BRANDI
RECHTSANWÄLTE

DATENLÖSCHUNG – ONLINE UND OFFLINE

Informationen zum Datenschutz I April 2024

Einleitung

Im Zusammenhang mit der Speicherung oder sonstigen Aufbewahrung von Daten und deren Löschung heißt es häufig, dass gelöschte Daten die sichersten Daten seien. Die Aussage bezieht sich insbesondere auf den Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e) DSGVO, eines der wesentlichen Prinzipien des Datenschutzrechts. Personenbezogene Daten dürfen hiernach nur so lange gespeichert bzw. in sonstiger Weise aufbewahrt werden, wie dies für die verfolgten Zwecke erforderlich ist. Sobald die Daten nicht länger benötigt werden, sind sie nach Art. 17 Abs. 1 DSGVO zu löschen. Durch die Vorgaben zur Löschung soll unter anderem verhindert werden, dass personenbezogene Daten in die Hände unberechtigter Dritter gelangen oder anderweitig missbraucht werden können.

Die Pflicht zur Löschung von Daten bzw. deren Vernichtung und das weitere Aufbewahrungsinteresse des Unternehmens stehen häufig in einem Spannungsverhältnis zueinander. In diesem Kontext stellen sich verschiedene Fragen: Wie lange dürfen personenbezogene Daten aufbewahrt werden? Was ist unter den Begriffen „Löschen“ und „Vernichten“ zu verstehen? Was ist bei der Löschung von Daten aus Online-Systemen zu beachten? Und was gilt mit Blick auf die Vernichtung von Datenträgern und Papierunterlagen?

Wie lange dürfen personenbezogene Daten aufbewahrt werden?

Aus den Grundsätzen der Datenverarbeitung sowie den Erwägungsgründen der DSGVO ergibt sich, dass personenbezogene Daten grundsätzlich nur so lange gespeichert werden dürfen, wie sie benötigt werden. Personenbezogene Daten, die für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind, müssen unverzüglich gelöscht werden. Dies ergibt sich ausdrücklich aus Art. 17 Abs. 1 lit. a) DSGVO. Darüber hinaus finden sich in Art. 17 DSGVO noch weitere Gründe, bei deren Vorliegen das verantwortliche Unternehmen zur Datenlöschung verpflichtet ist. Die grundsätzliche Pflicht zur Löschung entfällt, wenn die Daten einer Aufbewahrungspflicht unterliegen oder einer der anderen in Art. 17 Abs. 3 DSGVO aufgelisteten Ausnahmetatbestände erfüllt ist. Weitere Ausnahmen hat der deutsche Gesetzgeber in § 35 BDSG normiert, wobei die Zulässigkeit weiterer Ausnahmen außerhalb der DSGVO umstritten ist (Nolte/Werkmeister in Gola/Heckmann, § 35 Rn. 3). Hiernach besteht die Pflicht zur Löschung nach Art. 17 DSGVO unter anderem dann nicht, wenn eine Löschung im Falle nicht automatisierter Datenverarbeitungen wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und das Interesse des Betroffenen an der Löschung als gering anzusehen ist. In diesem Fall tritt an die Stelle der Löschung die Einschränkung der Verarbeitung nach Art. 18 DSGVO. Hiernach sind die Daten zu „sperren“ und dürfen - abgesehen von der Speicherung - nur noch mit Einwilligung des Betroffenen oder zur Ausübung, Geltendmachung oder Abwehr von Rechtsansprüchen bzw. aus wichtigem öffentlichen Interesse verarbeitet werden.

Zu beachten ist, dass die Löschpflicht nicht nur für online gespeicherte Daten, sondern auch für offline vorgehaltene Daten gilt. In letzterem Fall sind die Informationen bei Erreichen der Speicherfrist unkenntlich zu machen oder datenschutzkonform zu vernichten.

Was ist unter den Begriffen „Löschen“ und „Vernichten“ zu verstehen?

Was konkret unter dem Begriff „Löschen“ zu verstehen ist, wird in der DSGVO nicht näher beschrieben. Aus dem Umstand, dass Art. 4 Nr. 2 DSGVO zwischen der Löschung und der Vernichtung von Daten differenziert, ist zu schließen, dass eine Löschung nicht zwingend mit einer Vernichtung der Daten einhergehen muss. Der Begriff umfasst vielmehr jede Art der Unkenntlichmachung; erfasst sind daher alle Konstellationen von der Anonymisierung der Daten über das Überschreiben oder Schwärzen von Daten bis schließlich zu ihrer physischen Zerstörung (Vernichtung). Die Vernichtung stellt folglich nur eine mögliche Form der Löschung dar.

Grundsätzlich gilt, dass die Daten nach dem Löschen nicht mehr wahrnehmbar sein und dem Verantwortlichen nicht mehr für eine weitere Nutzung zur Verfügung stehen dürfen. Dies bedeutet auch, dass Daten vom Grundsatz her erst dann als gelöscht oder vernichtet angesehen werden können, wenn sichergestellt wurde, dass auch keine Datensicherungen oder andere Kopien der Datensätze im Verantwortungsbereich des Verantwortlichen mehr existieren. Rein organisatorische Maßnahmen, die lediglich eine Wahrnehmung der Information verhindern sollen (z.B. eine entsprechende Kennzeichnung) sind demgegenüber nicht ausreichend.

Was ist bei der Löschung von Daten aus Online-Systemen zu beachten?

Liegt ein Löschungsgrund vor, müssen die betreffenden Daten grundsätzlich unverzüglich aus den Online-Systemen entfernt werden, soweit sie nicht einer Aufbewahrungspflicht unterliegen. Der Verantwortliche hat insoweit die Pflicht, regelmäßig zu überprüfen, ob in Bezug auf die in seinem Verantwortungsbereich vorhandenen Daten ein Löschgrund vorliegt.

Soweit Daten ausschließlich zur Erfüllung von Aufbewahrungspflichten gespeichert bleiben, empfiehlt sich eine Trennung von den noch aktiv genutzten Daten. Auf diese Weise kann ohne größeren Aufwand überprüft werden, welche Datensätze nach Ablauf der Aufbewahrungsfrist zu löschen sind. Zur einfacheren Umsetzung der Löschung verfügt ein elektronisches Archivierungssystem idealerweise über eine Möglichkeit, bestimmte Datensätze systematisch aus den Archiven löschen zu können. Ist einer der Ausnahmetatbestände von § 35 BDSG erfüllt, dürfen die Daten, soweit dies technisch umsetzbar ist, in den Systemen auch gesperrt anstatt gelöscht werden.

Die Pflicht zur Datenlöschung bezieht sich nicht nur auf Live-Systeme und Archive, sondern erfasst grundsätzlich auch Datensicherungen und Backup-Systeme. Insoweit ergeben sich regelmäßig keine größeren Probleme, wenn die Sicherungen ohnehin in regelmäßigen, verhältnismäßig kurzen Abständen überschrieben und Altdaten auf diese Weise gelöscht werden. Bleiben Daten bei gestuften Backupkonzept dagegen auch für einen längeren Zeitraum noch gespeichert, dient dies der Datensicherheit; das Vorgehen kann als technische und organisatorische Maßnahmen auf Art. 32 DSGVO gestützt werden und steht der Löschpflicht gem. Art. 17 DSGVO nicht entgegen (Korte, ZD-Aktuell 2020, 07001). Es ist in diesem Fall nur darauf zu achten, dass die Backupdaten dann auch wirklich nur zu Backupzwecken genutzt werden und wenigstens eine Sperrung dieser Daten erfolgt.

Was gilt mit Blick auf die Vernichtung von Datenträgern und Papierunterlagen?

Da es sich bei der Vernichtung von Datenträgern und Ausdrucken, die personenbezogene Daten wie Namen und Adressen von Einzelpersonen beinhalten, gem. Art. 4 Nr. 2 DSGVO um eine Verarbeitung personenbezogener Daten, ist bei deren Entsorgung gem. Art. 32 Abs. 1 DSGVO ein dem Risiko angemessenes Schutzniveau zu gewährleisten ist. Welche Maßnahmen hierzu konkret zu ergreifen sind, richtet sich nach der Sensibilität der betroffenen Daten. Es ist insoweit festzuhalten, dass eine umfassende gesonderte Entsorgung aller Papierabfälle und Datenträger nicht zwingend erforderlich ist, da nicht in jedem Fall, in dem ein Papier oder Datenträger personenbezogene Daten enthält, eine geschützte Vernichtung zu erfolgen hat. Es bedarf vielmehr einer Einzelfallentscheidung.

Allgemein hat eine gesonderte Entsorgung insbesondere dann zu erfolgen, wenn es zu einer Datenverarbeitung durch das Unternehmen gekommen ist oder Daten Dritter offenbart werden. Die nachfolgenden, nicht abschließenden Beispiele dienen der Veranschaulichung sowie der Konkretisierung dieser allgemeinen Vorgabe. Enthalten die Papiere oder Datenträger Kundendaten, die vom Unternehmen erhoben, verarbeitet oder gespeichert wurden, ist eine Vernichtung regelmäßig angezeigt. Gleiches gilt, sofern die Papiere oder Datenträger zu schützende Mitarbeiterdaten enthalten. Sind hingegen ausschließlich Kontaktdaten des Unternehmens oder dienstliche Kontaktdaten der einzelnen Mitarbeiter betroffen, ist eine gesonderte Entsorgung nicht erforderlich. Dies gilt ebenso, wenn dem Unternehmen Kontaktdaten anderer Personen z.B. in Form von Absenderinformationen auf unerwünschten Werbebriefen aufgedrängt wurden. Bei internen E-Mails ist danach zu differenzieren, welche Informationen enthalten sind und auch der Kontext ist entscheidend. Eine Mitteilung wie „Ich komme später." oder „Die Besprechung muss verschoben werden." bedarf keiner gesonderten Entsorgung. Werden in der E-Mail jedoch Daten, wie z.B. das Treffen mit einer namentlich benannten externen Person oder Kundendaten offenbart, ist eine Vernichtung erforderlich. Gleiches gilt im Falle von geheimhaltungsbedürftigen Informationen, wie einem nicht öffentlichen Treffen oder dem Kontakt zu anderen Unternehmen, die nicht nach außen getragen werden sollen.

Um sicherzustellen, dass in allen Fällen, in denen es einer datenschutzgerechten Entsorgung bedarf, auch eine solche stattfindet, ist es möglich, sich generell für eine geschützte Vernichtung zu entscheiden. Grund hierfür kann zum einen die Überlegung sein, dass die Bewertung im Einzelfall den einzelnen Mitarbeitern nicht zugemutet werden soll. Zum anderen bedeutet eine Einzelfallentscheidung einen gesteigerten Aufwand und eine höhere Fehleranfälligkeit. Sofern bei der Entsorgung der Papierabfälle nach datenschutzrechtlicher Erforderlichkeit differenziert werden soll, ist es empfehlenswert, den Mitarbeitern Maßstäbe an die Hand zu geben, anhand derer sie in der Lage sind, eine eigene Einschätzung vorzunehmen, um das Risiko einer datenschutzwidrigen Entsorgung zu minimieren.

Fazit

Sind die Zwecke entfallen, für die die Daten erhoben oder in sonstiger Weise verarbeitet wurden, oder liegt einer der anderen Gründe des Art. 17 DSGVO vor, ist der Verantwortliche zur Datenlöschung verpflichtet, soweit er keiner weiteren Aufbewahrungspflicht unterliegt oder ein Ausnahmetatbestand erfüllt ist. Ob eine Pflicht zur Löschung besteht, hat der Verantwortliche regelmäßig von sich aus zu überprüfen. Der Begriff der Löschung umfasst nicht nur die physische Vernichtung der Daten, sondern auch ihre Anonymisierung, Überschreibung oder Schwärzung. Es muss dabei jeweils gewährleistet werden, dass die Informationen nach der Löschungshandlung nicht mehr wahrnehmbar sind und keine Kopien der Datensätze mehr existieren. Um die Einhaltung der Vorgaben sicherzustellen und die Prozesse zu vereinfachen, bietet sich eine Definition der anwendbaren Löschfristen und eine Dokumentation der vorgesehenen Abläufe zur Umsetzung der Löschung innerhalb eines Löschkonzeptes an.

Christina Prowald

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net