DSGVO VS. ÖFFENTLICHE VERWALTUNG

Warum Automatisierung von Datenschutz in der öffentlichen Verwaltung unverzichtbar ist.

| von JOCHEN ZELLMER

Mit der Einführung der Datenschutzgrundverordnung (DSGVO)[1] hat sich im Datenschutz vieles geändert, zum Beispiel bei Dokumentationspflichten, Vorschriften zur Datenverarbeitung und Geldbußen.

Aus IT-Sicht sind dabei zwei verschiedene Arten von Änderungen interessant. Zum einen diejenigen, die ohne IT nicht umgesetzt werden können, wie zum Beispiel Datenschutzerklärungen auf Webseiten und Bestätigungen von Cookies. Zum anderen solche Änderungen, für die eine IT-Unterstützung zwar nicht zwingend erforderlich ist, bei denen aber hohe Aufwände bei manueller Umsetzung entstehen – dazu zählen insbesondere die Auskunftspflicht und Löschpflicht, mit denen sich dieser Beitrag beschäftigt.

DATENSCHUTZHISTORIE IN DEUTSCHLAND

Das weltweit erste Datenschutzgesetz wurde 1970 im Bundesland Hessen eingeführt. 1977 folgte in Deutschland ein bundesweites Gesetz, das BDSG (Bundesdatenschutzgesetz).[2] Die im Jahr 1995 verabschiedete europäische Richtlinie mit Schwerpunkt auf die Verarbeitung personenbezogener Daten (Richtlinie 95/46/EG[3]) führte im Jahr 2001 zu einer Novellierung des BDSG. Die Verarbeitung von Cookies wurde in der europäischen Richtlinie 2009/136/EG[4] festgelegt und 2009 in das BDSG übernommen.

Die DSGVO vereinheitlichte und modernisierte den Datenschutz im Jahr 2016 für ganz Europa. Das Gesetz wurde nach einer zweijährigen Übergangszeit 2018 für alle Mitgliedsstaaten rechtskräftig.

WICHTIGE ÄNDERUNGEN DURCH DIE DSGVO

Die DSGVO verfolgt insbesondere das Ziel, den Datenschutz in Europa zu vereinheitlichen und zu modernisieren. Mit ihr fallen die meisten individuellen Ausprägungen von Gesetzen in verschiedenen EU-Mitgliedsstaaten weg und erleichtert sich die korrekte Umsetzung über Ländergrenzen hinweg.

Die Dokumentationspflichten wurden zum Teil ausgeweitet oder angeglichen. Es ist zum Beispiel nun erforderlich, die Verarbeitung personenbezogener Daten in einer Datenschutzrichtlinie zu dokumentieren und für jede gespeicherte Information auch darlegen zu können, warum und wie lange diese gespeichert wird.

Die Rechte natürlicher Personen wurden deutlich erweitert. Die Verarbeitung von personenbezogenen Daten erfordert nun eine persönliche Einwilligung der natürlichen Person sowie eine Rechtsgrundlage, warum die Verarbeitung notwendig ist. Sobald die Verarbeitung nicht mehr erforderlich ist, müssen die Daten gelöscht werden (Verarbeitungsverbot, Datenminimierung und Löschpflicht). Zu allen verarbeiteten Daten haben natürliche Personen umfangreiche Auskunfts- und Informationsrechte sowie Rechte auf Berichtigung und Löschung.

Falls personenbezogene Daten im Auftrag durch Dritte verarbeitet werden, liegt die primäre Verantwortung und Haftung nun bei dem Beauftragenden. Das ist insbesondere bei Verwendung von Cloud-Diensten relevant, die in heutiger Zeit an Popularität gewinnen. Falls ein Unternehmen also einen Cloud-Dienst verwendet, ist das beauftragende Unternehmen für die Einhaltung des Datenschutzes innerhalb der Cloud oder des Hosting-Angebots verantwortlich. Bei einem Sicherheitsvorfall haftet zunächst das beauftragende Unternehmen und nachgelagert auch der Betreiber.

Sicherheitsvorfälle muss der Verantwortliche selbstständig bei der Aufsichtsbehörde sowie allen Betroffenen innerhalb von 72 Stunden anzeigen. Die Beweislast, dass alle Vorschriften eingehalten wurden, liegt grundsätzlich beim Verarbeiter der Daten. Sicherheitsvorfälle können nun auch erhebliche Geldbußen nach sich ziehen.

HÜRDEN BEI DER UMSETZUNG DER DSGVO

Die Umsetzung der DSGVO erweist sich zum Teil als komplex und aufwendig. Zunächst einmal müssen alle personenbezogenen Daten auffindbar sein. In komplexen, heterogenen IT-Landschaften liegen die Daten aber in unterschiedlichsten Formaten vor, zum Beispiel Datenbanken, analoge Dokumente, Multimedia-Dateien oder nicht durchsuchbare digitale Dokumente. Damit ist das Auffinden extrem zeitaufwendig und in manchen Fällen nur manuell möglich.

Alt-Anwendungen können durchaus nicht konform zur DSGVO sein. Diese anzupassen ist allerdings aufgrund von Kosten, ausgelaufenen Wartungsverträgen oder komplexen Schnittstellen zu anderen IT-Systemen nicht immer möglich. Nicht viele Anwendung, die heute auf dem Markt sind, unterstützen bereits die Regelungen, die durch die DSGVO vorgegeben

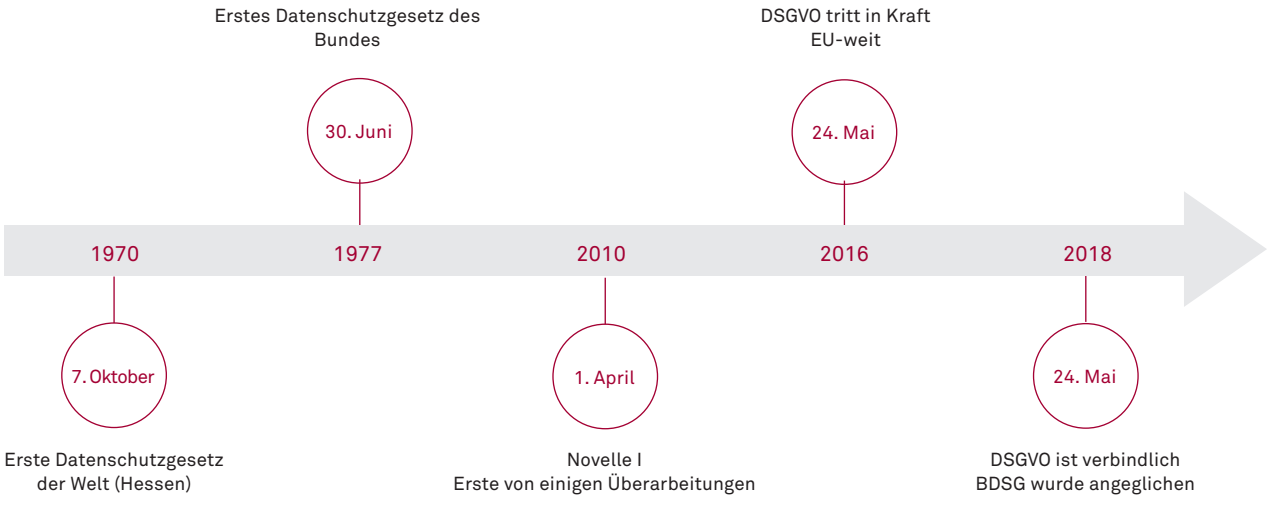

Abbildung 1: Datenschutzhistorie in Deutschland (vereinfachte Zeitschiene)

WICHTIGE ÄNDERUNGEN DURCH DIE DSGVO

Thema	Änderungen durch die DSGVO
Sicherheitskonzept (Art. 32 und 35 DSGVO)	• Datenschutzfolgeabschätzung (ehemals Vorabkontrolle) • Verzeichnis von Verarbeitungstätigkeiten • Datenschutzmanagement
Verarbeitungsverbot (Art. 4 Nr. 1 DSGVO)	• Persönliche Einwilligung notwendig • Rechtsvorschrift muss vorhanden sein
Datenminimierung (Art. 5 DSGVO)	• Nur die Erhebung von benötigten Daten • Personen mit Zugang nutzen diese nur zweckerfüllend
Löschpflicht (Art. 17 DSGVO)	• Nach Ablauf der Zweckhaftigkeit • Gesetzliche Aufbewahrungspflichten beachten
Informationspflicht (Art. 13 und 14 DSGVO)	• Offenlegung der Datenverarbeitung • Leicht zugänglich (z. B. verständlich, ggf. in Muttersprache)
Recht auf … (Art. 15-18 DSGVO)	• Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung • Bearbeitung innerhalb eines Monats • In Kenntnis setzen bei weitergegebenen Daten
Outsourcen (Art. 28 DSGVO)	• Auftraggeber ist für Datenschutz verantwortlich und haftet
Meldepflicht bei Sicherheitsvorfällen (Art. 33 DSGVO)	• Zerstörung, Verlieren, Verändern, unbefugter Zugriff, anderweitig verarbeitet oder gespeichert … • Meldung innerhalb 72 Stunden an Aufsichtsbehörde und Betroffene
Geldbußen (Art. 83 DSGVO)	• Bußgeld bis 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes des Vorjahres • Umkehrung der Beweislast – das Unternehmen muss faktisch belegen, dass die Vorschrift eingehalten wurde

werden. Insbesondere bei Speziallösungen für Behörden oder Kommunen ist die Auswahl für gute Softwareprodukte oft recht klein. Im Rahmen der Anschaffung müssen die Kosten für eine manuelle Abwicklung der DSGVO gegen eine Softwarelösung abwägt werden.

Cloudlösungen drängen mehr und mehr auf den Markt. Der gewonnene Komfort, einen schlüsselfertigen Dienst einzukaufen, bedeutet aber auch, dass das Vertrauen zum Anbieter entsprechend hoch sein muss, insbesondere nachdem die Verantwortung des Datenschutzes laut DSGVO nur nachgelagert beim Cloudanbieter liegt. Auch müssen Cloudlösungen die von der DSGVO geforderte Auskunfts- und Löschpflicht automatisiert anbieten, da ein manuelles Löschen durch die Sachbearbeitung noch schwieriger ist als im eigenen Haus.

AUSKUNFTSERSUCHEN HEUTE

Jede natürliche Person hat Anspruch auf Auskunft zu allen, zu ihrer Person gespeicherten Daten. Zusätzlich zu den Daten selbst müssen auch der Verarbeitungszweck, Speicherdauer, Herkunft der Daten und ggf. weitere Empfänger genannt werden.[5] Um dies zu bewerkstelligen, muss für jedes IT-System ein Konzept vorhanden sein, wie personenbezogene Daten gespeichert und bei einem Auskunftsersuchen gefunden werden können.

In der Praxis wird ein Auskunftsersuchen per E-Mail, Webformular oder Brief an den Datenschutzbeauftragen gesendet. Dieser verteilt die Anfrage auf alle infrage kommenden Organisationseinheiten oder Referate.

Bereits die Identifikation des Antragstellers ist in den verschiedenen Systemen unterschiedlich. Gerade in der öffentlichen Verwaltung reicht es nicht aus, einen Benutzernamen zu kennen, sondern jeder Bürger, egal ob er ein, mehrere oder gar kein Benutzerkonto erstellt hat, kann ein Auskunftsersuchen stellen. Die Identifikation erfolgt anschließend über die unterschiedlichsten Daten wie Name und Geburtsdatum, Steueridentifikationsnummer, Kindergeldnummer, Kfz-Kennzeichen, Personalnummer, IP-Adresse und vieles mehr.

In großen IT-Landschaften von zum Beispiel einer Behörde kann insgesamt von mehreren Tausend IT-Systemen ausgegangen werden, die personenbezogene Daten verarbeiten. Gehen wir von einer Behörde mit rund 3.000 solchen IT-Systemen aus, dann ist es essenziell, die Auswahl der für das Auskunftsersuchen relevanten Systeme von Anfang einzuschränken, was in der Regel aufgrund der Angaben im Ersuchen möglich ist. Die Anfrage könnte dann zum Beispiel auf eine einzelne Or-

ganisationseinheit beschränkt werden, die beispielsweise 50 IT-Systeme mit personenbezogenen Daten verwaltet. Der Datenschutzbeauftragte leitet dann die Anfrage an diese oder alle relevanten Organisationseinheiten weiter.

Für die im Beispiel genannten 50 IT-Systeme muss für das Auskunftsersuchen ermittelt werden, ob Daten des Antragstellers gespeichert sind. Falls in einem IT-System keine relevanten Daten enthalten sind, dauert diese Recherche pro IT-System mindestens einige Minuten. Falls Daten gespeichert sind, müssen diese aufwendig aufgefunden, herauskopiert und mit den notwendigen Metadaten angereichert werden – also zum Beispiel woher die Information kommt und wofür und für wie lange diese Information gespeichert wird. Die Erfahrung zeigt, dass dieser Vorgang mehrere Stunden oder sogar einige Tage für jedes System benötigt – je nach Komplexität und Menge der Daten. Leider bieten auch die wenigsten IT-Systeme eine Möglichkeit, die relevanten Daten zu einer Person als Dokument auszugeben. Gehen wir davon aus, dass von den 50 genannten Systemen 45 keine Daten zum Antragsteller speichern, dann sind ca. 45 mal 15 Minuten, also rund 1,5 Arbeitstage nötig, um diese Information zu ermitteln. Für die restlichen fünf Systeme gehen wir von recht wenigen Daten und einem Durchschnitt von je einem halben Tag aus, um die Daten zu extrahieren und anzureichern. Dann dauert die Datenrecherche rund vier Arbeitstage.

Die gespeicherten Daten liegen meist in vielfältigen Formaten vor – beispielsweise Datenbanken, DMS-Systeme (zum Beispiel Anhänge), Log-Dateien, Multimedia-Dateien und analoge Dokumente. Je nach Quellformat werden die gefunden Daten in einem sinnvollen Format an den Datenschutzbeauftragen zurückgeschickt. Dieser sammelt alle Daten für das entsprechende Auskunftsersuchen und sendet die Antwort per Post zurück. Die digitale Zustellung der Antwort ist in der Regel nicht möglich, da der Austausch verschlüsselt erfolgen müsste und ein Austausch von Zertifikaten für E-Mail oder Ähnliches zwar standardisiert, aber kaum verbreitet ist.

Wie hoch der Aufwand für ein Auskunftsersuchen tatsächlich ist, kann pauschal sehr schwer beantwortet werden. Einfache Fälle mit sehr wenigen oder gar keinen Daten können, wie im Beispiel oben, mit wenigen Personentagen beantwortet werden, komplexe Fälle erfordern deutlich mehr Bearbeitungszeit.

Für die Bearbeitung von Auskunftsersuchen räumt die DSGVO bis zu einem Monat Zeit ein. Eine denkbare Aufteilung wäre: eine Woche für die Verteilung der Anfrage an die notwendigen Organisa-

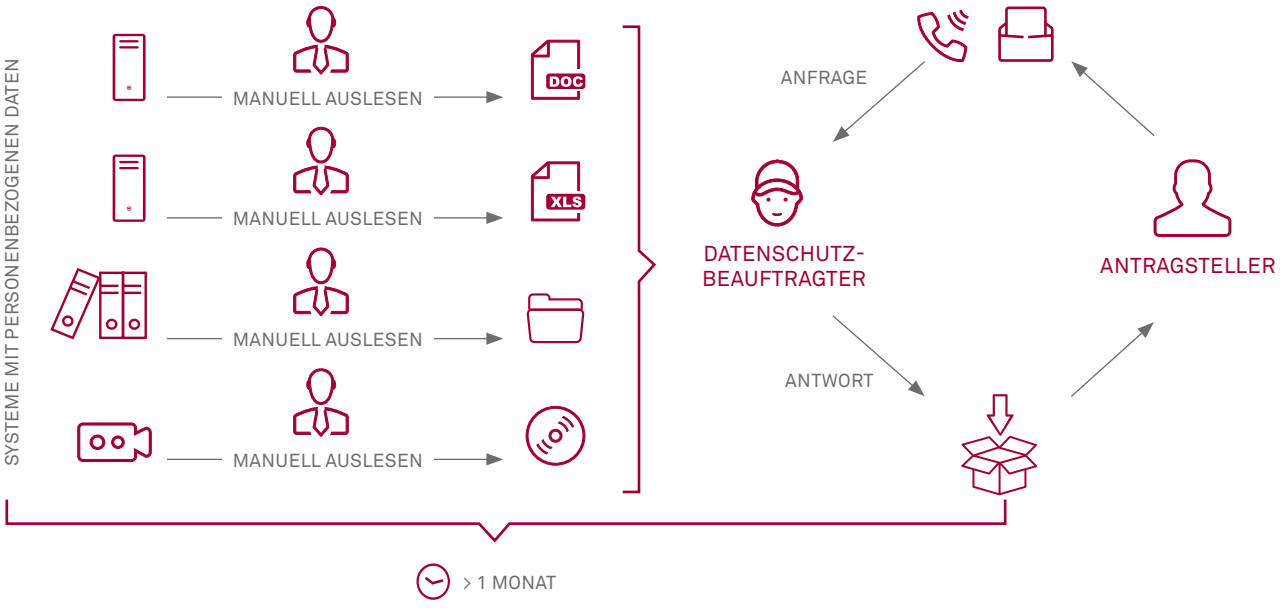

Abbildung 2: Ablauf eines Auskunftsersuchens heute

tionseinheiten, zwei Wochen zum Sammeln der Informationen und eine Woche für die Rücksendung. Insgesamt ist das eine recht kleine Zeitspanne, insbesondere, wenn man die Fülle an Systemen und Daten betrachtet.

AUSKUNFTSERSUCHEN ALS „AUSKUNFTSPORTAL“

Statt die Auskunft manuell zu erstellen, wäre ein Auskunftsportal für Selbstauskunft im Internet denkbar. Die Vorteile liegen auf der Hand, die Auskunft würde durch den Antragsteller selbst durchgeführt und quasi in Echtzeit erfolgen. Die Kosten für eine Auskunft würden sich erheblich reduzieren.

Die Einführung eines Auskunftsportals ist allerdings nicht einfach. Auf fertige Standardprodukte kann leider nicht zurückgegriffen werden, sondern es bedarf einer Make-Lösung.

Damit die gesamte Zielgruppe das Auskunftsportal verwenden kann, müsste sichergestellt werden, dass sich jeder anmelden kann. Das ist insbesondere im öffentlichen Sektor eine Herausforderung, da die Zielgruppe alle Bürger umfasst. In Deutschland gibt es derzeit nur wenige Standards für die digitale Authentifizierung aller Bürger (zum Beispiel die Online-Ausweisfunktion des Personalausweis[6]), und keines dieser Verfahren konnte sich bisher durchsetzen. Nach Anmeldung müsste diese Person auch in allen IT-Systemen identifiziert werden, was aufgrund der unterschiedlichen Daten (vgl. oben) nicht ohne Weiteres gegeben ist.

Um IT-Systeme an das Auskunftsportal anbinden zu können, müssen alle personenbezogenen Daten zu einer Person aus den anzubindenden Systemen automatisiert abgerufen werden können. Leider bieten heute kaum Systeme diese Möglichkeit an. Für einige IT-System wäre die Nachrüstung durchaus möglich, zum Teil sogar mit geringem Aufwand verbunden. Allerdings gibt es heute – trotz DSGVO – kaum Nachfrage für diese Funktion und wird durch Softwareanbieter damit auch nicht in ihre Produkte aufgenommen. Das Nachrüsten von Altanwendungen ist in vielen Fällen kaum oder gar nicht möglich. Hier ergeben sich Hürden in Form von nicht mehr aktiv entwickelten Produkten, bereits in der Ablöse befindlichen Systemen, zu hohen Kosten für die Änderungen oder bereits abgelaufenen Wartungsverträge.

Die Einführung eines Auskunftsportals für große IT-Landschaften mit heterogenen Datenbeständen für alle IT-Systeme gleichzeitig ist aufgrund der oben genannten Punkte kaum möglich. Stattdessen wäre der Aufbau eines Auskunftsportals durch folgende Maßnahmen denkbar:

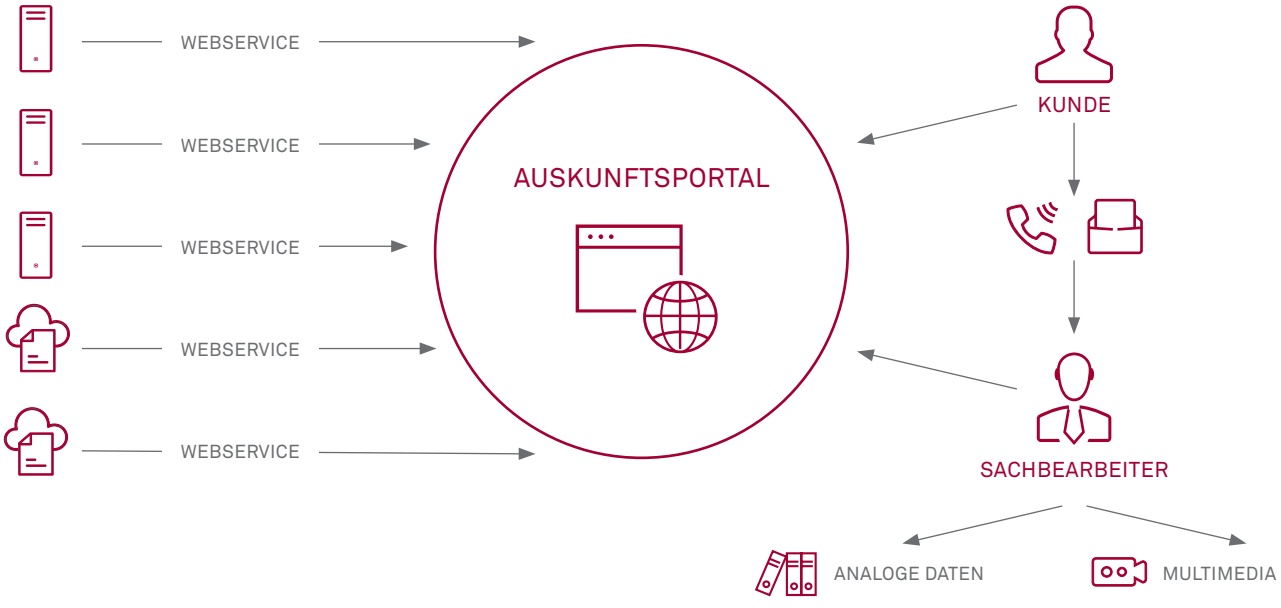

Abbildung 3: Auskunftsersuchen über ein Auskunftsportal

1. Neue IT-Systeme werden standardmäßig an das Auskunftsportal angebunden (Festlegung über IT-Richtlinie)
2. Alt-Systeme werden bei Umstellung angebunden oder, falls technisch und mit vertretbarem Aufwand möglich, auch innerhalb der Laufzeit

UMSETZUNG DER LÖSCHPFLICHT

Die in der DSGVO vorgeschriebene Löschpflicht erfordert das unverzügliche Löschen von personenbezogenen Daten, sobald die gesetzliche Aufbewahrungspflicht erloschen ist oder eine Person von ihrem Recht auf Löschen Gebrauch macht. Doch so einfach das Löschen scheint, so komplex und vielschichtig ist es in der Praxis.

Zunächst stellt sich die Frage, wie die einzelnen IT-Systeme die Löschfunktion grundsätzlich umsetzen. Werden Daten in einer Benutzeroberfläche gelöscht, können diese beispielsweise aus der Datenbank gelöscht oder als gelöscht markiert werden. Im Falle von Löschmarkierungen sind die Daten weiterhin gespeichert und damit das System nicht konform zur DSGVO. Dazu kommen Protokolle und Logdateien, die personenbezogene Daten wie Benutzernamen, IP-Adressen etc. beinhalten können. Löschvorgänge beziehen solche Daten in der Regel nicht ein, da dies technisch aufwendig ist und ein Interessenkonflikt für gegebenenfalls notwendige Fehlersuche oder Beweispflichten darstellt.

Die Back-up-Strategie muss ebenfalls geprüft werden. Ein Löschvorgang in der Benutzeroberfläche löscht die personenbezogenen Daten nicht aus eventuell erstellten Back-ups. Der Löschvorgang ist also genau genommen erst dann abgeschlossen, wenn das letzte Back-up, das die Daten beinhaltet, ebenfalls entfernt wurde. Im Falle eines Back-up-Restore müssten auch alle Löschvorgänge erneut durchgeführt werden, da sonst die Löschpflicht verletzt wird.

Betrachtet man Schnittstellen zwischen IT-Systemen, wird eine weitere große fachliche und technische Komplexität der Löschpflicht offenbar. Das Löschen einer Information aus einem System reicht in komplexen IT-Landschaften nicht aus. Vielmehr muss der Datensatz auch in allen nachgelagerten und vorgelagerten Systemen ebenfalls gelöscht werden – falls dies mit der gesetzlichen Aufbewahrungspflicht konform ist. In der Praxis ist dies leider nicht der Fall.

Beispielsweise müssen die meisten Daten aus der Personalakte nach Ausscheiden des Mitarbeiters nach spätestens zehn Jahren gelöscht werden.[7] Ein nachgelagertes Arbeitsschutzmanagementsystem erfordert aber, dass Daten rund um eine Person in einigen Fällen bis zum 75. Lebensjahr aufgehoben werden müssen. Allerdings gibt es auch Daten im Arbeitsschutz, die bereits nach einem Jahr zu löschen sind. Für all diese Fälle muss sichergestellt werden, dass Schnittstellen nicht dazu führen, dass entweder Daten zu lange aufgehoben oder zu früh gelöscht werden. Die Folge sind umfangreiche Anpassungen bestehender Schnittstellen, um die Löschpflicht korrekt umzusetzen.

Schnittstellen zu Dritten, also die Weitergabe von Daten, müssen ebenfalls dokumentiert werden und können durchaus andere Aufbewahrungsfristen als die zu löschenden Daten haben. Hinzu kommt, dass diese Information, auch wenn die Daten im eigenen System bereits gelöscht sind, bei einem Auskunftsersuchen relevant sein können.

Nach heutigem Stand sind die meisten IT-Systeme so aufgebaut, dass von den Anwendern bzw. Sachbearbeitern erwartet wird, die Daten nach eigenen Bedürfnissen zu löschen. Die oben dargestellte Komplexität sollte bereits zeigen, dass dieser Vorgang sehr zeitaufwendig und fehleranfällig und durch die Sachbearbeitung nicht zu leisten ist.

Ein möglicher Weg, die Löschpflicht zu automatisieren, wäre, das durch die DSGVO vorgeschriebene Löschkonzept, als Metamodell zum fachlichen Datenmodell mitzuführen. Für jede gespeicherte personenbezogene Information ist die zeitliche Aufbewahrungspflicht im Löschkonzept zu benennen, und ein IT-System wäre anhand dieser Information in der Lage, zu löschende Daten automatisch zum korrekten Zeitpunkt zu entfernen.

FAZIT

Die durch die DSGVO erweiterten Dokumentations-, Auskunfts- und Löschpflichten führen zu zusätzlichen Pflichten und damit auch zu Aufwänden bei der Umsetzung des Datenschutzes. Bei der Umsetzung dieser Pflichten müssen in jedem Fall ein Konzept zur Datenspeicherung und ein Löschkonzept erstellt werden.

Dass Auskunftsersuchen und die Löschpflicht nach heutigem Standard manuell bearbeitet werden, führt dazu, dass die Aufwände sehr hoch sind. Eine Automatisierung wäre zwar möglich, und der

Grundstein für die Automatisierung der Auskunfts- und Löschpflichten durch die gesetzlich vorgeschriebenen Konzepte ist bereits gelegt, doch es fehlt die Umsetzung in den jeweiligen IT-Systemen. Die Automatisierung von Auskunftsersuchen erfordert, alle personenbezogenen Daten zu einer Person automatisiert aus einem IT-System ausgeben zu können, idealerweise angereichert mit den oben genannten Metainformationen. Das Ausgabeformat könnte entweder ein Office-Dokument sein, das durch den Datenschutzbeauftragten ausgedruckt und zurückgesendet werden kann, oder ein Webservice, damit ein Auskunftsportal die Information abfragen kann.

Um die Löschpflicht zu automatisieren, muss der Zeitpunkt der Löschung für jede personenbezogene Information im IT-System hinterlegt werden. Die Software könnte dann anhand dieser Information die Löschung automatisch vornehmen.

Beide Funktionen sind heute nicht Standard und können, je nach IT-System, auch nicht ohne Weiteres in eine bestehende Software eingefügt werden. Die Umsetzung bedarf vielmehr einer wohlüberlegten Planung und größeren Änderungen in der vorhandenen Software. Aus der Sicht der IT-Architektur ist der Datenschutz ein essenzielles Querschnittsthema, das in Zukunft Bestandteil der grundlegenden Systemarchitektur sein sollte.

Bei Kaufsoftware und Cloudlösungen müssen die Änderungen durch die Softwareanbieter erfolgen. Die öffentliche Verwaltung sollte daher bereits bei der Vergabe darauf achten, dass diese Anforderungen bei der Ausschreibung berücksichtigt werden. Im Rahmen von Individuallösungen sollten die Anforderungen durch eine entsprechende IT-Richtlinie vorgegeben werden.

Um das Ziel der Automatisierung für Auskunfts- und Löschpflicht zu erreichen, wird ein längerer, mehrstufiger Prozess notwendig sein. Ein erster guter Schritt wäre, so viele IT-Systeme wie möglich mit den genannten Automatismen auszustatten, um die Sachbearbeitung zu entlasten und die IT-Systeme für die Anbindung an ein Auskunftsportal vorzubereiten. Ein Auskunftsportal könnte dann zunächst intern für den Datenschutzbeauftragten und später für die Bürger geöffnet werden.

Teile des Datenschutzes können durch IT-Systeme automatisiert werden. Und dabei sollte bei der Auskunfts- und Löschpflicht nicht haltgemacht werden. Noch gibt es viele Herausforderungen, diese Ziele zu erreichen. Bei Erfolg würden sich auf mittel- bis langfristige Sicht die manuellen Aufwände für die konforme Umsetzung und operative Durchführung des Datenschutzes stark reduzieren. Gleichzeitig bedient diese Vorgehensweise die Bemühungen, vermehrt Dienste für die Bürger online bereitzustellen und auch in diesem Bereich die Digitalisierung voranzutreiben. ●

1 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679, (Gesetzestext DSGVO – abgerufen am 11.04.2019).
2 https://de.wikipedia.org/wiki/Datenschutz (abgerufen am 26.05.2019).
3 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A31995L0046 (abgerufen am 26.05.2019)
4 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:de:PDF (abgerufen am 26.05.2019).
5 https://www.datenschutz.org/19-34-bdsg/ (abgerufen am 16.04.2019)
6 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Elektronischeldentitaeten/Online-Ausweisfunktion/online-ausweisfunktion_node.html (abgerufen am 27.4.19).
7 https://www.personal-wissen.net/wissen/aufbewahrungsfristen-personalwesen-so-lang-muessen-personalakten-archiviert-werden-785/ (abgerufen am 27.4.19).