Aufbewahrung und Archivierung von Daten unter der DSGVO

Einleitung

Im Hinblick auf die Speicherung und Löschung von Daten gibt es die Redewendung „Gelöschte Daten sind die sichersten Daten", die häufig im Zusammenhang mit der Festlegung von Aufbewahrungsfristen zitiert wird. Tatsächlich ist das Prinzip Speicherbegrenzung gem. Art. 5 Abs. 1 lit. e) DSGVO einer der zentralen Grundsätze des Datenschutzrechts. Personenbezogene Daten dürfen nur so lange gespeichert werden, wie dies für die verfolgten Zwecke erforderlich ist. Sobald die Daten nicht länger benötigt werden, sind sie zu löschen. Die Regelung zur Löschung von Daten gem. Art. 17 Abs. 1 lit. a) DSGVO greift diese Vorgabe explizit auf. Durch diese Vorgabe soll unter anderem verhindert werden, dass personenbezogene Daten in die Hände unberechtigter Dritter gelangen oder anderweitig missbraucht werden können.

Für Unternehmen stellt sich insoweit die Frage, in welchem Verhältnis diese Pflicht zur Löschung personenbezogener Daten zu den eigenen Unternehmensinteressen steht. Aus der Perspektive des Unternehmens kann es dabei durchaus berechtigte Interessen geben, die für eine möglichst lange Aufbewahrung der vorhandenen Daten sprechen. In jedem Fall gibt es für Unternehmen die Notwendigkeit, zumindest die verschiedenen gesetzlichen Aufbewahrungsfristen zu erfüllen und auf diese Weise den Compliance-Anforderungen nachzukommen.

Wie lange dürften personenbezogene Daten aufbewahrt werden?

Im Grundsatz gilt, dass personenbezogene Daten nur solange gespeichert werden dürften, wie sie benötigt werden. Dies ergibt sich aus den Grundsätzen der Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DSGVO), dem Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b) DSGVO) sowie dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO). In den Erwägungsgründen der DSGVO werden diese Anforderungen weiter konkretisiert: Die Speicherdauer soll auf das unbedingt erforderliche Mindestmaß beschränkt werden (ErwG 39 DSGVO) und Verantwortliche sollen sicherstellen, dass personenbezogene Daten nicht länger als nötig gespeichert werden (ErwGr 39).

Eine ausdrückliche Löschungspflicht ist in Art. 17 DSGVO normiert. Danach sind personenbezogene Daten zu löschen, wenn diese nicht länger notwendig sind (Art. 17 Abs. 1 lit. a) DSGVO). Daneben sind weitere Fälle normiert, die zu einer Löschung führen, und zwar der Widerruf einer zunächst erteilten Einwilligung, der erfolgreiche Widerspruch gegen eine Datenverarbeitung auf Basis eines eigenen berechtigten Interesses oder das Fehlen einer Rechtsgrundlage zur Datenverarbeitung bzw. sonstige Gründe, die zur Rechtswidrigkeit der Datenverarbeitung führen. Die Pflicht zur Löschung in Art. 17 Abs. 1 DSGVO wird nur ausgelöst, wenn der Betroffene einen Antrag dazu stellt. Anderenfalls würde das Individualrecht des Betroffenen auf Einschränkung der Verarbeitung aus Art. 18 Abs. 1 lit. c) DSGVO vereitelt. Aus der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO folgt aber auch unabhängig von Art. 17 DSGVO eine antragsunabhängige (laufende) Prüfpflicht des für die Verarbeitung Verantwortlichen. Im Ergebnis besteht damit neben dem Individualanspruch des Betroffenen auf Löschung auch eine objektive Verpflichtung, die Daten nicht länger zu speichern als rechtlich vorgesehen.

Welche gesetzlichen Aufbewahrungspflichten gibt es?

Unternehmen haben zahlreiche rechtliche Aufbewahrungspflichten zu berücksichtigen. Überall dort, wo andere Gesetze eine Aufbewahrungspflicht vorschreiben, ist die Speicherung der Daten zur Erfüllung der gesetzlichen Anforderungen zulässig (Art. 6 Abs. 1 S. 1 lit. c) DSGVO).

Für Unternehmen ergeben sich Pflichten zur Aufbewahrung von personenbezogenen Daten beispielsweise aus handels- und steuerrechtlichen Vorschriften, insbesondere aus den gesetzlichen Bestimmungen des § 257 Handelsgesetzbuch (HGB) und § 147 AO (Abgabenordnung). So müssen z. B. Handelsbücher und Aufzeichnungen sowie Rechnungen für zehn Jahre archiviert werden, auch wenn diese personenbezogene Daten Dritter enthalten. Für empfangene Geschäftsbriefe, Kopien von abgesandten Schreiben und vergleichbare Unterlagen gilt eine Aufbewahrungsfrist von sechs Jahren.

Auch hinsichtlich Mitarbeiterdaten gibt es gesetzliche Aufbewahrungspflichten, etwa in § 16 Abs. 2 Arbeitszeitgesetz (ArbZG), § 19 Abs. 1 Arbeitnehmer-Entsendegesetz (AEntG), § 17 Abs. 1 S. 1 Mindestlohngesetz (MiLoG) sowie in § 27 Abs. 5 Mutterschutzgesetz (MuSchuG). Nach diesen Vorschriften müssen bestimmte Informationen und Aufzeichnungen zum Nachweis der Einhaltung der gesetzlichen Vorschriften „mindestens zwei Jahre" aufbewahrt werden.

Daneben gibt es zahlreiche weitere Vorschriften, die eine Aufbewahrung vorschreiben, z.B. im Sozialversicherungs- und Steuerrecht und in der Gewerbeordnung.

Zusätzlich dürfen Daten gemäß Art. 17 Abs. 3 DSGVO i.V.m. § 24 Abs. 1 Nr. 2 BDSG so lange aufbewahrt werden, wie diese zur Geltendmachung, Ausübung oder Abwehr von (zivil-) rechtlichen Ansprüchen benötigt werden. In der unternehmerischen Praxis dürften zahlreiche Datenbestände unter diese Ausnahme fallen. Teilweise wird vertreten, dass eine bloß abstrakte Möglichkeit der rechtlichen Auseinandersetzung nicht ausreiche, um das Aufbe-

wahrungsrecht auszulösen. Stattdessen müsse eine hinreichende Wahrscheinlichkeit für eine bevorstehende Auseinandersetzung bestehen (Nolte/Werkmeister, in: Gola, DSGVO, 2. Aufl. 2018, Art. 17 Rn. 48 f.). Mit Hinblick auf den mit der DSGVO beabsichtigten Interessenausgleich zwischen dem Betroffenen und dem Verantwortlichen dürfen die Anforderungen an ein Recht zur Speicherung der Daten gem. Art. 17 Abs. 3 DSGVO i.V.m. § 24 Abs. 1 Nr. 2 BDSG allerdings nicht zu hoch angesetzt werden, da anderenfalls die Reichweite der explizit vorgesehenen Ausnahmen in unzulässiger Weise ausgehöhlt würden. Im Ergebnis wird es somit auch hier auf eine Abwägung der Schutzinteressen der Betroffenen unter Berücksichtigung mit der Wahrscheinlichkeit für einen Rechtsstreit und die dabei betroffenen Rechtsgüter ankommen, wofür wohl auch auf abstrakte Erwägungen zurückgegriffen werden kann.

Wie müssen die Daten während der Aufbewahrung geschützt werden?

Soweit Daten ausschließlich zur Erfüllung von Aufbewahrungspflichten gespeichert bleiben, empfiehlt sich eine Trennung von den noch aktiv genutzten Daten. Bei der Aufbewahrung in Papierform kann eine Ablage regelmäßig sortiert nach Jahren in einem entsprechenden Archivraum erfolgen. Auf diese Weise kann ohne großen Aufwand überprüft werden, welche Unterlagen nach Ablauf der Aufbewahrungsfristen vernichtet werden können. Bezüglich nicht-elektronisch gespeicherter Daten ist insoweit auch die besondere Ausnahme in § 35 BDSG zu beachten. Ist eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse des Betroffenen an der Löschung als gering anzusehen, kann gemäß § 35 BDSG an die Stelle der Löschung die Einschränkung der Verarbeitung treten. Bei der Einschränkung der Verarbeitung gemäß Art. 18 Abs. 2 DSGVO sind die Daten zu „sperren" und dürfen – abgesehen von der Speicherung – nur noch mit einer Einwilligung des Betroffenen oder zur Ausübung, Geltendmachung oder Abwehr von Rechtsansprüchen bzw. aus wichtigem öffentlichen Interesse verarbeitet werden. Offen bleibt allerdings die Frage, ob im Umkehrschluss aus der Ausnahmeregelung gefolgert werden kann, dass in allen anderen Konstellationen die Daten zwingend gelöscht werden müssen. In zahlreichen Konstellationen wird dies aufgrund der gewählten Art der elektronischen Archivierung praktisch gar nicht möglich sein.

Wie kann eine Archivierung praktisch erfolgen?

Grundsätzlich gibt es nur für wenige Unterlagen eine konkrete Vorgabe, in welcher Form die Aufbewahrung erfolgen muss. Für Jahresabschlüsse ist beispielsweise vorgesehen, dass diese immer im Original aufbewahrt werden müssen.

Soweit keine besonderen Vorschriften einschlägig sind, ist grundsätzlich sowohl die elektronische Aufbewahrung als auch die Datenhaltung in Papierform denkbar. Soweit elektronische Archivierungssysteme verwendet werden, verfügen diese idealerweise über eine Möglichkeit, bestimmte Datensätze systematisch aus den Archiven löschen zu können. Für das Unternehmen bietet dies den Vorteil, dass keine gesonderte datenschutzrechtliche Rechtfertigung für den Datenfortbestand im Archiv herangezogen werden muss. Zur Dokumentation der Einhaltung des Datenschutzrechts sollten die Verantwortlichen die Fristen für die Löschung oder regelmäßige Überprüfungen der Datenbestände vorsehen, die idealerweise in einem Löschungskonzept und ergänzend im Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO festgehalten werden.

Wird die Einhaltung der Vorgaben kontrolliert?

Die für die Verarbeitung verantwortlichen Unternehmen unterliegen gemäß Art. 5 Abs. 2 DSGVO einer Rechenschaftspflicht, die sich auch auf die Einhaltung der (datenschutz-) rechtlichen Anforderungen an die Löschung personenbezogener Daten bezieht. Zwar gibt es eigentlich keine eigenständigen Kontrollen, die sich allein auf die Beachtung der Aufbewahrungsfristen beziehen, allerdings kann das Thema bei anderweitigen Prüfungen der Aufsichtsbehörden relevant werden. Unter den Grundsätzen der Rechenschaftspflicht obliegt es dann den für die Verarbeitung Verantwortlichen, ihrerseits die Einhaltung der Datenschutzvorgaben zur Aufbewahrung und Löschung von Daten nachzuweisen.

Daneben haben die Betroffenen einen Anspruch auf Auskunftserteilung gemäß Art. 15 DSGVO. Soweit dem Betroffenen im Rahmen der Beantwortung Auskunft über Daten gegeben wird, die eigentlich nicht mehr hätten gespeichert werden dürfen, besteht – unabhängig von dem Anspruch auf Löschung der Daten – die Beschwerdemöglichkeit bei der zuständigen Aufsichtsbehörde.

Im Rahmen der Kommunikation mit Kunden und anderen Betroffenen ist übrigens zu beachten, dass diese keinen Anspruch auf Löschung ihrer Daten geltend machen können, solange entgegenstehende gesetzliche Aufbewahrungsfristen bestehen. Statt der Löschung kann der Betroffene unter Umständen aber die Einschränkung der Verarbeitung (Sperrung) verlangen. Ein unmittelbarer Anspruch auf Löschung besteht regelmäßig nur dann, wenn die Rechtsgrundlage für die ursprüngliche Datenverarbeitung die Einwilligung des Betroffenen war und diese Einwilligung später widerrufen wird.

Fazit

Das Datenschutzrecht verpflichtet alle Unternehmen, personenbezogene Daten nur so lange zu speichern, wie diese zur Erfüllung der verfolgten Zwecke erforderlich sind. Anschließend sind die personenbezogenen Daten zu löschen. Neben dieser allgemeinen Löschpflicht steht den Betroffenen ein ausdrücklicher Löschungsanspruch zu. Die Einhaltung der datenschutzrechtlichen Anforderungen an die Speicherung und Löschung personenbezogener Daten unterliegt der Rechenschaftspflicht, sodass Unternehmen diesbezügliche Aktivitäten gut dokumentieren sollten. Insbesondere empfiehlt es sich, ein Konzept zur Löschung im Unternehmen zu erarbeiten und die Speicherdauer für die jeweiligen Datenverarbeitungen im Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren.

Robert Bommel, LL.M. / Dr. Sebastian Meyer, LL.M.

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Dr. Sebastian Meyer, LL.M.
Rechtsanwalt
Datenschutzauditor (TÜV)

T +49 521 96535 - 812
F +49 521 96535 - 115
M sebastian.meyer@brandi.net
www.brandi.net