Europäischer Datenschutz

Wer speichert, muss auch löschen

Die EU-DSGVO bringt die Altsysteme in den Fokus der Datenschutzverantwortlichen – technisch wie finanziell.

Von Thomas Failer, Data Migration Services

Der Countdown läuft: In weniger als vier Wochen endet die Übergangsfrist der europäischen Datenschutz-Grundverordnung (EU-DSGVO). Doch die notwendigen technischen und organisatorischen Maßnahmen, um die Auflagen der Verordnung umfassend zu erfüllen, finden offenbar nur langsam ihren Weg auf die Prioritätenliste der IT-Verantwortlichen. So heißt es in einer IDC-Pressemitteilung vom Oktober 2017: „44 Prozent der befragten Organisationen haben noch keine konkreten Maßnahmen zur Erfüllung der Anforderungen gestartet, darüber hinaus fehlt vielen immer noch der ganzheitliche Blick auf alle personenbezogenen Daten im Unternehmen."

„Diese Situation kann ich aus meinen zahlreichen Gesprächen mit Geschäftsführern und Vorständen in den vergangenen Wochen und Monaten nur bestätigen", sagt Simon T. Oeschger, auf Datenschutzrecht spezialisierter Anwalt bei der Schweizer Kanzlei Suffert, Neuenschwander und Partner. „Schon die ersten drei Fragen, wo welche Daten liegen und wer darauf zugreift, versetzen viele meiner Gesprächspartner in Panik."

Thomas Failer,
Gründer von Data Migration Services.

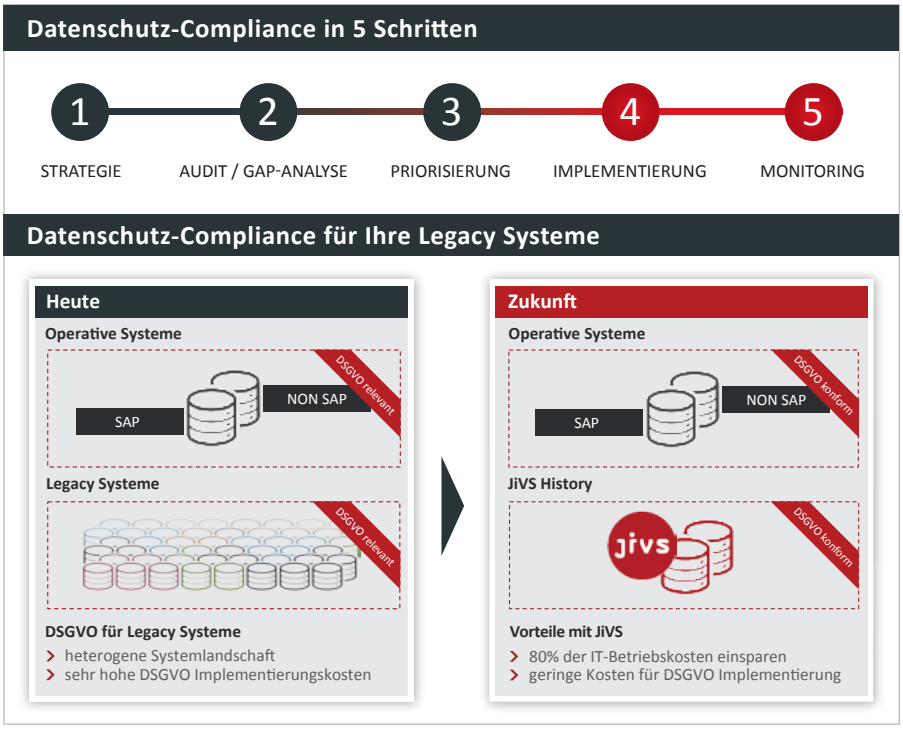
Im Grunde ist dieser Befund erstaunlich. Denn die meisten Grundsätze der neuen Verordnung sind seit Jahren Bestandteil früherer Gesetzgebungen, insbesondere des deutschen Bundesdatenschutzgesetzes. Dazu zählen etwa die Prinzipien der Datensparsamkeit, der Verhältnismäßigkeit, der Zweckbindung oder der Transparenz. „Das ist alles seit Jahren bekannt, doch die bisherigen Regularien waren eher zahnlose Tiger", weiß Simon Oeschger aus der Praxis. Und auch das neue Gesetz macht es den Verantwortlichen nicht leicht, die Brisanz des Themas zu verstehen.

Nur Bäume, kein Wald

Laut Oeschger ist der Gesetzestext umfangreich und vielfach für Laien nicht ohne Weiteres verständlich, was wirklich zu tun ist. „Das ist der berühmte Wald, den man vor lauter Bäumen nicht mehr sieht", resümiert der Anwalt.

Greift man jedoch einige der neuen Pflichten aus dem Regelwerk heraus und sieht sie sich näher an, zeigen sich schnell ihre Konsequenzen in allen Bereichen und Ebenen eines Unternehmens: So sind die Firmen ab Ende Mai Kunden und betroffenen Personen gegenüber auskunftspflichtig. Diese haben das Recht zu erfahren, welche personenbezogenen Daten die Unternehmen gespeichert haben, für welche Verarbeitungszwecke die Daten erhoben wurden und ob diese Speicherung zulässig war und ist. Darüber hinaus müssen die Firmen ein Verzeichnis zu den Zwecken erstellen und führen, für die diese Daten erhoben und aufbewahrt wurden. Stellt sich dabei heraus, dass zu viele Daten abgelegt sind, müssen die Unternehmen in der Lage sein, einzelne Datensätze gezielt zu löschen.

„Spätestens ab diesem Zeitpunkt ist klar, dass die neue Verordnung eine Aufgabe für die Geschäftsleitung und Vorstände ist", erklärt Simon Oeschger. „Mehr noch: Der Schutz personenbezogener Daten muss Teil des allgemeinen Risikomanagements werden. Das hat sowohl technische als auch organisatorische Konsequenzen. Dafür braucht es freilich digitales Know-how in den Unternehmensleitungen, das notfalls eingekauft werden muss."



Datenschutz-Compliance in 5 Schritten.

Dennoch besteht laut Oeschger kein Grund zur Panik. Das Wichtigste sei es, nicht die Hände in den Schoß zu legen, weil man die Frist bis Ende Mai 2018 sowieso nicht einhalten könne. Er empfiehlt, umgehend ein Projekt zu starten, um die größten Datenschutzdefizite zu beseitigen und damit schrittweise mit dem neuen Recht konform zu werden, auch wenn dies erst nach dem Stichdatum erreicht werden könne. So ließen sich auch die Rechtsrisiken reduzieren: Die drakonischen Geldbußen würden nach den Umständen des Einzelfalls verhängt, wobei gebührend berücksichtigt werde, welche Bemühungen zur Einhaltung des Gesetzes vorgenommen worden seien.

Fünf Schritte zur Datenschutzkultur

Der erste Schritt auf dem Weg zum digitalen Risikomanagement ist die Datenbestandsaufnahme. Das Unternehmen muss genau ermitteln, wo welche personenbezogenen Daten abgelegt sind. Dies ist die Voraussetzung für Schritt zwei, die GAP-Analyse. Sie dient der Ermittlung der Hauptrisiken und damit drittens ihrer Gewichtung, woraus sich unmittelbar eine priorisierte Liste mit den zu treffenden Maßnahmen ableitet. Der vierte Schritt ist laut Oeschger die Implementierung der Maßnahmen. Dazu gehören Prozesse ebenso wie die Neuformulierung von Verträgen bis hin zu regelmäßigen Schulungen des Personals. Der fünfte Schritt besteht darin, eine Datenschutzkultur auf Basis iterativer Prozesse einzuführen und zu leben. „Die Unternehmenslenker müssen begreifen, dass es sich beim Datenschutz nicht um ein Einmalprojekt handelt“, betont Simon Oeschger. Vielmehr zeichne sich eine Datenschutzkultur durch iterative Prozesse wie regelmäßige Revisionen und Risikoanalysen aus.

Alles beginnt also mit der Datenbestandsaufnahme. Diese darf aber nicht bei den Produktivsystemen haltmachen. Denn aufgrund diverser Aufbewahrungspflichten und -fristen liegt ein Teil der schützenswerten personenbezogenen Daten in Altsystemen. Dabei gilt die Faustregel: Je größer ein Unternehmen, desto höher fällt dieser Anteil aus. So hat bereits 2011 der erste Application Landscape Report von Capgemini zutage gefördert, dass die Hälfte der großen Unternehmen davon ausgeht, jedes zweite Altsystem abschalten zu können. Und im Bericht von 2014 gaben die Befragten an, darin nicht nur eine Möglichkeit, sondern eine Notwendigkeit zu sehen. Grund ist in vielen Fällen die Modernisierung der ERP-Landschaft in den vergangenen Jahren, die gleichzeitig mit einer Konsolidierung und Zentralisierung einhergeht. Das bedeutet, dass viele verschiedene Altsysteme auf wenige zentrale Live-Systeme migriert werden. Doch nur ein Teil der Daten wird dabei in die neue Umgebung übernommen.

Das ist der berühmte Wald, den man vor lauter Bäumen nicht mehr sieht.

Simon T. Oeschger, auf Datenschutzrecht spezialisierter Anwalt bei der Schweizer Kanzlei Suffert, Neuenschwander und Partner, zur DSGVO.

Mit dem anstehenden Umstieg auf S/4 Hana wird diese Konsolidierungs- und Zentralisierungswelle weiter anschwellen. Trotz aller Startschwierigkeiten bei der Markteinführung und anhaltender Kritik aus der SAP-Community zeigt eine im Frühsommer 2017 von der Deutschsprachigen SAP-Anwendergruppe (DSAG) durchgeführte Online-Befragung von 500 Entscheidern im deutschsprachigen Raum: Mittlerweile investieren knapp 64 Prozent der befragten Unternehmen in SAP S/4 Hana in den Varianten Cloud und on-premise. Bis 2020 wird ein Drittel der SAP-Bestandskunden auf die neue Softwaregeneration aus Walldorf umsteigen und schon heute planen weitere 20 Prozent die Migration für die Zeit nach 2020.

Weniger Pflicht als Kür

Einer der Hauptgründe für Konsolidierung und Zentralisierung heißt Kostenersparnis. Denn der Umstieg auf neue Softwaregenerationen kostet viel Geld – Geld, das eigentlich nicht vorhanden ist. Zwar sind laut einer Umfrage der Deutschsprachigen SAP-Anwendergruppe die IT-Budgets 2017 durchschnittlich um fast fünf Prozent gegenüber dem Vorjahr gewachsen.

Doch selbst eine so deutliche Steigerung wird nicht ausreichen, um den IT-Abteilungen die finanziellen Mittel bereitzustellen, die sie für die Digitalisierung ihrer Unternehmen und deren Geschäftsmodelle benötigen werden. Dass nicht mehr Mittel zur Verfügung stehen, liegt daran, dass rund 80 Prozent des gesamten IT-Budgets der reine IT-Betrieb verbraucht, während nur 20 Prozent für Investitionen in Innovationen zur Verfügung stehen. Umfragen zeigen das immer wieder. Allein 70 Prozent entfallen oftmals auf den Aufwand für Altsysteme. Ideal wäre hingegen eine Aufteilung von 60 Prozent für den IT-Betrieb und 40 Prozent für Innovationen, und zwar dauerhaft.

Dieses Ziel ist jedoch nur zu erreichen, wenn die Altsysteme dauerhaft abgeschaltet werden. „Genau hier liegt die Schnittmenge zwischen Datenschutz und Betriebswirtschaft“, betont Simon Oeschger. „Denn durch die Bestandsaufnahme in Schritt eins rücken die Altsysteme wieder in den Fokus. Die Unternehmen können es sich einfach nicht leisten, diese wegen der Datenschutz-Grundverordnung wieder in Betrieb zu nehmen.“

Zu den Kostenüberlegungen kommen aber noch technische Limitierungen hinzu. So bieten viele Altsysteme gar keine Möglichkeit, gezielt Datensätze zu löschen. Auch die Nachrüstung ist in vielen Fällen gar nicht möglich, denn zumindest zum Teil sind diese Systeme bereits aus der Wartung der Hersteller herausgenommen oder befinden sich im rein lesenden Betrieb.

Historisierung statt Archivierung

Was nottut, ist ein Perspektivenwechsel. Oft entpuppt sich ein Problem als die Lösung für ein anderes. Wenn es wegen der neuen Verordnung nötig, aber zu teuer ist, Altsysteme weiterzubetreiben oder gar aus dem Winterschlaf zu holen; wenn es andererseits nicht genügend finanzielle Spielräume für die Modernisierung der IT gibt, diese aber genau dafür gebraucht werden, dann bleibt nur ein Ausweg: den teuren Betrieb von Altsystemen zu beenden und dadurch den damit verbundenen operativen Kostenblock dauerhaft zu senken.

So wird die Compliance-Pflicht zur Kür. Voraussetzung dafür ist allerdings ein neuer Ansatz für das Datenmanagement. Das betrifft im Übrigen nicht nur Daten, sondern auch Dokumente, die personenbezogene Daten enthalten.

Daten und Dokumente existieren darüber hinaus nicht für sich allein, sondern stehen in einem spezifischen Geschäftskontext. Um entscheiden und rechtfertigen zu können, ob personenbezogene Informationen zu Recht erhoben wurden und aufbewahrt werden, muss dieser Kontext mit erhalten werden, will man Altsysteme auf Dauer abschalten. Es geht also nicht um Archivierung, sondern um das Management des gesamten Lebenszyklus von Informationen. Bezogen auf Altdaten und -dokumente ist es deshalb sinnvoller, von Historisierung zu sprechen.

Wie bei der Modernisierung von IT-Umgebungen gilt auch bei der Historisierung der Grundsatz der Standardisierung. Das ist eine Kerneigenschaft von JiVS, einer zentralen Lösung für das Management historisierter Daten und Dokumente. Mithilfe der Java-basierenden Plattform und insbesondere ihrer Komponente „JiVS History for GDPR“ lassen sich die aus stillgelegten Altsystemen übernommenen Informationen mit Aufbewahrungsfristen belegen und nach Ablauf der gesetzlichen Aufbewahrungsfristen unwiederbringlich und automatisch löschen. Zudem erlaubt dieses umfassende „Retention Management“, das automatisierte Löschen für Ausnahmefälle wie laufende Gerichtsverfahren auf der Ebene der einzelnen Datensätze und Dokumente im Sinne eines sogenannten Legal Hold auszusetzen.

In der Praxis hat JiVS erwiesenermaßen nach der Stilllegung der Altsysteme die Betriebskosten um 80 bis 90 Prozent gesenkt. Mit den restlichen 10 bis 20 Prozent lassen sich die aus Compliance-Gründen aufzubewahrenden Altdaten inklusive SAP-Geschäftslogik weiterhin nutzen. Das bietet gleichzeitig eine einmalige Gelegenheit, die vorhandenen Datensätze und insbesondere die Stammdaten zu bereinigen. Gerade diese Bereinigung ist für den erfolgreichen Umstieg auf S/4 Hana aus Kostengründen entscheidend. Das gilt im Übrigen genauso und uneingeschränkt für die Erfüllung der Auflagen der EU-DSGVO, um dem Grundsatz der Datensparsamkeit zu genügen.

Fazit

SAP-Bestandskunden stecken in einem Dilemma zwischen Budgetzwängen einerseits und Innovationsdruck sowie Compliance-Anforderungen à la EU-Datenschutz-Grundverordnung andererseits. Die Stilllegung von Altsystemen und -archiven ist der Weg, der aus dieser Sackgasse führt.

Intelligente Plattformen reduzieren die Zahl der operativen SAP-Systeme und die Menge der darin vorgehaltenen Informationen. JiVS schafft die nötigen finanziellen Freiräume für die neue Generation der SAP-Software und macht die IT-Landschaften der Bestandskunden wetterfest für aktuelle und zukünftige Compliance-Auflagen. Dann klappt’s auch mit dem Löschen.

www.jivs.com

Bitte beachten Sie auch den Community-Info-Eintrag Seite 103

DATA MIGRATION SERVICES