GDPR / DSGVO – Löschen mit Konzept

Zusammenfassung: Mit der Datenschutzgrundverordnung (DSGVO), die in der EU unmittelbar Gesetz ist, wird beim Datenschutz mit Wirksamkeit zum 25. Mai 2018 vieles anders. Unter anderem wurden die Regeln für das Löschen personenbezogener Daten neu gefasst. Die Rechte der betroffenen Personen wurden erweitert und erstmals ist es möglich, beim Anbieterwechsel Daten mitzunehmen. Da gleichzeitig die Bußgelder bei Verstößen drastisch angehoben wurden, ist die Zeit für funktionierende Löschkonzepte mehr als reif. Verantwortliche müssen sich mit der Thematik beschäftigten. Im folgenden Praxistipp wird ein generisches Löschkonzept empfohlen, das Grundlage für fachbezogene Löschkonzepte sein soll.

Lebenszyklen von Daten: Täglich werden in Unternehmen Daten verarbeitet. Neue kommen hinzu, werden erfasst, bearbeitet, verändert, abgespeichert. Irgendwann werden sie nicht mehr benötigt. Wenn dann auch eine mögliche gesetzliche Aufbewahrungsfrist abgelaufen ist, ist das Ende der Datenhaltung, also des Lebenszyklus der Daten, gekommen. Eigentlich.

Nicht nur Katzen haben sieben Leben: Das „Leben" von Daten kann erstaunlich zäh sein. Katzen wird nachgesagt, sie hätten sieben Leben. Das kann man von Daten auch behaupten. Einerseits verschwinden sie mitunter aus unerfindlichen Gründen und sind nicht mehr auffindbar. Andererseits können Daten rasch und beliebig oft kopiert werden, nicht zuletzt im Rahmen der Datensicherungen, die auf mehreren Datensicherungsmedien erfolgen kann. Dateien verlässlich zu löschen, ist also mitunter gar nicht so leicht, aber genau das fordert der Datenschutz in bestimmten Fällen.

Erweiterte Löschregeln: Mit der DSGVO/ GDPR sind erweiterte Löschvorschriften in Kraft getreten. Insbesondere werden die Verbraucherrechte gestärkt. Betroffene Personen haben erweiterte Rechte auf Löschen oder zumindest Sperren sie betreffender Daten. Außerdem wurde ein neues Recht auf Vergessenwerden in Kraft gesetzt. Damit können Verbraucher beim Anbieterwechsel verlangen, dass ihre Daten mit zum neuen Anbieter genommen werden. Derzeit dürften die wenigsten Organisationen auf diese neue Rechtslage eingerichtet sein. Da diese Rechte jedoch nicht verhandelbar sind, muss sich jeder Verantwortliche mit dieser Herausforderung beschäftigen.

Worauf müssen Verantwortliche vorbereitet sein? Verantwortliche müssen Löschregeln schaffen, mit deren Anwendung es möglich wird, Daten dann zu löschen, wenn die Zweckbindung endet und mögliche gesetzliche Aufbewahrungsfristen abgelaufen sind. Weiterhin sind Vorbereitungen zu treffen, alle personenbezogenen oder auf Personen beziehbaren Daten einer betroffenen Person zu finden und dann unverzüglich zu löschen, wenn eines der weiteren Betroffenenrechte des Artikels 17 ff DSGVO/GDPR geltend gemacht wird.

Wo die Risiken liegen: Ein Bewerber um eine Stelle erhielt eine Absage. Nach Erhalt der Absage verlangte er als Betroffener dass alle seine Daten zu löschen seien. In der Folge wurde ihm mitgeteilt, dass seine in elektronischer Form vorliegenden Daten wie gewünscht gelöscht worden seien. Einige Monate später erhielt er eine Nachricht aus dem betreffenden Unternehmen, wonach seine Bewerbungsunterlagen beim seinerzeitigen Bewerberverfahren an eine andere Abteilung weitergegeben worden seien. Diese suche nun einen Mitarbeiter wie ihn und lade ihn daher zum Vorstellungsgespräch ein. In der Zwischenzeit hatte er eine andere Stelle angetreten und wunderte sich nun sehr darüber, dass ihm einerseits die Mitteilung über die Löschung aller seiner Daten erreicht hatte, andererseits aber die Bewerbung in einer anderen Abteilung noch vorlag. Er schaltete die zuständige Aufsichtsbehörde ein. Diese verhängte nach näherer Prüfung ein Bußgeld.

Herausforderung: Wenn Daten über bestimmte Projekte oder Personen auf zentral administrierten Laufwerken vorliegen, ist deren Auffinden und Löschen bei Bedarf normalerweise kein Problem. Liegen aber wie im genannten Fall Daten auch noch in Kopie vor, und dazu noch auf persönlichen Laufwerken, wird das systematische Löschen schon schwieriger – in einigen Organisationen scheinbar unmöglich. Ohne ein strukturiertes Löschkonzept ist das dann kaum zu verwirklichen.

Was zu klären ist: Erstens ist zu klären, welche personenbezogenen oder auf Personen beziehbare Daten in den einzelnen Geschäftsprozessen (Verarbeitungstätigkeiten) vorliegen. Hier sind die Beschreibungen der Bearbeitungstätigkeiten eine wichtige Unterstützung. Diese enthalten Angaben über Personenkategorien und Datenkategorien bzw. einzelne Daten im Prozess. Zweitens muss für alle diese Datenkategorien oder Daten ermittelt werden, ob es eine gesetzliche Mindestaufbewahrungszeit gibt und wie lang diese gegebenenfalls ist. Drittens muss geprüft werden, wie lange die Daten für die Erfüllung der Prozessanforderungen erforderlich sind. Dann muss der Beginn der jeweiligen Frist festgelegt werden – der erste Januar des auf den Eintritt der Aufbewahrung folgenden Jahres

ist vor allem bei kürzeren Verjährungsristen nicht immer geeignet. Und schließlich ist festzulegen, wer dann wie die erforderliche Löschung durchführt und wie diese zu dokumentieren ist.

Erstens ein generisches Löschkonzept: Da der Überblick über die unterschiedlichen gesetzlichen Aufbewahrungsfristen mitunter sehr komplex sein kann, müssen für die Klärung dieser Fristen die Fachleute aus dem jeweiligen Fachbereich herangezogen werden. Das generische Löschkonzept unterstützt die Verantwortlichen bei der Erfüllung der Löschpflichten. Es enthält die Definition über die Datenkategorien und deren gesetzliche Aufbewahrungsfristen. Weiterhin wird hier definiert, wie die Prozesserfordernis ermittelt und festgelegt werden kann. Sind gesetzliche und prozessuale Aufbewahrungsdauer identisch, ist die Löschung einfach festzulegen. Ist die prozessuale Kürzer, sind die Daten zur Erfüllung der gesetzlichen Aufbewahrung für den unbefugten Zugriff von Prozessseite aus zu sperren. Ist die Prozesserfordernis länger als die gesetzliche, ist eine stichhaltige Begründung erforderlich. Ohne objektives Erfordernis ist eine längere Aufbewahrung mit der Erfüllung der Betroffenenrechte beim Datenschutz nicht vereinbar. Schließlich enthält das generische Löschkonzept Bestimmungen zu den Modalitäten und der Dokumentation des tatsächlichen Löschvorgangs.

Zweitens fachbezogene Löschkonzepte: In einem zweiten Schritt werden aus dem generischen Löschkonzept die fachspezifischen Löschregeln erarbeitet. Diese sind sicherlich im Vertrieb andere als im Bereich HR. Die Verantwortlichen aus den Bereichen sind in der Pflicht, die Regeln für die Aufbewahrung und Löschung der personenbezogenen Daten aus dem jeweiligen Bereich gewissenhaft festzulegen und deren Umsetzung in die Wege zu leiten sowie die Löschung zu überwachen und zu dokumentieren. Die fachbezogenen Löschkonzepte müssen auch Regeln für den Umgang mit Anträgen von betroffenen Personen zum Löschen ihrer Daten enthalten.

Objektive Erfordernisse zur Datenhaltung: Entgegen landläufiger Meinungen geht es hierbei aber nicht darum, gierig wie die Geier hinter allem her zu sein, was nach löschbaren Daten aussieht, etwa nach dem Motto; was nicht bei drei auf den Bäumen ist, wird gelöscht. Es geht vielmehr darum, Daten so lange verfügbar zu halten, wie sie objektiv erforderlich sind oder wie der Gesetzgeber dies fordert. Das Motto: „wer weiß, vielleicht können wir die Daten irgendwann noch einmal brauchen“ ist jedoch kein objektives Erfordernis. Je besser Fachbereichsverantwortliche und Datenschutzbeauftragte hierbei zusammenarbeiten, desto besser ist das für die Wahrung der Betroffenenrechte, also der Rechtssicherheit einerseits und die Funktionalität der Fachbereiche andererseits.

Interne Audits: Wenn die fachbezogenen Löschregeln definiert und eingeführt sind, müssen regelmäßig Überprüfungen stattfinden. Nur so kann sichergestellt werden, dass nicht aus Versehen Regelverstöße begangen werden, die teure Folgen nach sich ziehen können. Dazu sollten die Verantwortlichen regeln, wer die Kontrollen übernimmt. In Frage kommen neben den Datenschutzbeauftragten auch Kollegen des Controlling, des Fachbereichs Compliance oder der internen Revision. Entscheidend ist jedoch, dass die Kontrollen verlässlich dokumentiert, Abweichungen geprüft und Maßnahmen zur Vermeidung der Wiederholung solcher Fälle ergriffen werden.

Externe Überprüfungen: Im Rahmen von Kontrollen seitens der Aufsichtsbehörden kann es auch zu externen Überprüfungen der Einhaltung der Löschverpflichtungen kommen. Ist das Unternehmen Auftragsverarbeiter, können auch Kontrollen durch die Verantwortlichen erfolgen. Dies kann unter anderem dann der Fall sein, wenn der Auftragsverarbeiter temporäre Projekte bearbeitet und für den Fall, dass diese ausgelaufen sind, Löschregeln definiert wurden. Für derartige externe Überprüfungen muss immer eine Rechtsgrundlage vorliegen. Im Falle eines Vertrags über Auftragsverarbeitung sind dies die vereinbarten Modalitäten zur Vertragserfüllung und die vereinbarten Kontrollen.

Unterstützung durch Datenschutzbeauftragte: Mit ihrem Wissen und ihrer Erfahrung können Datenschutzbeauftragte die Verantwortlichen bei diesem Prozess tatkräftig unterstützen. Sie sind jedoch nicht per se diejenigen, die die Verantwortung für das Einleiten, die Definition, die Umsetzung und die Kontrolle der damit zusammenhängenden Prozesse tragen. Es macht Sinn, wenn sich Verantwortliche und Datenschutzbeauftragte hier eng abstimmen. Aber die Verantwortung für die gesetzeskonforme Umsetzung liegt nicht beim Datenschutzbeauftragten.

Fazit: Systematisches Löschen von personenbezogenen oder auf Personen beziehbaren Daten ist mit etwas Vorbereitung machbar. Andererseits dürfen die Anforderungen an funktionierende Löschkonzepte auch nicht unterschätzt werden. Da die Vorbereitungen sich über mehrere Monate erstrecken können, sollte rasch mit der Verwirklichung begonnen werden, um bis zur Gültigkeit der DSGVO/ GDPR mit den wichtigsten Arbeiten fertig zu sein.

Eberhard Häcker, Ensdorf

Der Autor Eberhard Häcker ist Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und seit vielen Jahren als Externer Datenschutzbeauftragter und Datenschutzberater tätig. Seine Fachaufsätze erscheinen regelmäßig in unterschiedlichen Publikationen. Außerdem ist er Geschäftsführer der HäckerSoft GmbH, die unter anderem mit der Datenschutzsoftware DATSIS und der Lernplattform Optilearn (Pflichtschulungen für Datenschutzbeauftragte) am Markt aktiv ist. Sein Lieblingsprojekt ist datenschutzkabarett.de.