Hohe Anforderungen an die Beauftragung von Akten- und Datenträgervernichtung

Sehr geehrte Datenschutz-Kunden,

in meiner heutigen Rundmail geht es um die datenschutzkonforme Beauftragung von Dienstleistern mit der Akten- und Datenträgervernichtung.

Wir erinnern uns: Zur Datenverarbeitung entsprechend EU-DSGVO gehören alle Vorgänge von der Erhebung bis zur Löschung personenbezogener Daten. Ausdrücklich einbezogen sind alle Dokumente, deren Inhalt in "... einem Dateisystem gespeichert sind oder gespeichert werden sollen." Es stellt sich auch nicht mehr die Frage, ob diese Daten aus einem automatisierten oder nicht automatisierten Verfahren stammen (vgl. Art. 2 Abs. 1 EU-DSGVO). Papierdokumente, die aus einem IT-technischen Verfahren kommen oder mit dem Zweck erstellt wurden, in einem solchen weiterverarbeitet zu werden, unterliegen damit vollständig den Anforderungen der EU-DSGVO, wenn sie personenbezogene Daten enthalten. Dies gilt gleichermaßen für Datenträger, die personenbezogene Daten beinhalten, auch wenn es sich "nur" um manuell erstellte Briefe oder andere Textdateien handelt. Die Vernichtung entspricht daher einer Datenlöschung und ist Bestandteil der Datenverarbeitung durch den Verantwortlichen.

Für die sachgerechte Entsorgung von Dokumenten und Datenträgern werden häufig externe Dienstleister beauftragt. Ist es bei der Vernichtung von Datenträgern noch weitgehend selbstverständlich, dass hier erhöhte Anforderungen an die Beauftragung gestellt werden, so wurde in der Vergangenheit bei der Vernichtung von Papierdokumenten gerne einmal "ein Auge zugedrückt" - allerdings nur vom Auftraggeber und Auftragnehmer, nicht von den Aufsichtsbehörden. Im konkreten Fall ging es darum, dass der Verantwortliche ein Unternehmen mit der Aktenvernichtung beauftragt hatte, welches diese vor Ort auf bzw. unmittelbar vor dem Firmensitz des Verantwortlichen durchgeführt hat. Weil der gesamte Vorgang (Verbringen der Akten zum Fahrzeug mit dem Schredder, Einwurf der Akten in das Gerät etc.) vom Personal des Verantwortlichen beaufsichtigt wurde, stellte sich die Frage, ob für den Vorgang die hohen Maßstäbe einer Auftragsverarbeitung anzulegen waren.

Um Rechtssicherheit zu erlangen, den Kunden aber nicht mit zu hohen Anforderungen zu belasten, habe ich den Vorgang mit einem Vertreter des Bayerischen Landesamtes für Datenschutzaufsicht diskutiert (Die Datenschutzbehörden der Länder sind ständig in Kontakt zueinander und stimmen Ihrer Einschätzungen ab, so dass nicht zu erwarten ist, dass in anderen Bundesländern abweichende Anforderungen gestellt werden.). Die Antwort ist eindeutig: Auch ein Verarbeitungsvorgang, der vollständig unter der Kontrolle von eigenem Personal durch externe Dienstleister durchgeführt wird, begründet eine Auftragsverarbeitung nach Art. 28 EU-DSGVO. Unter dem Aktenzeichen LDA-1085-2922/20 teilt die Aufsichtsbehörde mit: "... Es ist doch auch bei dieser Gestaltung so, dass die 'eigentliche Arbeit an den Daten' durch Personal des Dienstleisters erledigt wurde; Dass

Volker Baron (Dipl.-Geograph / IT-Systemelektroniker) – **Tel.:** +49 89 18923500 – **Fax:** +49 89 18923501
Büro: Haydnstraße 2, 80336 München – **E-Mail:** volker.baron@baron-consult.de – **Internet:** www.baron-consult.de
Finanzamt München I, USt-ID: DE 216791626
Bankverbindung: Münchner Bank eG, IBAN: DE84 7019 0000 0000 3389 15, BIC: GENODEF1M01

Auftraggeber-Personal dies beaufsichtigt hat, ändert daran nichts. Denn es bleibt dabei, dass es Fremdpersonal war, das 'Hand angelegt' hat. ... Daher liegt unseres Erachtens hier für das Shreddern Auftragsverarbeitung vor."

Was bedeutet dies konkret für Sie als Verantwortlichem, wenn Sie eine Datenvernichtung beauftragen?

1. Der Dienstleister muss nachweisbar sorgfältig ausgewählt werden. Er muss "... hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet." (Art. 28 Abs. 1 EU-DSGVO). Ein geprüftes Qualitätsmanagementsystem beim Anbieter kann hier also ein Kriterium für die Auswahl sein, eine Zertifizierung entsprechend DIN 66399 ein weiteres. Auch ein vernünftiger Internet-Auftritt mit Impressum, Datenschutzerklärung etc. ist eventuell ein Indiz für eine seriöse Firma, genauso wie die Verwendung von Briefpapier mit vollständigen Firmenangaben. Auch die Mitgliedschaft in Verbänden oder einer Innung kann die Auswahl beeinflussen. In jedem Fall gilt: Bitte dokumentieren Sie, warum Sie einen bestimmten Dienstleister ausgewählt haben.

2. Bestehen Sie auf einer korrekten Vertragsgrundlage für die Beauftragung. Ein Vertrag zur Auftragsverarbeitung muss zwingend bestimmte Mindestinhalte aufweisen. Tut er dies nicht, wäre die Übergabe der Akten mit einer unerlaubten Offenbarung an Dritte gleichzusetzen, also mit einem Vorgang, der eindeutig bußgeldbewährt ist. Zu den zwingend erforderlichen Bestandteilen gehört insbesondere auch die Anlage, in der der Dienstleister die technisch-organisatorischen Maßnahmen beschreibt, unter denen die Dienstleistung erbracht wird. Ein Vertragsmuster, jedoch ohne den erforderlichen Anhang, finden Sie z. B. auf der Internet-Präsenz des LDA-Bayern: https://www.lda.bayern.de/media/muster/formulierungshilfe_av.pdf). Das bedeutet nicht, dass Sie den Vertrag für den Dienstleister ausarbeiten müssen. Das Muster soll Ihnen lediglich helfen, die Eignung und Vollständigkeit des Vertrags zu überprüfen, der Ihnen vom Dienstleister angeboten wird.

3. Dokumentieren Sie für sich, welche Arten von Unterlagen vernichtet wurden (z. B. "Belege und Geschäftsbriefe der Jahrgänge von ... bis ...", "Personalakten von Personen, die vor dem ... aus dem Unternehmen ausgeschieden sind.". Ich empfehle sogar, auch den Lieferschein oder einen anderen Nachweis des Dienstleisters in Ihren Datenschutzunterlagen aufzubewahren.

BITTE BEDENKEN SIE: Als Auftraggeber bleiben Sie datenschutzrechtlich verantwortlich für die Leistungen, die ein Auftragsverarbeiter erbringt! Unterläuft ihm ein Fehler und es kommt zu einer Datenschutzpanne, so können Sie aus der Haftung nur dann entlassen werden, wenn Sie nachweisen können, dass der Dienstleister die Verarbeitung entgegen den vertraglichen Vereinbarungen und den zugesicherten technisch-organisatorischen Maßnahmen durchgeführt hat.

München, 2020-07-03

Volker Baron