des BSI zu finden: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02435.html, besucht am 3. 6. 2016.

17 Siehe dazu die weiteren Ausführungen zur Aktenvernichtung durch Dritte im Kapitel IV.

18 BSI, Datenschutzgerechte Löschung/Vernichtung, abrufbar auf https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02515.html, besucht am 6. 6. 2016.

19 Datenschutzbeauftragter des Kantons Zürich, Merkblatt Vernichtung elektronischer Daten, abrufbar auf https://dsb.zh.ch/internet/datenschutzbeauftragter/de/ueber_uns/formulare_und_merkblaetter/_jcr_content/contentPar/form/formitems/merkblatt_vernichten/download.spooler.download.1462802855676.pdf/Merkblatt+Vernichten+elektronischer+Daten+V1.0.pdf, besucht am 6. 6. 2016.

20 M 2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten, zu finden auf https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02167.html, besucht am 6. 6. 2016.

21 DSB Zürich, Merkblatt Vernichtung elektronischer Daten.

Datenbestände de-anonymisiert werden können.[22] Bei einer *Pseudonymisierung* werden die Daten, die Rückschlüsse auf eine konkrete Person zulassen, durch ein Pseudonym, beispielsweise eine Zahl, ein Zeichen oder einen künstlich erzeugten Namen, ersetzt. Da der Personenbezug über den Pseudonymisierungsschlüssel wiederhergestellt werden kann, handelt es sich aber immer noch um Personendaten, die gemäss den Vorgaben des Datenschutzgesetzes bearbeitet werden müssen. Gewisse Speichermedien lassen zwar keine Löschung der Daten zu, erlauben aber die *Löschung von Referenzen* zu diesen Daten, sodass diese in der Folge durch Suchmechanismen nicht mehr auffindbar sind. Da die Daten selbst noch vorhanden sind, handelt es sich nicht um eine definitive Vernichtungsmethode, auch wenn damit sichergestellt werden kann, dass mit den in den Anwaltskanzleien üblicherweise zur Verfügung stehenden Massnahmen ein Zugriff auf die Daten unmöglich ist. Da aber davon auszugehen ist, dass mit den entsprechenden technischen Mitteln und bei einem hohen Wert der Daten für externe Dritte eine Rekonstruktion erfolgen kann, kann eine unwiderrufliche Löschung wohl nur durch die Vernichtung des Datenträgers selbst erfolgen.

Die Frage, ob bei einer Vernichtung von Daten diese auch von *Backups* gelöscht werden müssen, gibt in der Praxis immer wieder Anlass zu Diskussionen. Die Autorin dieses Artikels vertritt grundsätzlich die Auffassung, dass eine Manipulation an einem Backup nur dann durchgeführt werden sollte, wenn diese unbedingt erforderlich ist, um die betroffene Person vor schwerwiegenden Folgen eines Missbrauchs der Daten zu schützen oder wenn dies aus Geheimhaltungsgründen zwingend erforderlich ist. Im Normalfall wird es auch für eine Anwaltskanzlei ausreichend sein, wenn sichergestellt wird, dass bei einem allfälligen Einspielen eines Backups die bereits gelöschten Daten unverzüglich und sicher gelöscht werden, sodass diese nicht mehr in die produktiven Systeme überführt werden. Wenn es sich allerdings um besonders sensible Daten handelt, an denen Dritte ein sehr hohes Interesse haben oder haben könnten, dann ist zu empfehlen, die auf den produktiven Systemen oder dem Archiv gelöschten Daten auch auf den Backup-Medien zu löschen. Beim Löschvorgang muss allerdings sichergestellt werden, dass die übrigen Daten, die sich auf dem Backup-Medium befinden, nicht verändert oder versehentlich gelöscht werden. Der Vorgang muss daher nicht nur sehr gut geplant, sondern auch dokumentiert werden.

Wenn die Mitarbeitenden der Anwaltskanzlei vertrauliche Daten auf ihren privaten mobilen Devices wie Smartphones oder Tablet-PC speichern und bearbeiten, dann hat die Anwaltskanzlei über diese Geräte keine direkte Verfügungsgewalt. Scheiden Mitarbeitende aus dem Unternehmen aus oder geht das mobile Gerät verloren, kann eine Vernichtung der vertraulichen Informationen nur sichergestellt werden, wenn auf dem mobilen Gerät zuvor eine entsprechende Software installiert wurde, die es dem Unternehmen erlaubt, die Geräte zu kontrollieren. Die Installation der Software auf dem privaten Gerät setzt aber die vorgängige Einwilligung der Mitarbeitenden voraus, und eine Löschung ist grundsätzlich nur möglich, wenn das Gerät selbst eingeschaltet ist. Aus Risikoüberlegungen ist es daher zu empfehlen, in Anwaltskanzleien die Verwendung privater Mobilgeräte im Rahmen von sogenannten *«Bring Your Own Device»*-Projekten zu verzichten. Befinden sich die Mobilgeräte im Eigentum des Arbeitgebers, kann dieser auch darüber verfügen und insbesondere die zu beachtenden Sicherheitsvorgaben verbindlich regeln und durchsetzen.

IV. Datenvernichtung durch Dritte

Sofern keine gesetzliche oder vertragliche Geheimhaltungspflicht besteht, die das Outsourcing der Datenbearbeitung an einen Dritten verbieten würde, darf eine Anwaltskanzlei externe Dienstleister zur Bearbeitung ihrer Daten beiziehen. Das Berufsgeheimnis selbst verbietet es der Anwaltskanzlei nicht per se, die Datenbearbeitung an Dritte auszulagern. Hilfstätigkeiten, bei denen eine Weisungsbefugnis der Anwaltskanzlei besteht, können ausgelagert werden.[23] Sie muss aber durch geeignete Massnahmen sicherstellen, dass die damit verbundenen Risiken für die betroffene Person angemessen reduziert werden und die Geheimhaltung der Informationen weiterhin gewährleistet bleibt. So muss vertraglich sichergestellt werden, dass der Dienstleister die Daten nur für den vertraglich vereinbarten Zweck verwendet und die Datensicherheit gewährleistet ist.[24]

Wenn die elektronischen Daten der Anwaltskanzlei bei einem externen Dienstleister gespeichert werden, dann muss mit diesem auch der Prozess der Datenvernichtung verbindlich geregelt und dokumentiert werden. Dies unabhängig davon, ob die Daten der Anwaltskanzlei beim externen Dienstleister auf dessen Speichermedien gespeichert werden oder sich auf einem eigenen Datenträger der Anwaltskanzlei befinden, der im Rechenzentrum des Dienstleisters gehostet wird. Neben den Voraussetzungen und Zuständigkeiten der Löschung von Dokumenten und Daten bzw. der Rückgabe oder Vernichtung des Speichermediums müssen auch die anzuwendenden Löschverfahren bzw. die dabei einzuhaltenden Sicherheitsvorgaben verbindlich geregelt werden. Dabei sollten nicht nur die aufgrund des Ablaufs der Aufbewahrungsfristen von Dokumenten regelmässig stattfindenden Löschungen geregelt werden sondern auch die Vernichtung oder Rückgabe der Daten oder Datenträger bei Beendigung des Vertragsverhältnisses.

---

22 EDÖB, Erläuterungen zu Big Data, abrufbar auf www.edoeb.admin.ch/datenschutz/00683/01169/01344/index.html, besucht am 6. 6. 2016.

23 Siehe dazu insbesondere BRUNO BAERISWYL, Stämpflis Handkommentar 2015, Kommentar zu Art. 10a DSG RZ 35, sowie DAVID ROSENTHAL, Handkommentar zum Datenschutzgesetz, Kommentar zu Art. 10a DSG, Rz. 102 ff.

24 Art. 10a DSG.

NÜTZLICHE LINKS

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)
Datenvernichtung
www.edoeb.admin.ch/datenschutz/00683/00803/00818/index.html?lang=de

Datenschutzbeauftragter des Kantons Zürich
Merkblatt Vernichtung elektronischer Daten
https://dsb.zh.ch/internet/datenschutzbeauftragter/de/ueber_uns/formulare_und_merkblaetter/_jcr_content/contentPar/form/formitems/merkblatt_vernichten/download.spooler.download.1462802855676.pdf/Merkblatt+Vernichten+elektronischer+Daten+V1.0.pdf

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Datenschutzgerechte Löschung/Vernichtung
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02515.html

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02167.html

Bundesamt für Sicherheit in der Informationstechnik (BSI)
M 2.435 Auswahl geeigneter Aktenvernichter
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02435.html

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Vernichtung von Datenträgern durch externe Dienstleister
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02436.html

Soll die Vernichtung der physischen oder elektronischen Akten an einen Dritten ausgelagert werden, liegt es in der Verantwortung der Anwaltskanzlei, sich vor Vertragsabschluss über den genauen Ablauf der Vernichtung sowie die dabei angewandten Verfahren zu informieren und entsprechende vertragliche Vereinbarungen zu treffen. Die Übergabe der Akten an den externen Dienstleister muss dokumentiert werden.

Bei jeglicher Auslagerung der Datenbearbeitung muss sich die Anwaltskanzlei ein Kontrollrecht einräumen lassen und dieses wenn nötig auch ausüben. Kann das externe Unternehmen eine Zertifizierung im Bereich der Informationssicherheit und/oder des Datenschutzes nachweisen, dann kann die Anwaltskanzlei sich darauf verlassen, dass ein entsprechendes Managementsystem besteht und unter anderem gewährleistet ist, dass der externe Dienstleister die Verantwortlichkeiten und Prozesse im Zusammenhang mit den betreffenden Datenbearbeitungen systematisch geregelt hat. Allerdings sind Datenschutz- oder Datensicherheitsverletzungen auch bei einer Zertifizierung nicht ausgeschlossen. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte betont daher auch, dass sich ein Auftraggeber in einem solchen Fall nicht alleine auf ein Zertifikat verlassen darf. Vielmehr muss die Datensicherheit durch technische und organisatorische Massnahmen gewährleistet werden. Als Beispiele nennt er die Protokollierung der Arbeitsschritte des Auftragnehmers, die Stichprobenkontrollen (was ein entsprechendes vertragliches Kontrollrecht voraussetzt) oder vertraglich vereinbarte Konventionalstrafen für Datenschutzverletzungen.[25] Empfehlenswert ist es, zusätzlich zu einem Kontrollrecht auch eine Informationspflicht des Dienstleisters bei Datenschutz- und Datensicherheitsvorfällen vertraglich festzulegen.

V. Empfehlungen

Da eine nicht gesetzeskonforme Vernichtung der Akten mit grossen Risiken sowohl für die betroffenen Personen als auch für die betroffenen Anwältinnen und Anwälte verbunden ist, sollte der *Prozess der Aktenvernichtung* in der Anwaltskanzlei geregelt und die involvierten Mitarbeitenden sollten entsprechend geschult werden.

Abhängig von der Vertraulichkeit der zu vernichtenden Akten müssen dabei Geräte und Löschverfahren zur Anwendung kommen, die eine sichere Vernichtung gewährleisten.

Schreddert die Anwaltskanzlei vertrauliche Papierakten selbst, sollten *Aktenvernichter* verwendet werden, die mindestens die Sicherheitsstufe P-5 aufweisen.

Elektronische Akten müssen für eine sichere Löschung mehrfach unter Verwendung von zufälligen Datenmustern *überschrieben* werden. Können elektronische Akten nicht sofort und unwiderruflich gelöscht werden, müssen bis zum Löschzeitpunkt Massnahmen ergriffen werden, mit denen die Risiken einer unbefugten Bearbeitung angemessen reduziert werden. Als Beispiele können hier die Anonymisierung der Daten oder die Löschung von Referenzen genannt werden.

Zieht die Anwaltskanzlei *externe Dienstleister* bei, dann bleibt sie für die korrekte Vernichtung verantwortlich. Daher sollte bei der Auswahl des externen Partners sorgfältig vorgegangen werden. Dienstleister, die ihre Datenbearbeitungsprozesse standardisiert und dokumentiert haben, sollten bevorzugt werden. Die Vereinbarung von Kontrollrechten und Informationspflichten sowie von Konventionalstrafen bei Datenschutz- und Datensicherheitsvorfällen dient der Wahrnehmung der eigenen Verantwortung bei einem allfälligen Verstoss gegen die vertraglich vereinbarten Sicherheitsmassnahmen.

25 EDÖB, Datenvernichtung.

Kompaktes Nachschlage-werk

Datenschutzgesetz (DSG)

Bruno Baeriswyl, Kurt Pärli (Herausgeber)
Dominika Blonski, Marco Fey, Sandra Husi-Stämpfli, Claudia Mund, Beat Rudin, Monique Sturny, Amédéo Wermelinger (Autoren)

Juli 2015, CHF 165.–

Stämpflis Handkommentar SHK, 474 Seiten, gebunden, 978-3-7272-2539-0

Das Datenschutzrecht gewinnt zunehmend an Bedeutung in der Rechtspraxis. Als Querschnittsmaterie beeinflusst es alle Rechtsgebiete. Das Datenschutzgesetz (DSG) stellt dabei die Rahmenbedingungen auf für die Datenbearbeitungen durch private Personen und die Bundesverwaltung.

Der Handkommentar zum Datenschutzgesetz kommt dem Bedürfnis aus der Praxis nach, über ein kompaktes Nachschlagewerk verfügen zu können, das die wesentlichen Rechtsfragen umfassend darstellt und dabei klar und übersichtlich bleibt. Er berücksichtigt die einschlägige Lehre und Rechtsprechung. Die Ausführungen werden mit zahlreichen Beispielen aus der Praxis illustriert. Damit ist der Handkommentar ein unentbehrliches Arbeitsinstrument für Juristinnen und Juristen, die datenschutzrechtliche Fragen beantworten müssen, sowie für Praktikerinnen und Praktiker, die kurze, verständliche und fundierte Ausführungen zu den Bestimmungen des DSG suchen.

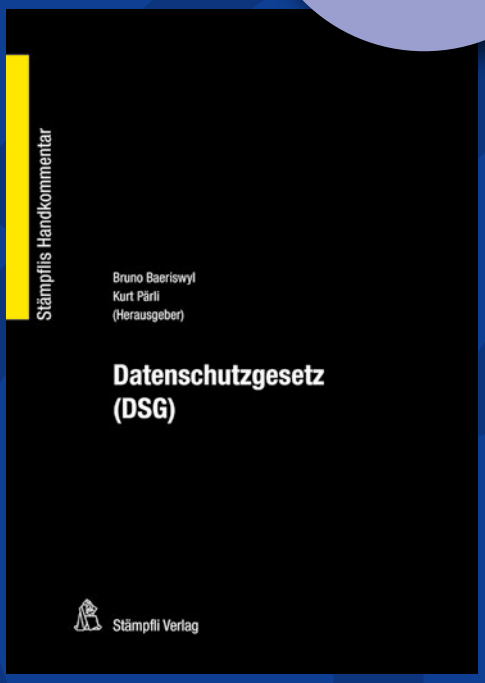
Stämpfli Verlag

Stämpfli Verlag AG
Wölflistrasse 1
Postfach
CH-3001 Bern

Tel. +41 31 300 66 44
Fax +41 31 300 66 88

verlag@staempfli.com
www.staempfliverlag.com

Bestellen Sie jetzt



Ich bestelle ____ Ex.

Name, Vorname

Strasse/PLZ,Ort

Datum, Unterschrift

1400-94 /16

www.staempfliverlag.com/anwaltsrevue