

Unternehmensweite Löschkonzepte

Einleitung: Vom Segen des Löschens

Ich weiß nicht, meine Damen und Herren, wer von Ihnen den Film „The Dark Knight“ gesehen hat, den letzten Batman-Film? Dieser Film ist insbesondere wegen seiner Schlusszene eigentlich ein Muss für jeden Datenschützer. Lucius Fox, der Geschäftsführer der diversen Batman-Unternehmungen, dargestellt von dem auch in dieser Rolle großartigen Morgan Freeman, löscht alle Überwachungsvideos, die Batman in einer gigantischen Überwachungsmaaschinerie gespeichert hatte. Ich habe mich bemüht, die Schlussequenz dieses Films für diesen Vortrag zu bekommen. Dies ist mir leider nicht gelungen. Insoweit muss ich also an Ihre Phantasie appellieren. Stellen Sie sich einen riesigen Raum vor, an dessen Stirnwand 5.000 Monitore, die Zahl lässt sie beliebig vergrößern, flimmern und Bilder aus allen möglichen Teilen der Stadt Gotham übertragen. Lucius Fox gibt nun über seine Konsole einen Droptable-Löschbefehl an das System, dreht sich um und verlässt stolz und erhobenen Hauptes den Raum, während im Hintergrund alle Bildschirme erlöschen. Eine wirklich beeindruckende Szene. Eine Szene, die einerseits beispielhaft Gefahren und Risiken der Informationsgesellschaft für das Individuum transparent machen. Diese Gefahren gehen ja doch viel weiter als der bloß fahrlässige Umgang mit Kundendaten. Zugleich aber symbolisiert dieses Bild auch, und das ist es eben, was das Herz des Datenschützers erwärmt, das nur gelöschte Daten vor möglichen Missbräuchen schützen. Aber beim Löschen geht es nicht nur um den Schutz vor Missbrauch. Vielmehr ist der Löschkprozess die logische Konsequenz der datenschutzrechtlichen Grundsätze von Datensparsamkeit und Erforderlichkeit und damit unabdingbarer Bestandteil eines Systemdatenschutzes.

Rechtlicher Rahmen

Insofern müsste die Verpflichtung zur Datenlöschung im BDSG eigentlich an herausragender Stelle geregelt sein. Zur Löschung von Daten bei ansonsten ordnungsgemäßer Datenverarbeitung heißt es aber lediglich in § 35 Abs. 2 Nr. 3 BDSG Daten, sie seien zu löschen, sobald Ihre Kenntnis für die Erfüllung des Zweckes ihrer Speicherung nicht mehr erforderlich sei. Diese Formulierung ist zunächst einmal so ergebnisoffen, das es nicht verwundert, wenn die Löschung von Daten häufig generell unterbleibt. Da hilft auch die Tatsache wenig, dass in § 4 e Abs. 1 Nr. 7 BDSG eine Regelfrist für Löschungen gefordert wird. Dieser Forderung des Gesetzes wird in der realen Welt kaum Beachtung geschenkt. Dies verwundert nicht, denn selbst die Kommentarliteratur schenkt dieser Vorschrift kaum Beachtung. So heißt es etwa bei Schafflandt/Wiltfang lapidar: Wegen der Aufbewahrungs-

pflichten (Nr. 7) wird regelmäßig 10 Jahre einzutragen sein.“ Diese Aussage wird in keiner Weise dem Löschgebot des § 35 gerecht. Denn das ist ja der eigentliche Sinn und Zweck dieser Regelung: Die permanente Selbstvergewisserung darüber, ob die Kenntnis der Daten für die Erfüllung des Zweckes ihrer Speicherung noch erforderlich ist. Eine pauschale, sich offensichtlich an den Regeln der AO oder des HGB orientierende Löschfrist für die Daten wird dieser vom Gesetz geforderten differenzierten Betrachtung aber gerade nicht gerecht. Vielmehr muss betont werden, dass die verantwortliche Stelle bereits bei der Festlegung der Verarbeitungszwecke Regelfristen für die Löschung festzulegen hat.

Die Realität

In der wirklichen Welt aber gibt es eine eindeutige Tendenz, die dahin geht, einmal erhobene Daten, unabhängig davon, ob sie für den Geschäftszweck eines Unternehmens noch erforderlich sind oder nicht, möglichst lange zu speichern, nach Möglichkeit gar nicht erst zu löschen.

Dies ist, meine Damen und Herren, nicht etwa Ausfluss eines Vergnügens am Rechtsbruch. Nein, vielmehr diktiert die Angst des Unumkehrbaren das Verhalten der Akteure. Einmal gelöschte Daten sind halt weg. Und wer weiß, vielleicht hätte man auf bestimmte Daten doch noch einmal zugreifen müssen. Ein mir ansonsten lieber Kollege hat dies plastisch auf den Punkt gebracht: „Ein Ostwestfale“, so hielt er mir in einer Datenschutzprüfung entgegen, „löscht keine Daten!“

Mittlerweile weiß ich, dass dies keine landsmannschaftliche Besonderheit ist, sondern eher ein Zug ist, der bei allen anzutreffen ist, die mit Daten umgehen, unabhängig davon, ob sie nun Bayern, Ostwestfalen, Niedersachsen oder Berliner sind.

Die Tendenz, Daten möglichst lange zu halten, wird natürlich dadurch gefördert, dass die Kosten für Speicherplatz betriebswirtschaftlich bei den meisten Unternehmen heute nicht mehr ins Gewicht fallen.

Löschung muss sein

Und dennoch führt an der Löschung von Daten kein Weg vorbei. Es geht dabei einerseits darum, natürlich bestimmte rechtliche Vorschriften einzuhalten, beispielsweise das Löschgebot des § 35 BDSG. Es geht aber vor allem auch darum, dass ein Unternehmen sich über seine Prozesse klar wird.

Diese Aussage, meine Damen und Herren, mag Sie überraschen. Der besondere Charme aber, der in einem Verfahren steckt, das den Prozess von hinten her aufrollt, also den Weg zurück verfolgt von der Löschung über alle anderen Verarbeitungsstufen bis zu Erhebung von Daten, liegt gerade darin, dass er in besonderer Weise der rationalen Planung verpflichtet ist.

Beginnt ein neues Projekt, dann herrscht anfangs große Euphorie und Aufbruchsstimmung. Man plant, man verplant, man baut Umwege, Irrwege, Sackgassen ein, all dies natürlich gesteuert von einem rationalen Projektmanagement. Alle glauben, auf Alles Zugriff haben zu müssen. Kurz: Es ist ein kreatives, gelegentlich aber auch chaotisches Gewusel, an dessen Ende dann sicherlich ein Ergebnis steht, das auch die Probleme tragfähig löst, bei dem aber in aller Regel über die Löschung von Daten nicht nachgedacht wird.

BDSG versus bereichsspezifischer Regelungen

Diese mangelnde Berücksichtigung eines Löschkonzeptes hat ihre Ursache teilweise auch im BDSG. Die Löschnorm des § 35 Abs. 2 Nr. 3 BDSG legt ja gerade nicht zeitlich konkret Löschfristen fest. Die grundsätzliche Möglichkeit einer zweckändernden Nutzung der Daten verschärft das Problem. Die ergebnisoffene Regelung des BDSG führt daher leider allzu oft dazu, dass der Löschung der Daten im Rahmen der Entwicklungsprozesse von IT-Projekten keine oder kaum nur Beachtung geschenkt wird.

Dies ist natürlich überall dort anders, wo aufgrund bereichsspezifischer Datenschutzregelungen konkrete Löschfristen vorgegeben werden. So schreibt beispielsweise die Postdienstschutzverordnung (PDSV) vor, dass die Daten, die im Zusammenhang mit Nachsendeverfahren erhoben wurden, 2 Jahre nach Erhebung zu löschen sind. Auch das Autobahnmautgesetz (ABMG) enthält zwar ausfüllungsbedürftige, aber ansonsten sehr klare Löschvorgaben. Aber, wie der Name bereits sagt, sind es eben bereichsspezifische Ausnahmen, die immer nur für einen kleinen Teil der Unternehmen greifen. Datenschutzrechtlich haben es die meisten Unternehmen mit dem BDSG zu tun und da muss eben die ergebnisoffene Regelung des § 35 BDSG ausgefüllt werden. Dies bedeutet ohne Zweifel eine besondere intellektuelle Herausforderung. Aber sie lohnt sich!

Ich möchte hier, meine sehr geehrten Damen und Herren, für ein durchgängiges Löschkonzept aller personenbezogenen Daten in einem Unternehmen werben. Die Löschpflicht besteht sowieso. Da kommt man früher oder später nicht drum herum. Ein durchgängiges Löschkonzept, das alle Arten personenbezogener Daten in einem Unternehmen umfasst, führt, und dies ist der Lohn der Anstrengung zu umfassender Transparenz aller Geschäftsprozesse. Naturwüchsig entstandene Prozesse werden auf ihre

Rationalität hin befragt, wenn der Prozess vom Ende, also von der Datenlöschung her, neu gedacht wird. Darin liegt, wie gesagt, der besondere Reiz dieser Methode.

Wer trägt Verantwortung?

Normadressat der Löschpflicht ist die verantwortliche Stelle. Die Geschäftsführung also muss dieser Verantwortung nachkommen und für ihre Organisation sicherstellen, dass Zuständigkeiten geklärt sind und Anweisungen zur Löschung erteilt werden. Versäumt es die verantwortliche Stelle, die notwendigen Maßnahmen zu ergreifen, trägt sie die volle Organisationsverantwortung. Es ist in diesem Zusammenhang die Pflicht des bDSB, seine Geschäftsführung auf entsprechende Versäumnisse hinzuweisen.

Zum Löschkonzept allgemein

Um nachzuweisen, dass die verantwortliche Stelle ihre Pflichten im geforderten Umfang wahrgenommen hat, muss sie die Analyse der verschiedenen Datenarten und die Umsetzung der daraus resultierenden Löschrmaßnahmen dokumentieren. Vollständigkeit kann erreicht werden, wenn eine systematische Vorgehensweise gewählt wird - zu empfehlen ist daher ein durchgängiges Löschkonzept mit folgenden Inhalten:

- Regelung der Verantwortlichkeiten;
- Abgrenzung zwischen den Aufgaben des bDSB und denen der System- oder - Informationsverantwortlichen bis hin zur Verantwortung für das Monitoring von Löschrfunktionen;
- Identifikation der personenbezogenen Datenbestände;
- Festlegung der Regellöschfristen für die verschiedenen Datenarten auf der Basis der gesetzlichen Regelungen;
- organisatorische und technische Maßnahmen, die im Einzelnen zur Löschung in den produktiven Prozessen ergriffen werden;
- Steuerung von Auftragnehmern, soweit personenbezogene Daten im Auftrag verarbeitet werden.

Da sich Unternehmen und Geschäftsprozesse kontinuierlich verändern, unterliegen auch die Löschrprozesse einem stetigen Wandel. Soll ein Löschkonzept nicht nur die Augenblicksskizze eines Unternehmens wiedergeben, sondern als dauerhafter Prozess gelebt werden, ist es schließlich erforderlich, die Anpassung des Löschrkonzepts als einen Teil des allgemeinen Change-Managements aufzufassen. Der bDSB wie die anderen Verantwortlichen müssen an diesem Anpassungsprozess mitwirken.

Die Erstellung eines Löschkonzeptes erfordert die konzeptionelle und inhaltliche Zusammenarbeit zwischen dem bDSB, der Rechtsabteilung und den IT-Verantwortlichen eines Unternehmens. Die Erstellung eines Löschkonzepts ist also ein interdisziplinäres Projekt, dessen Erfolg wesentlich davon abhängt, dass die Notwendigkeit des Löschkonzepts den Akteuren vermittelt wird. Dies kann gelingen, wenn deutlich wird, dass die Erstellung des Löschkonzepts nicht Selbstzweck ist, sondern dem Unternehmen selbst vielfältige Vorteile erschließt.

Zur Struktur eines unternehmensweiten Löschkonzepts

Das Löschkonzept setzt ein Oberdokument voraus. Wir nennen es **Regellöschfristen**. In diesem Oberdokument müssen zunächst einmal unabhängig von den Systemen alle im Unternehmen vorkommenden Datenarten analysiert und aufgrund der vorhandenen Rechtsnormen Löschrufen bestimmt werden. Die Erstellung und Pflege dieses Oberdokuments sollte die Aufgabe des Datenschutzbeauftragten bzw. des Datenschutzteams, natürlich in enger Abstimmung mit allen Fachabteilungen sein. Um einem entsprechenden Oberdokument die verbindliche Wirkung zu verleihen, ist es auch notwendig, dass die Geschäftsführung eines Unternehmens dieses Dokument beschließt. Damit wird dieses Dokument Teil der unternehmensverbindlichen Regeln.

Die Umsetzung aber dieses Löschkonzeptes muss von den Fachabteilungen geleistet werden. D. h. auf Basis der vorgegebenen Regeln müssen für die einzelnen Systeme Systemlöschkonzepte erstellt werden. Für die Erstellung dieser Systemlöschkonzepte, also beispielsweise für das SAP-System oder für ein CRM-System, für HP Openview oder Peoplesoft, aber auch, um es im Hinblick auf Mitarbeiterdaten nicht zu vergessen, für Telefonanlagen, was insbesondere dann wichtig ist, wenn im Unternehmen auch ein Callcenter betrieben wird. Für all diese Systeme müssen nach den in den Regellöschfristen vorgegebenen Fristen für die in den jeweiligen Systemen verarbeiteten Datenarten Systemlöschkonzepte erstellt werden. Sie zu erstellen ist, wie gesagt, Aufgabe der Fachabteilungen. Deswegen auch muss man die Fachabteilungen, die ja die Regellöschfristen umsetzen sollen, in den Prozess der Erarbeitung einbinden. Natürlich unterstützt der Datenschutzbeauftragte bei der Erstellung der so genannten SLKs, die er auch freigibt.

Diese Prozedur ist mühsam aber ertragreich. Auf der einen Seite wird der bDSB nicht als lästige Prüfinstanz, sondern als Kollege und aktiver Mitarbeiter wahrgenommen. Der

Datenschutzbeauftragte lernt auf diese Weise nicht nur die Menschen kennen, die operativ mit Daten umgehen, sondern er lernt auch alle Systeme im Unternehmen kennen, mit denen personenbezogene Daten verarbeitet werden. Er erhält auf diese Weise noch einen viel tieferen Einblick in die Datenverarbeitung des Unternehmens als es die bloße Gestellung eines Verfahrensverzeichnis mit sich bringen würde. Den Gesamtüberblick, den er auf diese Weise erhält, versetzt ihn auch in die Lage, redundante Datenhaltungen zu erkennen bzw. aufzudecken und daraufhin zu wirken, **redundante Datenhaltungen** auf ihre Notwendigkeit hin zu befragen und im Zweifel darauf hinzuwirken, redundante Datenhaltungen abzuschaffen.

Vor allem aber dienen die Systemlöschkonzepte als Folie für **interne Datenschutzaudits**. Ein Löschkonzept ist nichts wert, wenn seine Einhaltung nicht überprüft wird. Da ein ausgereiftes Systemlöschkonzept alle in einem System gehaltenen Tabellen bis hin auf die Feldinhalte einzelner Tabellen benennt und Löschparameter vorgibt, ist es dann entsprechend einfach, auf Datenbankebene die Einhaltung der Löschparameter zu überprüfen.

Der Prozess der Datenverarbeitung wird auf diese Weise zunehmend eben von **seinem Ende her gedacht**. Dies verhindert eine naturwüchsige Ausbreitung von Systemen. Auf diese Weise erweist sich die römische Weisheit „Was auch immer es ist, tue es klug und bedenke das Ende“ zu einer hochaktuelle Maxime moderner Datenverarbeitung.

Ich danke Ihnen, meine Damen und Herren, für Ihre Aufmerksamkeit. Hoffe, dass ich Sie nicht gelangweilt habe und stehe jetzt für weitere Fragen gern zur Verfügung.