EFFICIENT EXTENDED ENTERPRISE

EXTRA

Mai 2018 e-3.de

DSGVO

DAS WISSEN ZUR EU-DSGVO AUS DER SAP®-COMMUNITY

Persönlichkeitsschutz in Zeiten von Big Data und KI

Datenschutzraum Europa

Am 25. Mai startet der Praxistest. Lässt sich ein einheitlicher Datenschutz in der Europäischen Union umsetzen? Mit welchen Auswirkungen müssen Unternehmen, aber auch kleine Vereine rechnen?

Von Robert Korec, E-3 Magazin

Der Ansatz der Europäischen Union, das Menschenrecht auf Privatsphäre ins 21. Jahrhundert zu holen, war ambitioniert. Mit der DSGVO soll ein Ausgleich zwischen den Bürgerrechten des Einzelnen und der Freiheit des Datenverkehrs geschaffen werden. Für Unternehmen, aber auch ehrenamtlich geführte Vereine könnte das einen enormen Mehraufwand bedeuten.

Dass die neuen Spielregeln nicht ganz oben auf der Beliebtheitsskala stehen, lässt sich einerseits durch die empfindlichen Strafandrohungen von bis zu 20 Millionen Euro oder bis zu vier Prozent des weltweiten Jahresumsatzes erklären. Zum anderen war die Übergangsfrist, ab der die Nichteinhaltung der beschlossenen Regeln sanktioniert wird, für viele Unternehmen zu kurz angesetzt. Die DSGVO trifft auch kleinere Organisationen, etwa ehrenamtlich geführte Sportvereine, für deren Verantwortliche es kaum möglich ist, die 99 Artikel umfassende Verordnung auch nur ansatzweise zu verstehen, geschweige denn diese mit einem vernünftigen Zeitaufwand umzusetzen.

Ausgangssituation 1995

Um zu verstehen, warum sich Unternehmen und andere Organisationen mit einer Fülle an neuen Bestimmungen auseinandersetzen müssen, muss man auch im Blick behalten, dass die bisherigen Regelungen nicht weniger komplex waren. Die Ausgangssituation war jene, dass die in der Vorgängerregelung, der „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“, festgeschriebenen Regeln bereits aus dem Jahr 1995 stammten. 1995 gab es laut Schätzungen des Marktforschungsinstituts EITO 16 Millionen Internetuser weltweit (heute sind es über vier Milliarden). Selbst bei Microsoft hielt man das Ganze für einen kurzfristigen überschätzten Hype. Windows 95 wurde beispielsweise ohne jede Internetfunktion ausgeliefert. Mobile Computing, Social Media oder Big Data und KI waren zum damaligen Zeitpunkt unvorstellbar. Die Regelungen aus dem Jahr 1995 waren als Richtlinie beschlossen worden. Die Anwendung bedurfte also weiterer Gesetzesakte in den Mitgliedsstaaten, um die in der Richtlinie festgeschriebenen Ziele umsetzen zu können und zur Anwendung zu bringen. In Deutschland etwa wurde das Gesetz zur Änderung des Bundesdatenschutzgesetzes in Kraft gesetzt, in Österreich das Datenschutzgesetz von 2000.

Inhalt

Robert Korec
Chef vom Dienst, E-3 Print

Mit der DSGVO hat die Europäische Union die Bestimmungen nun vereinheitlicht. Statt der bisherigen 28 nationalen Gesetze steht nun eine Rechtsvorschrift, die in der gesamten EU anwendbar ist und die nicht durch nationale Parlamente abgeändert werden kann. Das bringt für Unternehmen, deren Geschäftsaktivitäten über die eigenen nationalen Grenzen hinausgehen, eine deutliche Erleichterung.

Insgesamt ist die DSGVO sehr konsumentenfreundlich ausgefallen. Das wurde im Zuge der Ausarbeitung der Verordnung gerade von der IT-Branche, aber auch konservativen EU-Parlamentariern zunächst kritisiert. Gründe dafür, dass eine Mehrheit im EU-Parlament dennoch zustande kam, dürften auch das zeitliche Zusammentreffen mit den Snowden-Enthüllungen und die erfolgreiche Klage des österreichischen Datenschutzaktivisten Max Schrems vor dem Europäischen Gerichtshof gewesen sein. Diese hatte das transnationale Safe-Harbor-Abkommen zwischen der EU und den USA beendet. Insgesamt beurteilen nun auch Vertreter der IT-Branche das Zustandekommen der Verordnung als wichtigen Schritt. Etwa begrüßte der Digitalverband Bitkom in einer Stellungnahme die DSGVO als eine Initiative zur Modernisierung und Harmonisierung des europäischen Datenschutzrechts. Zur Stärkung des europäischen Binnenmarktes und zur Förderung neuer digitaler Geschäftsmodelle seien EU-weit einheitliche, modernisierte Datenschutzvorgaben unerlässlich.

Datenschutzverein beruhigt

Auch der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. beruhigt kleinere Organisationen: „Die DSGVO für Vereine ist kein Hexenwerk." Der Verband unterstützt kleine Organisationen wie Vereine und Stiftungen, sich vorzubereiten. „Manche Vereine blicken mit Schrecken auf die neuen Regeln. Aber die Anforderungen für kleinere Organisationen sind meist nicht neu und mit nur wenig Aufwand schnell umzusetzen", sagte BvD-Vorstand Thomas Spaeing. Freiwillige Feuerwehren, lokale Sportvereine oder Landfrauenverbände würden in der Regel keinen Datenschutzbeauftragten benötigen. Für etwaige Datenerhebungen über eine Internetseite, bei Kommentaren oder für Newsletter, böten die meisten Dienstleister mittlerweile vorgefertigte Verträge an. Die DSGVO sei eine gute Gelegenheit, den Umgang mit Daten im Verein grundsätzlich zu hinterfragen. „Nicht jeder Übungsleiter eines Sportvereins muss auf die Zahlungsdaten der Mitglieder zugreifen", sagte Spaeing. Zudem können Dachverbände die Vereine unterstützen und einen Datenschutzbeauftragten benennen, der die Mitgliedsvereine berät.

KI: DSGVO greift zu kurz

Ein ausgeblendetes Problem könnten Algorithmen sein. Sie bewerten Menschen und entscheiden über sie. Solche automatisierte Entscheidungsfindung bleibt aber bislang fast unkontrolliert, obwohl sie sich auf das Leben der Menschen und ihre Teilhabechancen auswirkt. Doch die DSGVO wird nur für einen kleinen Teil der bereits heute eingesetzten ADM-Systeme (Algorithmic Decision Making) wirksam. Zudem lassen sich durch die individuellen Auskunftsrechte der DSGVO keine systematischen Mängel oder Diskriminierungen ganzer Personengruppen aufdecken. Das zeigt eine Analyse, die die Rechtswissenschaftler Wolfgang Schulz und Stephan Dreyer vom Hans-Bredow-Institut für Medienforschung an der Universität Hamburg im Auftrag der Bertelsmann Stiftung verfasst haben.

Problem bekannt – Umsetzung schleppend

Abseits dieser speziellen Herausforderung haben sich laut einer neuen Studie des Analystenhauses PAC nur 19 Prozent der europäischen Unternehmen und Behörden auf das Inkrafttreten des gesamten Regelwerkes der Datenschutz-Grundverordnung vorbereitet, und das, obwohl ihnen die Problemlage bewusst ist. Die Gespräche mit mehr als 200 IT-Leitern und Führungskräften mittelgroßer und großer europäischer Unternehmen fan-

ALLGEIER ES

Ihr Partner für Sicherheit und Datenschutz in SAP

Unsere Experten helfen Ihnen bei Maßnahmen und Monitoring zum Schutz von personenbezogenen Daten in SAP.

www.allgeier-es.com

den nur drei Monate vor Inkrafttreten der DSGVO statt. 57 Prozent der Organisationen möchten das Inkrafttreten der DSGVO zum Anlass nehmen, in Werkzeuge zur Datenintegration zu investieren, um Daten besser zu nutzen. Weitere 49 Prozent zielen auf bessere Datenqualität dank verbesserten Datenmanagements und Reporting Tools ab.

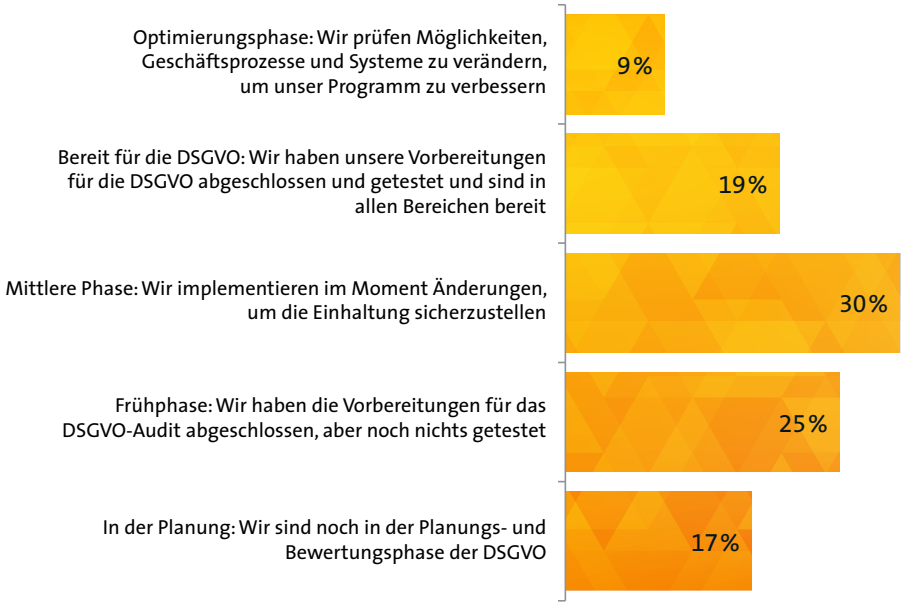
Nur fünf Prozent der europäischen Organisationen stellen laut der PAC-Studie einen neuen Datenschutzbeauftragten ein. 26 Prozent betrauen vorhandene Mitarbeiter mit dem Datenschutz nach DSGVO bzw. erweitern den Aufgabenbereich ihres Datenschutzbeauftragten um dieses Thema. Etwa 28 Prozent übertragen die Verantwortung ganz einfach dem IT-Leiter bzw. CIO. Paul Fisher, Research Director bei PAC: „Die Durchführung unserer Studie so kurz vor Einführung der DSGVO lässt die besten Rückschlüsse darauf zu, wie gut vorbereitet europäische Unternehmen sind und wie sie sich über das Auslaufen der Frist am 25. Mai hinaus anpassen werden. Trotz des Brexit stellen wir fest, dass die britischen Unternehmen das Regelwerk durchaus sehr ernst nehmen, was ein großes Engagement in puncto Datenschutz und Anpassung an ein sich veränderndes Datenumfeld belegt."

Im Januar veröffentlichte Techconsult eine Studie, wonach nur 13 Prozent der mittelständischen Unternehmen bereits konkrete Maßnahmen zur Umsetzung der DSGVO ergriffen haben. Die Studie Security Bilanz Deutschland hat im vergangenen Jahr ermittelt, dass in mehr als der Hälfte der Unternehmen noch nicht einmal definiert war, wer zu informieren sei, wenn es zu einem Datenverlust kommt.

SAP-Anwender bedingt zuversichtlich

Unzureichende Vorbereitung stellt auch ein Problem bei den SAP-Anwenderunternehmen dar. In einer Ende November von der Deutschsprachigen SAP-Anwendergruppe e. V. (DSAG) vorgestellten Umfrage gab gerade einmal etwas mehr als die Hälfte der befragten Mitgliederunternehmen an, eine Roadmap zur Umsetzung der DSGVO in ihrem Unternehmen ausgearbeitet zu haben. Dementsprechend niedrig war die Zahl derer, die wirklich zuversichtlich sind, dass ihr Unternehmen es schafft, sich fristgerecht bis zum Stichtag entsprechend den EU-Datenschutzvorgaben aufzustellen. Dass lange Zeit kein lizenzkostenfreies Angebot zur Umsetzung der neuen europäischen Datenschutzbestimmungen bestand, war für viele SAP-Bestandskunden ein unbefriedigender Zustand. Viele der DSAG-Mitgliederunternehmen sahen sich gezwungen, in zusätzliche Produkte von SAP zu investieren, um die gesetzlichen Anforderungen zu erfüllen. Insbesondere vor dem Hintergrund, dass ohne „SAP NetWeaver Information Lifecycle Management" (ILM) die Umsetzung der Vorgaben nur mit hohem Zusatzaufwand machbar ist.

Das ILM werde unter anderem zum Sperren und Löschen von personenbezogenen Daten benötigt. „Wir brauchten also dringend Klarheit, welche Möglichkeiten unsere Mitglieder haben, die gesetzlichen Anforderungen kostenfrei und effizient umzusetzen", so DSAG-Vorstand Gerhard Göttert. Dabei war für die SAP-Anwender klar, dass die Lieferung und die Verfügbarkeit einer aufwandsarmen Lösung zur Erfüllung von Anforderungen aus der DSGVO über die Wartungsgebühren abgedeckt sein müssen.



Wie würden Sie den derzeitigen Stand Ihrer DSGVO-Initiativen beschreiben? Laut einer neuen Studie von PAC (CXP Group) ist jedes sechste Unternehmen noch in der Planungsphase.

SAP reagiert, aber spät

Im Januar ist SAP der DSAG-Forderung nachgekommen. Konkret hat SAP die Lizenz für SAP NetWeaver Runtime um die Retention-Management-Funktionen von ILM erweitert. Mit dieser Lösung und weiteren Standardfunktionen der SAP-Software – wie beispielsweise dem Berechtigungsmanagement – ist es möglich, die Projekte zur Realisierung der technischen und organisatorischen Maßnahmen in den Firmen umzusetzen.

Wird mit der neuen europäischen Datenschutzverordnung das grundlegende Ziel – Schutz persönlicher Daten vor dem Missbrauch durch Organisationen – erreicht? Die in der oben erwähnten PAC-Studie befragten Experten sehen optimistisch in die Zukunft: Beachtliche 85 Prozent der Befragten glauben, dass mit dem neuen Regelwerk die Klassifizierung persönlicher Daten erleichtert und der Datenschutz verbessert wird. 63 Prozent sind der Ansicht, Verstöße ließen sich so leichter erkennen.

Nach der Verordnung ist vor der Verordnung

Während nun in drei Wochen die Übergangsfrist der DSGVO endet, hat die Europäische Kommission bereits den Entwurf einer E-Privacy-Verordnung zur Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation ausgearbeitet. Sie soll die DSGVO ergänzen. Aus Sicht des Digitalverbands Bitkom sei dies weder schlüssig noch notwendig, da diese Regelungsbereiche bereits durch die strengen Vorschriften der DSGVO abgedeckt seien und Asymmetrien schaffen, da bei vergleichbaren Datenverarbeitungen unterschiedliche Datenschutzregeln gelten.

Es bleibt abzuwarten, wie der finale Gesetzestext hierzu aussieht. Es besteht die Hoffnung, dass sowohl die E-Privacy-Verordnung als auch die DSGVO zu einer soliden Basis für den Schutz personenbezogener Daten in der EU werden und dass die neuen Regeln unternehmerisches Handeln im europäischen Binnenmarkt nicht nur ermöglichen, sondern mittel- und langfristig sogar erleichtern.

EU-DSGVO: Wissen Sie, wie Sie personenbezogene Daten in Ihrem SAP löschen und sperren?

Zuerst mal eine gute Nachricht, die Sie sicher nicht überall hören: Das Kürzel EU-DSGVO ist kein Grund dafür, dass Sie in Panik ausbrechen müssen. Zugegeben, der 25. Mai 2018 ist in direkter Sichtweite und dann müssen öffentliche Stellen und private Unternehmen in allen EU-Mitgliedsstaaten die neue Datenschutz-Grundverordnung einhalten. Dennoch ist noch Zeit, sich darauf konzentriert vorzubereiten.

Viele von Ihnen nähern sich dem Thema zunächst organisatorisch. Die technische Umsetzung bleibt vorerst auf der Strecke. Dabei ist diese häufig weitaus komplexer als erwartet. Aber wie gesagt, mit einem geplanten Projektvorgehen können Sie die Herausforderungen deutlich entspannter angehen.

Am Anfang auch hier eine ausführliche Analyse

Dazu sollten Sie folgende Fragen beantwortet haben: Was sind meine personenbezogenen Daten? In welchen Tabellen befinden sich diese in meinem SAP-System? Hier werden Sie sehen, dass die personenbezogenen Daten weit verteilt sind. Nutzen Sie gern Textfelder, Eigenentwicklungen oder „missbrauchen“ Tabellenfelder, um diese mit anderen Inhalten als vorgesehen zu befüllen? Dann wird es leider besonders kompliziert. Häufig entsteht mit den Erkenntnissen aus der Analyse dann doch ein wenig Panik, Sie fühlen sich erschlagen von der Komplexität.

Die Analyse bekommt Struktur

GISA hat ein Vorgehen entwickelt, die Analyseergebnisse zu strukturieren, die verschiedenen Anforderungen in Pakete zu bündeln und dann sukzessive abzuarbeiten. Dabei werden auch technische Vorgaben berücksichtigt. Für die Umsetzung des Sperrens und Löschens personenbezogener Daten im SAP-System nutzen wir die Funktionen des SAP ILM (Information Lifecycle Management), welches auf der klassischen Datenarchivierung basiert. Dabei sind verschiedene Vorgaben der SAP zwingend einzuhalten:

- Bewegungsdaten können nur über die klassische Datenarchivierung gesperrt werden
- Stammdaten können über SAP-ILM-Reports gesperrt werden, jedoch müssen vorher alle dazugehörigen Bewegungsdaten abgeschlossen sein
- gesperrte (archivierte) Bewegungsdaten können mittels SAP ILM aus dem Archivsystem herausgelöscht werden
- gesperrte (nicht archivierte) Stammdaten können mittels SAP ILM von der Datenbank gelöscht werden

Neben diesen Vorgaben gibt es häufig auch Abhängigkeiten unter den verschiedenen Datenobjekten, was die Erstellung eines konsistenten Ablaufplans erschwert.

Zeitgleich kümmern Sie sich schon um die technischen Voraussetzungen

Während dieser Plan erstellt wird, können Sie sich bereits um die technischen Voraussetzungen kümmern. Zunächst sollte Ihr System mindestens SAP ECC EHP7 SP05 mitbringen. Da die SAP derzeit noch stark am Produkt SAP ILM arbeitet und dadurch nahezu täglich neue OSS-Hinweise entstehen, ist es sinnvoll, ein möglichst aktuelles SP einzuspielen. Andernfalls verursacht das Einspielen zahlreicher OSS-Hinweise viele manuelle Vorarbeiten. Dann sollten Sie die notwendigen Business Functions aktivieren. Ein Teil der SAP-ILM-Transaktionen wird nicht über die SAP GUI, sondern über den Browser angezeigt. Hierfür sollten Sie prüfen, ob die notwendigen http-Services bereits eingerichtet sind. Spätestens an dieser Stelle werden Sie auf Berechtigungsprobleme stoßen. Eine Anpassung der Benutzerberechtigungen für das Ausführen der ILM-Transaktionen bleibt Ihnen da nicht erspart. Neben den Vorarbeiten im SAP-System benötigen Sie ein Archivsystem, welches das SAP-Zertifikat für die WebDAV-3.0-Schnittstelle hat. Falls Sie noch kein Archivsystem nutzen, können Sie sich bei der SAP eine Liste mit den zertifizierten Archivsystemprodukten geben lassen. Sie benutzen bereits ein Archivsystem? Dann prüfen Sie, ob Ihr Archivsystem die WebDAV-3.0-Schnittstelle bereits in sich trägt oder ob gegebenenfalls ein Upgrade oder eine Umgestaltung der Archivsystem-Infrastruktur notwendig ist.

Sie sind am Zug: Beginnen Sie!

Sie merken sicher: Schon allein die Vorarbeiten sind nicht trivial und die Zeit drängt. Es ist spät und jeder, der mit der Umsetzung des Sperrens und Löschens noch nicht begonnen hat, wird es bis zum 25. Mai 2018 kaum schaffen. Aber beginnen Sie! Mit fachkundiger Unterstützung können Sie innerhalb weniger Wochen Analyse, Ablaufplan und technische Vorbereitungen treffen. Im Falle einer Datenschutzprüfung können Sie dann vorzeigen, dass die technische Umsetzung begonnen wurde und Sie einen strukturierten Plan für die kommenden Schritte der Umsetzung bereits erstellt haben. Übrigens ergeben sich durch das Sperren und Löschen von Daten in Ihrem SAP-System Synergieeffekte für Ihren HANA-Umstieg!

GISA®
IT. Mehr als Standard.

GISA GmbH
Leipziger Chaussee 191a
06112 Halle (Saale)
Tel.: + 49 800 7000 585 (kostenfrei)
kontakt@gisa.de
www.gisa.de

EU-DSGVO-Realisierung mit SAP ILM und passgenauen Ergänzungslösungen

Smarte Umsetzung

Um den aktuellen EU-DSGVO-Anforderungen mit SAP ILM gerecht zu werden, wird ein Archivsystem mit einer WebDAV-Schnittstelle benötigt. Hier bietet sich der Einsatz einer SAP-Ergänzungslösung an.

Walter Steffen, Senior Software Architect PBS Software GmbH.

Mit dem „Recht auf Vergessenwerden“ hat die Europäische Kommission das Recht von Endverbrauchern gestärkt. Durch das Inkrafttreten der EU-Datenschutz-Grundverordnung (EU-DSGVO) wird eine dauerhafte uneingeschränkte Verarbeitung digitaler Informationen mit Personenbezug reguliert und eingeschränkt. Mit dem Inkrafttreten der EU-DSGVO zum 25. Mai dieses Jahr müssen alle IT-Systeme, die personenbezogene Daten vorhalten und verarbeiten, diese nach Beendigung des Zwecks der Erhebung löschen beziehungsweise massiven Zugriffsbeschränkungen unterwerfen.

Wer sich auf Spurensuche begibt, welche SAP-Systeme von der EU-Datenschutz-Grundverordnung betroffen sind, dem wird schnell klar, dass nicht nur HCM-Systeme (Human Capital Management)dazu zählen. Darüber hinaus tangiert die DSGVO in Unternehmen ganz konkret auch SAP ERP, SAP BW und SAP-Industrielösungen. Und zwar insbesondere solche, die B2C-Anwendungsfunktionalität (Business-to-Consumer) nutzen.

Beispielsweise Versorgungs-, Telekommunikations- und Versicherungsunternehmen haben sich dementsprechend mit der Verordnung auseinanderzusetzen. Ein Kernpunkt dabei ist, dass die technische Umsetzung der EU-DSGVO eine strikte Regulierung des Datenzugriffs auf personenbezogene Stamm- und Bewegungsdaten während und nach der Zweckbindung ihrer Erhebung erfordert. Deshalb ist eine Überprüfung der eigenen Unternehmensprozesse und Datenstrukturen grundsätzlich zu empfehlen. Ein entsprechender DSGVO-Lösungsansatz steht im Rahmen des SAP Information Lifecycle Management (SAP ILM) zur Verfügung.

DSGVO-Funktionalität in SAP ILM verfügbar

Bisher hat sich die SAP-ILM-Lösung im Wesentlichen auf die Organisation der zeitlich befristeten und unveränderbaren Aufbewahrung von Dokumenten und SAP-Datenobjekten auf einem geeigneten Ablagesystem beschränkt. Zusätzlich gibt es die Option, nach Ablauf der Aufbewahrungsfrist (sogenannte Retention) aus der SAP-Applikation das Vernichten der Anwendungsdaten aufgrund von gesetzlichen Vorgaben zu organisieren.

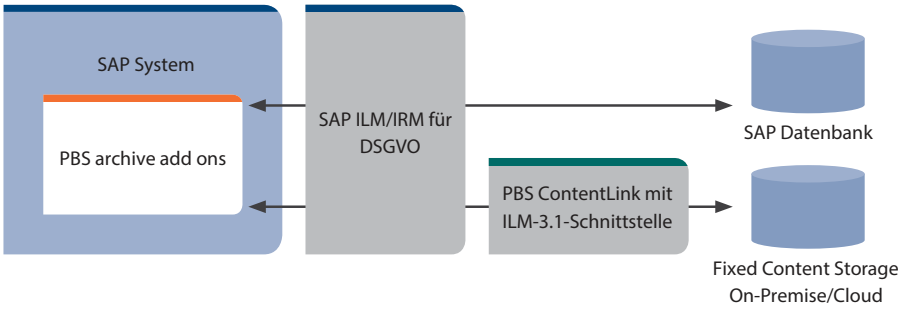
Wesentliche Elemente der Lösung sind zum einen die SAP-spezifische WebDAV-Schnittstelle zur hierarchischen Ablage von Archivdaten sowie der sogenannte Retention Manager (IRM) zur Lebenszyklusverwaltung von Datenobjekten. Durch eine Erweiterung des Regelwerks im IRM hat SAP den Anforderungen der DSGVO Rechnung getragen. Bewegungsdaten können nach Ablauf ihrer Zweckbindung durch Archivierung und Zugriffskontrolle gesperrt werden, wenn umfassendere Gesetzesvorschriften ein sofortiges Löschen nicht gestatten. So etwa die GoBD, Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen in Unterlagen in elektronischer Form und Datenzugriff. Der Lösungsansatz setzt eine Datenarchivierung für Bewegungsdaten zwingend voraus, um sowohl die Zeitspanne für den Datenzugriff als auch das Zugriffsrecht DSGVO-konform realisieren zu können.

Stammdaten wie Debitoren oder Kreditoren werden in der jeweiligen SAP-Umgebung durch ein erweitertes Berechtigungskonzept in ihrer Verarbeitung eingeschränkt und für den allgemeinen Datenzugriff gesperrt. Nach Ablauf aller Aufbewahrungsfristen kann das in der DSGVO geforderte Löschen der Anwendungsdaten nach den in SAP IRM hinterlegten Regeln erfolgen.

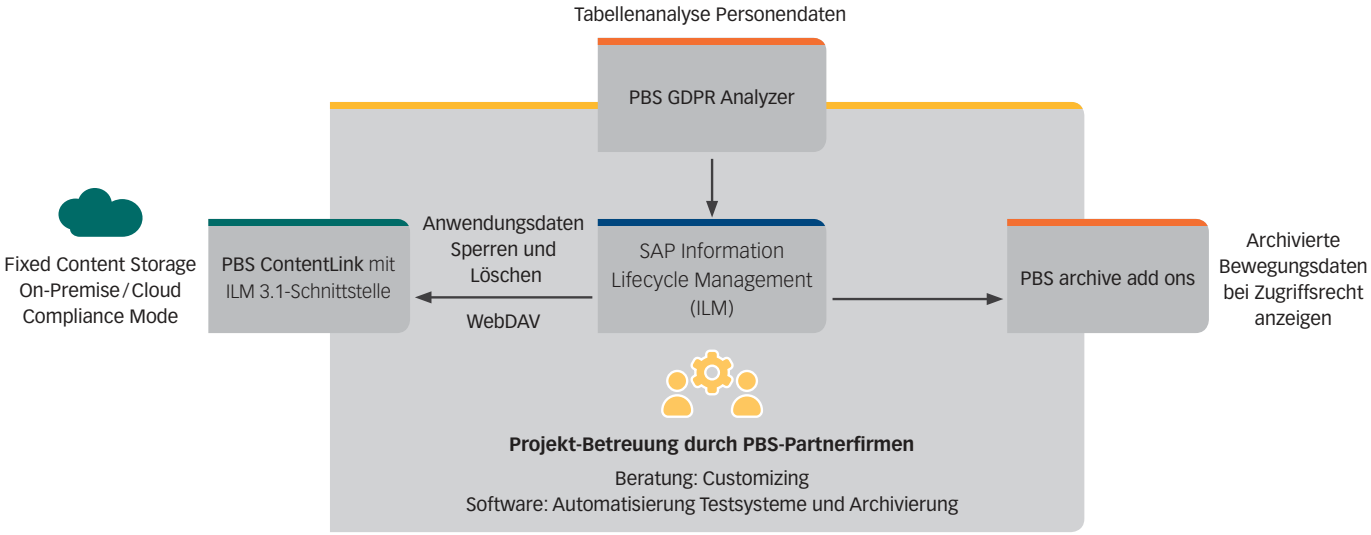
SAP ILM sinnvoll ergänzt

Um den aktuellen Anforderungen mit SAP ILM gerecht zu werden, wird ein Archivsystem mit einer WebDAV-Schnittstelle benötigt. Hier bietet sich der Einsatz einer SAP-Ergänzungslösung an, etwa ContentLink von PBS. Es fungiert als effizientes Interface zwischen SAP-Systemen und revisionssicheren Ablagesystemen, um die vorliegenden aufgabenspezifischen Anforderungen bedarfsgerecht zu unterstützen oder zu erfüllen. Hochverfügbarkeit, hohe Skalierbarkeit und geringer Administrationsaufwand zeichnen die genannte Lösung aus. PBS ContentLink ist von SAP sowohl für die aktuelle SAP ArchiveLink- als auch für die WebDAV-ILM-Schnittstelle zertifiziert.

Das Sperren von Bewegungsdaten erfolgt durch ein erweitertes Berechtigungskonzept während des Datenzugriffs auf archivierte Bewegungsdaten. Implizit ist die Durchführung der klassischen ADK-Archivierung zentrale Voraussetzung zur Anwendung des Sperrkonzeptes für Bewegungsdaten im Rahmen



Nahtlose Integration der PBS archive add ons in SAP ILM.



Verarbeitung personenbezogener Daten wirksam einschränken mit SAP-(ILM-)Ergänzungslösungen.

der DSGVO in SAP ILM. Eine Anzeige von archivierten Anwendungsdaten ist im gewohnten Umfang über das SAP-Archivinformationssystem (SAP AS) möglich, sofern die zusätzliche Berechtigung S_IRM_BLOC im Benutzerstamm definiert wurde. SAP AS ermöglicht über erweiterte SAP-Standardtransaktionen den Zugriff auf Archivdaten. Allerdings ist die Anzahl der unterstützenden Transaktionen begrenzt und nicht alle Prozesse, wie beispielsweise der SD-Belegfluss, können nach erfolgter Datenarchivierung uneingeschränkt weiterbenutzt werden.

Kompletter Datenzugriff umfänglich sichergestellt

Für den vollständigen und komfortablen Zugriff auf Daten aus Archiv und Datenbank bietet die PBS Software GmbH mit den PBS archive add ons sofort einsetzbare Ergänzungslösungen zur SAP-Datenarchivierung an. Sie korrespondieren mit den entsprechenden SAP-Modulen und erweitern SAP-Standardtransaktionen und -Reports um optimierte Archivdatenzugriffe. Anwender, die die PBS archive add ons parallel zu SAP ILM einsetzen, können von einem synchronen Verhalten der PBS-Datenzugriffe ausgehen, wenn durch den SAP Information Retention Manager (SAP IRM) eine Sperr- oder Löschaktion auf Stamm- und insbesondere auf archivierte Bewegungsdaten mittels SAP ILM erfolgt.

Synchron erfolgt seitens PBS automatisch ein Sperren aller relevanten PBS-Archivindexdaten, die den Datenzugriff steuern. Asynchron können diese dann durch einen Löschlauf aus dem PBS-Indexbestand entfernt werden. Bereits im Vorfeld der DSGVO-Umsetzung können durch den PBS GDPR Analyzer Tabellen mit personenbezogenen Daten im SAP-System ermittelt werden. Dies erleichtert erheblich den Einstieg in die Umsetzung.

Archivdaten mit System verändern

Die Verwendung der SAP-DSGVO-Funktionalität ist an Release-Voraussetzungen geknüpft, die nicht in allen betroffenen Unternehmen sofort zur Verfügung gestellt werden können. Hier bietet sich für die Übergangsphase die klassische SAP-Datenarchivierung als zentrales Instrument an, um eine gezielte Zugriffskontrolle/-beschränkung über das SAP-Berechtigungskonzept auf DSGVO-relevante Daten zu erreichen.

Letztendlich müssen sich Unternehmen flexibel neuen gesetzlichen Anforderungen anpassen, auch in Bezug auf archivierte personenbezogene SAP-Daten. Aspekte wie branchenspezifische Verhaltenskodexe oder die Datensicherheit, so beispielsweise der Schutz vor Missbrauch gespeicherter Bank- und Versicherungsinformationen, spielen ebenfalls eine Rolle. Sensible Daten müssen demnach verschlüsselt werden und dürfen nur einem berechtigten Personenkreis zugänglich sein. Aber auch organisatorische Veränderungen, wie die Verschmelzung von Business Units oder ein Carve-out, können eine Anpassung der archivierten Daten erforderlich machen.

Haftungs- und Garantieansprüche können eine wesentlich längere Aufbewahrungsdauer (nämlich bis zu 30 Jahre) notwendig machen als die gesetzlich vorgeschriebene Frist von 10 Jahren. Dies betrifft jedoch in der Regel nicht alle Daten, sondern lediglich einzelne Datenobjekte oder Datentypen.

Die Umsetzung dieser spezifischen Anforderungen kann es notwendig machen, bereits archivierte Daten zu maskieren, zu verschlüsseln oder in Einzelfällen zu löschen. Dies ist für die derzeit mehr als 600 verschiedenen SAP-Archivierungsobjekte mit SAP-Standardmitteln nicht möglich. Aus diesem Grund hat PBS für eine generische Archivdatenkonvertierung das PBS-Tool namens Archive Data Conversion (PBS ADC) entwickelt. Die unterschiedlichen Konvertierungsaufgaben können damit zentral konfiguriert und über einen Freigabeprozess von den Fachabteilungen validiert werden.

Die Dokumentation der durchgeführten Änderungen erfolgt direkt in der entsprechenden Archivdatei, sodass auch bei einer Portierung in eine andere Systemlandschaft die Anpassung der Archivdaten transparent bleibt. Ändern sich Compliance-Anforderungen für Geschäftsdaten, die mit einem Änderungsschutz versehen sind, erfolgt der Konvertierungsprozess durch Fortschreibung in eine neue Archivdatei. Nicht mehr benötigte Altarchivdatenbestände werden im SAP-Standard logisch gelöscht.

PBS Software GmbH
Schwanheimer Straße 144 A
64625 Bensheim
Telefon: +49 (0) 6251/1740
info@pbs-software.com
www.pbs-software.com

Anwender werden bei der DSGVO in die Pflicht genommen

Paradigmenwechsel

Bei der technischen Umsetzung der EU-Datenschutz-Grundverordnung in einer SAP-Landschaft sind mehrere Aspekte zu berücksichtigen. Ein E3-Interview dazu mit Gernot Reichling, Geschäftsführer PBS Software GmbH.

Gernot Reichling, Geschäftsführer PBS Software GmbH.

Welche Kernaspekte haben SAP-Anwender im Zusammenhang mit der DSGVO zu beachten?

Reichling: Zum einen sind SAP-Bestandskunden in organisatorischer Hinsicht gefordert, ihre IT-Infrastruktur DSGVO-konform zu konzipieren und aufzustellen. Hierbei bieten entsprechende Berater oder Consulting-Unternehmen Unterstützung. Die andere Seite der DSGVO-Medaille ist, dass die technische Umsetzung der EU-Datenschutz-Grundverordnung in einer SAP-Landschaft realisiert werden muss. Und dies insbesondere vor dem Hintergrund, dass man es beim Technikthema mit einem Paradigmenwechsel hinsichtlich der Ablage von Daten und Dokumenten zu tun hat. Die Mehrzahl der SAP-Bestandskunden nutzt bisher lediglich das Transferprotokoll ArchivLink, um Anwendungsdaten auf ein geeignetes Ablagesystem auszulagern. Die Anforderungen der DSGVO setzen aber für das Datenmanagement neue Maßstäbe und machen hier eine Neuausrichtung der Datenablage unerlässlich. Konkret steht mit WebDAV ein neues Ablagedatenprotokoll auf dem Plan.

Warum ist dieses neue Protokoll in Verbindung mit der EU-Datenschutz-Grundverordnung so bedeutsam?

Reichling: Im Blick stehen Objektverwaltung und Objektmanagement; verbunden mit der Frage, wie Objekte, die dem Storage übergeben wurden, zu handhaben sind. Schließlich werden Anwender durch die DSGVO in die Pflicht genommen, einen Prozess zu installieren, der das Löschen aus einer Applikation zulässt. Mehr noch: Es ist das Aufbewahren, das Verwalten und das Löschen von Anwendungsdaten aus der Applikation heraus zu bewerkstelligen. Das bedeutet, dass die Applikation für das Datenmanagement verantwortlich ist. Dies ist nur über das WebDAV-Protokoll realisierbar.

Es sind Objekte anzureichern, und zwar um erweiterte Verwaltungsfunktionalität oder -informationen. Etwa um Informationen, wie lange ein Objekt einen Schutz aufweisen muss. Oder eben im Nachgang, dass nun das Objekt gelöscht werden muss. Dabei verwendet die Anwendung SAP ILM als Steuerungsinstrument, um Anwendungsdaten kontrolliert zu sperren oder final zu löschen.

WebDAV gibt es aber schon eine gewisse Zeit, oder?

Reichling: Das ist richtig. Bisher übernahm das WebDAV-Protokoll im Rahmen von SAP ILM die zeitlich befristete und unveränderbare Aufbewahrung von Dokumenten und SAP-Datenobjekten auf einem revisionssicheren Speichersystem und nach Ablauf der Verweildauer die Datenvernichtung. Im Rahmen der DSGVO wurde der SAP-ILM-Ansatz noch einmal verfeinert. Wenn man so will, löst WebDAV ArchiveLink durch die Anforderungen der DSGVO als führendes Transferprotokoll ab. Es besteht also Handlungsbedarf!

Unsere Empfehlung ist, zunächst einmal eine sichere DSGVO-Infrastruktur zu implementieren. Man sollte bei verwendeten Storage-Systemen quasi hinter die Fassade schauen. Wo liegen beispielsweise Schutz oder Nutzungsmechanismen auf ein Objekt, das abgelegt wurde? Die Umsetzung der Notwendigkeiten im Sinne der DSGVO lässt sich zwar mit einer zusätzlichen Softwareschicht lösen, die mit dem Storage verbunden ist. In diesem Fall ist aber eigentlich der Speicher nicht immer ausreichend geschützt.

Was heißt das?

Reichling: Ein Administrator beispielsweise kann Storage-Objekte relativ leicht löschen. Was zur Folge hat, dass Objekte schlicht weg sind – und zwar ohne Anwendungsbezug. Von Relevanz für Unternehmen ist, dass ein Storage im Sinne einer Art Compliance-Storage verwendet wird. Hierbei bilden Hardware und Software in einer Landschaft eine Art Appliance und realisieren einen notwendigen Schutz gemeinsam. Wichtig ist insbesondere, dass sich von außen ein notwendiger Schutz nicht aushebeln lässt. Nicht alle Speichersysteme erfüllen diese Anforderungen.

Für welche Lösung plädiert PBS?

Reichling: Wir empfehlen die Nutzung eines Storage-Systems mit Softwareschutz – eine Art Compliance-Storage – und einer Direktkoppelung mit der PBS-Lösung ContentLink, die wiederum mit einem SAP-System verbunden ist. Das bedeutet für einen SAP-Bestandskunden den Einsatz einer schlanken Umgebung, die vom Wartungsaufwand, vom Upgrade und vom Betrieb her kostengünstig ist.

Und was können dabei die PBS-Lösungen leisten?

Reichling: Zum einen den reibungslosen und schnellen Betrieb respektive die Verbindung zu einem Compliance-Storage und dem SAP-System – mit der Verknüpfung von PBS ContentLink und SAP sowie dem Storage-System. Mit dem SAP-ILM-3.1-zertifizierten PBS ContentLink werden die beiden relevanten Protokolle, die SAP anbietet für die Ablage von Daten, nämlich ArchiveLink und WebDAV, unterstützt. ContentLink kann sperren, löschen und führt dies dann auch auf dem Storage aus. Mit anderen Worten: Die Lösung setzt die entsprechenden Anweisungen über ein API in dem Storage-System um, damit das Storage-System weiß, was die SAP-ILM-Anwendung will.

PBS bietet mit seinen archive add ons einen vollständig integrierten Archivdatenzugriff über nahezu alle Transaktionen einer SAP-Applikation an. Damit wird die Akzeptanz der Datenarchivierung in den Fachabteilungen erhöht und eine gleichzeitige DSGVO-konforme Zugriffskontrolle ist garantiert. Dabei entsteht kein zusätzlicher Customizing-Aufwand, um der DSGVO gerecht zu werden. Obendrein arbeiten die PBS archive add ons und ContentLink nahtlos zusammen.

PBS-Ergänzungslösungen

Datenarchivierung · Datenmanagement · Datenanalyse

DSGVO-Paket Migration S/4HANA

EU-DSGVO meistern

Die Erfüllung der neuen EU-Datenschutzrichtlinien stellt Unternehmen vor große Herausforderungen im Betrieb ihrer SAP-Landschaft. Mit dem PBS-DSGVO-Paket ergänzen wir die SAP ILM-Lösung und optimieren die Zugriffskontrolle auf sensible Daten, unterstützen die revisionssichere Ablage Ihrer Archivdaten und erreichen ein bedarfsgerechtes Maskieren und Löschen von nicht mehr erforderlichen personenbezogenen Informationen bei Bedarf.

Komfortabler Archivdatenzugriff unter SAP S/4HANA

Zur Optimierung des S/4HANA-Systembetriebs ist ein durchdachtes ILM-Konzept unerlässlich. Um komplett und bedarfsgerecht auf die Archivdaten zugreifen zu können, wurden die PBS archive add ons an S/4HANA angepasst und sind bereits von SAP zertifiziert.

Archivdaten, die in älteren ERP-Release-Ständen erzeugt wurden, lassen sich nahtlos in S/4HANA anzeigen und analysieren. Hierdurch wird der Migrationsprozess entscheidend vereinfacht und kann somit kostengünstiger durchgeführt werden.

Neugierig geworden?
Dann senden Sie uns einfach eine kurze E-Mail an vertrieb@pbs-software.com oder treffen Sie unsere Experten bei dem PBS-Informationstag am 22.06.2018 (Bensheim).
Jetzt kostenlos anmelden unter: pbs-software.com/Anmeldung

www.pbs-software.com
PBS Software GmbH · Schwanheimer Straße 144 a · 64625 Bensheim · Telefon: 06251 1740

KOMMENTAR

Von **Gabriele Ernst,** Allgeier ES

Lässt sich die Verantwortung für den Datenschutz auslagern?

Gabriele Ernst ist Senior Consultant für SAP Compliance Services mit dem Schwerpunkt „Datenschutz in SAP“ bei Allgeier ES.

Am Freitag, dem 25. Mai 2018, ist es so weit. Die EU-Datenschutz-Grundverordnung (EU-DSGVO) gilt. Artikel 24 regelt die „Verantwortung des für die Verarbeitung Verantwortlichen“.

Liegen personenbezogene Daten im eigenen Haus auf eigenen Servern, ist die Verantwortung klar. Der Verantwortliche, also die Organisation, die für ihre Unternehmenstätigkeit Daten von natürlichen Personen sammelt, speichert und verarbeitet, trägt die Verantwortung dafür, dass die Vorgaben der EU-DSGVO eingehalten werden. Sammelt eine Organisation Daten von natürlichen Personen, speichert und verarbeitet diese aber nicht selbst, konkretisiert der sogenannte Erwägungsgrund 074 den Artikel 24 wie folgt: „Die Verantwortung und Haftung des Verantwortlichen für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte geregelt werden. Insbesondere sollte der Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Verordnung stehen und die Maßnahmen auch wirksam sind.“ Gemäß EU-DSGVO ist „Software as a Service“ möglich, „Verantwortung as a Service“ hingegen nicht. Der Verantwortliche kann einen Teil seiner Verantwortung an seinen Auftragsverarbeiter abgeben. In diesem Fall sollten Verantwortungsübergänge klar geregelt sein. Angesichts der empfindlich hohen Strafen, die ab 25.5.2018 auf Verantwortliche zukommen können, ist eine Überprüfung bestehender Verträge ratsam. Das betrifft neben Verträgen mit Auftragsverarbeitern auch jene mit Mitarbeitern, Banken, Kunden, Lieferanten etc. Liegt kein Rechtsgrund zur Verarbeitung personenbezogener Daten vor, ist diese verboten. Daten dürfen nur so lange im System verbleiben, wie es zur Erfüllung des Zwecks erforderlich ist. Der Verantwortliche muss die Zweckgebundenheit gegenüber der Aufsichtsbehörde belegen können.

Sind meine Daten in SAP sicher?

Angesichts des jüngsten Facebook-Datenskandals ist das Interesse der Nutzer groß, ob und bei wem ihre Daten sicher sind. Auf entsprechende Nachfragen sollten SAP-Kunden vorbereitet sein. Artikel 5 der EU-DSGVO fordert: „Personenbezogene Daten müssen [...] in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (‚Integrität und Vertraulichkeit‘)“. Wichtige Bausteine dafür sind die Netzwerksicherheit, durchdachte Zugangskontrollen, eine hohe Systemzuverlässigkeit, die Absicherung von Schnittstellen und eine fundierte Verschlüsselung bei Datenübertragungen. Im Rahmen des Lizenz- und Wartungsvertrages stehen SAP-Kunden Bordmittel und regelmäßige Services zur Verfügung. Sie helfen, den Ist-Stand zu überwachen und die Qualität dauerhaft auf einem hohen Niveau zu halten. Dazu gehören zahlreiche Protokollmöglichkeiten, die Feinjustierung von Rollen und Berechtigungen, regelmäßige Security-Hinweise, der SAP Early Watch Report und der SAP Security Optimization Service. Auch SAP Read Access Logging kann ohne zusätzliche Lizenzkosten genutzt werden. Wichtig ist, sämtliche Maßnahmen zu dokumentieren und so nach und nach ein Datenschutz-Management-System aufzubauen. Darin werden alle Dokumente, Nachweise, Übersichten und Prozessbeschreibungen gesammelt und aktualisiert, die bei einer Überprüfung vorhanden sein müssen. Was das Datenschutz-Management-System beinhaltet, welches Budget und welche Ressourcen dafür bereitgestellt werden, entscheidet der Verantwortliche auf Basis seiner unternehmensinternen Risikoeinschätzung.

Werden meine Daten aus SAP gelöscht?

Artikel 17 regelt das „Recht auf Vergessenwerden“: „Eine betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden“, wenn z. B. die betroffene Person die Einwilligung zurückgezogen hat oder der Zweck, für den die Daten erhoben wurden, entfallen ist. Daten müssen nicht unverzüglich gelöscht werden, wenn gesetzliche oder sonstige glaubhaft nachvollziehbare Aufbewahrungsfristen gelten. Die Umsetzung kann toolunterstützt durchgeführt werden. So bildet etwa das SAP Information Lifecycle Management den Lebenszyklus von Daten ab. Es hilft Sperr- und Löschfristen mittels eines Regelkataloges einzuhalten und Daten automatisiert zu archivieren und zu löschen. In der Vergangenheit haben sich viele Unternehmen vor der Sperrung und Löschung gedrückt. Ab dem 25.5.2018 gilt: Der Verantwortliche kann Maßnahmen und die Überwachung zum Schutz von personenbezogenen Daten an einen IT-Partner auslagern, die Verantwortung dafür leider nicht.

www.allgeier-es.com

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.

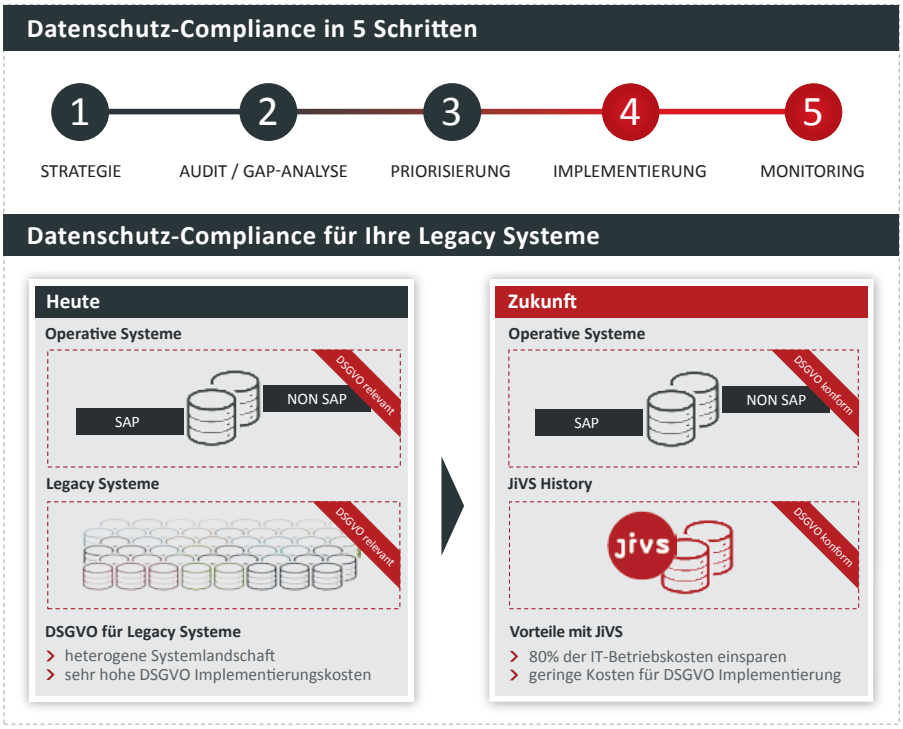
Im Grunde ist dieser Befund erstaunlich. Denn die meisten Grundsätze der neuen Verordnung sind seit Jahren Bestandteil früherer Gesetzgebungen, insbesondere des deutschen Bundesdatenschutzgesetzes. Dazu zählen etwa die Prinzipien der Datensparsamkeit, der Verhältnismäßigkeit, der Zweckbindung oder der 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

Information und Bildungsarbeit von und für die SAP® Community

Das E-3 Magazin

LICENSE TO ILL

Kopfschmerzen vor dem Lizenzaudit? Dagegen hilft die doppelte E-3 Wissensprophylaxe: mit den Wirkstoffen der Kolumnen „Lizenzen“ und „Lizenztransformation“.

SAP® ist eine eingetragene Marke der SAP AG in Deutschland und in den anderen Ländern weltweit.

www.e-3.de

© Yupa Watchanakit, Shutterstock.com

Mit parsionate wird die DSGVO zur Chance für Ihr Unternehmen

Es ist fünf Minuten vor zwölf!

Am 25. Mai 2018 ist es also soweit: Die neue Datenschutz Grundverordnung (DSGVO) ersetzt die bislang geltende Datenschutzrichtlinie 95/46/EC sowie das Bundesdatenschutzgesetz und regelt zukünftig den Umgang von Organisationen mit Daten europäischer Bürger.

Dadurch sehen sich Unternehmen oft ratlos vor einem Berg signifikanter Änderungen und Verschärfungen stehen. Oliver Hach ist MDM-Experte bei parsionate, einem der führenden europäischen Beratungsunternehmen für Stammdatenmanagement, und weiß, wie Unternehmer die DSGVO-Regularien erfolgreich umsetzen und gleichzeitig Nutzen für ihr Business daraus ziehen können.

Herr Hach, die DSGVO steht direkt vor der Tür aber noch zögern einige Unternehmen sich wirklich damit zu beschäftigen. Woran liegt das?
Oliver Hach: Die DSGVO (im Englischen GDPR) beinhaltet umfassende Änderungen was den Umgang mit personenbezogenen Daten angeht. Um diese erfüllen zu können, müssen viele Unternehmen neue grundlegende Maßnahmen in den Unternehmensstrukturen und -prozessen implementieren. Das ist kein Kinderspiel, sondern mit großem Aufwand verbunden. Kein Wunder also, dass man in vielen Unternehmen nicht recht weiß, wie und wo man anfangen soll.

Womit sollte ein Unternehmen starten für eine erfolgreiche Umsetzung?
Hach: Wichtig ist, dass es sich mit den gesetzlichen Rahmenbedingungen auseinandersetzt und mit den Grundlagen der DSGVO vertraut macht. Daten spielen eine zentrale Rolle, um als Unternehmen im Markt zukünftig erfolgreich und wettbewerbsfähig zu sein. Wir bei parsionate unterstützen Unternehmen dabei, eine für sie passende und zukunftsorientierte Datenstrategie zu entwickeln, die jetzt im Unternehmen verankert werden muss. Ein Ergebnis dieser Strategie ist die große Chance einen umfassenden Blick auf die Kundeninformationen zu erhalten – dabei helfen wir mit unserer Beratungsmethodik.

Wieso ist der 360 Grad Blick auf den Kunden wichtig für die DSGVO?
Hach: In nahezu allen Unternehmen befinden sich personenbezogene Daten – z. B. über Kunden, Lieferanten oder auch eigenes Personal – in diversen Systemen, Applikationen und Datenbanken. Oft auch dort, wo man sie überhaupt nicht vermutet. Die DSGVO-Regularien erfordern eine lückenlose Dokumentation der genutzten Systeme und Prozesse – das Unternehmen muss alle Daten und Informationen über seine Kunden identifizieren, bewerten und sicher ablegen können. Es muss wissen, wo sie im Unternehmen gespeichert und wie verwendet werden – und wo es Lücken geben könnte. Um genau das zu analysieren, bietet parsionate dezidierte Healthchecks an, die dafür die notwendige Transparenz liefern. Damit kann das Unternehmen seinen Status der DSGVO-Compliance erheben, identifiziert offene Punkte und kann notwendige Schritte für Lösungen entwickeln.

Erklären Sie uns bitte den parsionate Healthcheck genauer
Hach: Der GDPR Healthcheck ist ein Workshop-Programm, das ein Unternehmen hinsichtlich der strengen DSGVO-Vorgaben über Abteilungen hinweg analysiert und den Compliance-Status erhebt und dokumentiert. Auf Basis einer strukturierten Methodik werden Unterneh-

mensprozesse analysiert und die jeweilige System-, Datenbank- und Applikationslandschaft dokumentiert. Darüber hinaus erfährt das Unternehmen, ob diese genutzten Systeme und Stellen, die personenbezogene Daten beinhalten, den Anforderungen der DSGVO genügen. So identifizieren wir die relevanten Daten und Systeme, visualisieren sie in einem Compliance Report und interpretieren die Ergebnisse. Natürlich bieten wir auch Unterstützung zur Umsetzung der notwendigen Maßnahmen an.

Ein wichtiger Teil der DSGVO ist – wie der Name schon sagt – der Datenschutz. Welche Sicherheitskontrollen braucht ein Unternehmen jetzt für seine Daten?
Hach: Personenbezogene Daten verlangen besonderen Schutz. Das Einwilligungs- (oder auch Consent-) Management ist ein zentraler Punkt der DSGVO-Verordnung, denn Daten dürfen nur noch mit ausdrücklicher Einwilligung der betroffenen Person gesammelt werden. Viele Unternehmen denken, dass dies mit einem Häkchen-Feld im CRM-System getan ist. Das reicht aber nicht aus, denn auf Anfrage müssen Unternehmen in der Lage sein, Auskunft über die Verwendung der personenbezogenen Daten zu geben. Zudem müssen Sie jederzeit nachweisen können, dass ihre Schutzmechanismen greifen, der Ablauf sowie Änderungen der Einwilligung auch wirklich umgesetzt werden und, dass bei weiteren Verwendungen oder Archivierung der Daten entsprechend anonymisiert wird.

Wer ist im Unternehmen verantwortlich für die Datenschutzrichtlinien und ihre Einhaltung?
Hach: Die Benennung von Verantwortung tragenden Personen ist eine der ersten und zentralen Punkte der DSGVO. Wir bei parsionate empfehlen einen dedizierten, möglicherweise externen Datenschutzbeauftragten (DPO) zu engagieren, der mit einem explizit benannten Chief Data Officer zusammenarbeitet. Der Datenschutzbeauftragte ist für die korrekte Umsetzung der DSGVO verantwortlich und ist Ansprechpartner bei Verstößen. Gibt es im Unternehmen keinen DPO, dann ist der Geschäftsführer persönlich verantwortlich und auch haftbar. Bei unserem GDPR Healthcheck wird geklärt, wer verantwortlich ist für bestimmte Daten, Prozesse und Applikationen mit personenbezogenen Daten. Dies wird im parsionate Compliance Report dokumentiert und damit kommt das Unternehmen auch seiner vorgeschriebenen Dokumentationspflicht nach.

Oliver Hach, MDM-Experte bei parsionate:
Seit Anfang 2018 verstärkt Oliver Hach das Vertriebs- und Marketingteam bei parsionate. Sein Fokus liegt dabei auf Kunden in den Bereichen Master Data Management (MDM), Data Quality Management und Business Process Management. Dazu gehört die aktuell für viele Unternehmen relevante Verordnung DSGVO.

Wie schnell muss ein Unternehmen auf Daten-Änderungen oder Auskunftswünsche reagieren können?
Hach: Die DSGVO-Regularien verordnen eine zeitnahe Antwort an Personen die Auskunft verlangen. Als Unternehmen müssen Sie zudem nachweisen, dass Sie innerhalb von 72 Stunden reagieren können, beispielsweise im Falle eines Datendiebstahls. Ist unsere Methodik umgesetzt, können Fragen zur Verwendung, Speicherung und Änderung der Kundendaten mit wenig Aufwand beantwortet werden.

Welche Chancen kann ein Unternehmen aus solch einem analytischen Blick wie dem parsionate Healthcheck auf seine Strukturen und Systeme ziehen?
Hach: Die DSGVO bietet die Chance, ineffiziente Prozesse im Datenmanagement zu beheben. Der Aufwand für die Pflege und Verwaltung doppelter, falscher und redundanter Datensätze beispielsweise kann eingespart werden, genauso wie Marketingmaßnahmen, die auf unzuverlässigen Kundendaten basieren. Wir bei parsionate sehen die DSGVO als echte Chance für Unternehmen einen zuverlässigen und korrekten Gesamtüberblick nicht nur über jeden Kunden, sondern auch über weitere betroffene Personengruppen und die dazugehörenden Daten zu bekommen und so ein effizientes Stammdatenmanagement aufbauen zu können. Konzentrieren wir uns auf die Kundenseite: Eine Vereinheitlichung des Datenmanagements mit zentralen Kundendaten bedeutet eine Reduzierung der Kosten und mehr Transparenz. Die integrierten Datensilos können mit Social-media-Daten kombiniert werden und bieten so einen viel umfangreicheren Überblick über die Kunden und ihr Verhalten im digitalen Umfeld. Daraus resultieren signifikant bessere Optionen im 1:1 Marketing und der individuellen Kundenansprache. Das gesamte Unternehmen erfährt ein neues und tieferes Verständnis über den Umgang mit Daten. „Daten sind das neue Gold“ – und diesen Schatz können Unternehmen mit solch einem neuen Bewusstsein heben und nutzbringend einsetzen. Ein großer Schritt in der Digitalisierung!

parsionate.
omnichannel excellence

parsionate GmbH
Motorstraße 25
70499 Stuttgart
Telefon: 49 711 75886 600
kontakt@parsionate.com
parsionate.com

EU-DSGVO ist mehr als Double-Opt-In Lösungsansätze für weitere kritische Handlungsfelder

Die EU-DSGVO greift in wenigen Wochen, wirklich vorbereitet ist laut einer aktuellen DSAG-Studie allerdings nur ein einstelliger Prozentsatz der befragten Unternehmen*.

Viele offensichtliche Themen wie Double-Opt-In oder das Recht auf Auskunft sind x-fach in unterschiedlichsten Veröffentlichungen thematisiert, mit unterschiedlichsten Ansätzen, wie darauf reagiert werden sollte oder könnte.

Doch es gibt weitere – jedoch weniger beachtete – kritische Handlungsfelder. Zu diesen zählen unter anderem das **Recht auf Vergessenwerden (Art. 17)** und die **Sicherheit der Verarbeitung (Art. 32),** die sich wiederum auf die **Sicherstellung der Schutzziele** wie etwa Vertraulichkeit, Integrität und Verfügbarkeit auffächert.

Jede Person hat also das Recht, in einem angemessenen zeitlichen Rahmen zu erfahren, welche Daten zu welchem Zweck in Unternehmensdatenbanken gespeichert sind. Mit einem ordentlichen Datenmodell und geeigneten Abfragen oder Tools lässt sich dies auch wunderbar beantworten. So weit, so gut.

Jederzeit auskunftsbereit – Verfügbarkeit personenbezogener Daten

Doch wie kommen Sie an die Daten, wenn das System zu einem denkbar ungünstigen Zeitpunkt nicht verfügbar ist? Was, wenn aufgrund eines erzwungenen Restore eines Einzelsystems Daten plötzlich inkonsistent zu anderen Systemen sind?

Im Falle eines Falles greift Libelle **Business***Shadow,* eine Lösung, die Verfügbarkeits- und Disaster-Szenarien auf logischer Ebene abbildet. Der Vorteil: Nicht nur RPO und RTO, sondern speziell auch die RCO (Recovery Consistency Objective) sorgen dafür, dass Unternehmen sehr schnell mit konsistenten Datenbeständen wieder umfassend aussagefähig sind.

Löschen/Sperren personenbezogener Daten – Recht auf Vergessenwerden

Was, wenn Personen darüber hinaus von ihrem Recht auf Vergessenwerden Gebrauch machen möchten?

Besteht keine laufende Geschäftsbeziehung mehr, dürfen personenbezogene Daten auch nicht mehr im System gespeichert sein. Dem gegenüber stehen die gesetzlichen Aufbewahrungspflichten, für die auch abgeschlossene Geschäftsbeziehungen nachverfolgbar vorgehalten werden müssen. Ein Dilemma.

Abhilfe kann ein spezieller **Datentresor** schaffen, der im Libelle Toolset **Master Data Services Suite (MDSS)** enthalten ist. In diesem werden solche Stammdaten gelagert, deren Lebenszyklus aus DSGVO-Sicht beendet ist, sowohl regelmäßig automatisch ermittelt als auch explizit getriggert. In den Produktivdaten wird lediglich ein Lösch-/Sperrhinweis zu sehen sein, während die Echtdaten im Datentresor nur noch für Personen mit darüber hinausgehendem berechtigten Interesse verfügbar sind.

Testdaten anonymisieren – Vertraulichkeit personenbezogener Daten

Neben dem Recht auf Vergessenwerden ist auch das Thema Zweckgebundenheit personenbezogener Daten im Fokus. Es dürfen nur solche Daten verarbeitet werden, die für den konkreten geschäftlichen Zweck benötigt werden, und auch nur von einem berechtigten Personenkreis. Für Produktivumgebungen ist dies eine prozessuale/organisatorische Frage und Thema des Berechtigungswesens. Doch wie sieht es mit nicht-produktiven Umgebungen aus?

In der Praxis werden Q-/Projekt-/Schulungssysteme oft mit Systemkopien aktualisiert. Ergo: Echtdaten landen in nicht-produktiven Umgebungen. Somit hat eine Vielzahl nicht-berechtigter Personen (Entwickler, Berater, Admins) Zugriff auf diese. Vielleicht nicht tagesaktuell, aber doch ganz klar personenbezogen. Möglichkeiten, den unberechtigten Zugriff einzuschränken: entweder ein umfassendes Berechtigungskonzept analog der Produktivumgebungen, das häufig dem Einsatzzweck nicht-produktiver Umgebungen widerspricht. Oder dafür sorgen, dass personenbezogene Echtdaten zu dem werden, was diese Systeme tatsächlich brauchen: Testdaten.

Das Mittel der Wahl ist hierfür die **Anonymisierung der Echtdaten,** so dass diese keinen konkreten Personenbezug mehr besitzen, trotzdem realistisch und vor allem nicht mehr rückführbar sind.

Ein pragmatisch und schnell umsetzbarer Ansatz im Sinne der EU-DSGVO gelingt mit Libelle **Data***Masking* (LDM), einem Tool, das Daten auf nicht-produktiven Systemen und Systemlandschaften logisch konsistent anonymisiert. Somit können Geschäftsprozesse mit sinnvollen Testdaten nach Herzenslust Ende-zu-Ende durchgetestet werden.

www.libelle.com/dsgvo

Libelle AG
Gewerbestraße 42
70565 Stuttgart
Telefon: +49 711 78335-0
sales@libelle.com
www.libelle.com

* DSAG (2018, 7. Februar): Artikel „Die Zeit drängt". URL: https://www.dsag.de/dossier-datenschutz [17. April 2018].

Das Heft des Handelns in die Hand nehmen – DSGVO & Datensicherheit im SAP-Umfeld

Es hat sich mittlerweile herumgesprochen, die Datenschutz-Grundverordnung wird am 25. Mai 2018 „scharf geschaltet“ und Verfehlung oder Missachtung mit drakonischen Strafzahlungen geahndet. Kernpunkt der EU-weiten DSGVO bildet der Schutz personenbezogener wie auch personenbeziehbarer Daten, die im geschäftlichen Kontext verarbeitet werden.

„Es gibt also einige Herausforderungen zu meistern, um DSGVO-Konformität zu erreichen. Dabei sind Datenschutz und IT-Sicherheit im Zeitalter der Digitalisierung untrennbar miteinander verbunden. Auch wenn die Erfüllung der Datenschutzanforderungen einen durchaus nicht unerheblichen zeitlichen wie auch finanziellen Aufwand für die Unternehmen bedeutet, so könnte die DSGVO möglicherweise das Beste sein, was uns im Bereich der elektronischen Datenverarbeitung in den letzten Jahren passiert ist.

„Die DSGVO ist die große Chance, Datenschutz und IT-Sicherheit endlich ernst zu nehmen!“

Die DSGVO betrifft alle Unternehmen & Gewerbetreibenden, vom Multi-Konzern bis zum Ein-Mann-Betrieb, ja sogar Vereine. Insofern müssen sich natürlich auch sämtliche SAP-Anwenderunternehmen mit dem Thema Datenschutz tiefgehend auseinandersetzen, um die Gesetzesvorgaben erfüllen zu können. Im Kontext der SAP-Systeme wird täglich und selbstverständlich eine Vielzahl von Daten in den Geschäftsprozessabläufen verarbeitet, die mittelbaren und unmittelbaren Personenbezug haben. Diese sind im Sinne der DSGVO besonders zu schützen. Darüber hinaus ist für SAP-Anwender eine Vielzahl weiterer Daten schützenswert, sogar unternehmenskritisch, wie beispielsweise geheimes Unternehmens-Know-how, Innovationen, Finanz- oder Kundendaten. Auch diese Daten müssen im Interesse des Unternehmens vor Missbrauch, Manipulation oder digitalem Diebstahl geschützt werden.

Um dies zu erreichen, muss ein kontinuierliches Management der Sicherheitsrisiken etabliert werden. Im Zeitalter der Digitalisierung braucht effektiver Datenschutz eine ebenso wirksame wie umfassende IT-Sicherheit.

„Im Zeitalter der Digitalisierung sind Datenschutz und IT-Sicherheit untrennbar verbunden!“

Wirksamer Datenschutz im SAP-Kontext erfordert die Betrachtung aller Sicherheitsaspekte. So gehören zu den Eckpfeilern der SAP-Systemsicherheit neben wirksamen Berechtigungsstrukturen auch die Schnittstellen-, Betriebssystem- und Netzwerksicherheit, effektive Patchmanagement- und Logging-Mechanismen sowie sicherheitskonformer ABAP-Custom Code.

Neben der Etablierung eines offiziellen Datenschutzbeauftragten ist eine Reihe weiterer organisatorischer und vor allem auch technische Maßnahmen zu implementieren, um den Anforderungen der DSGVO zu entsprechen.

Nachfolgend auszugsweise eine beispielhafte, aber konkrete Anforderung der DSGVO und ihre Konsequenz für SAP-Anwenderunternehmen:

Art. 32 – Sicherheit der Verarbeitung, darin heißt es:

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

Konsequenz: Die Robustheit (Härte) der SAP-Systeme gegen Cyber-Attacken und damit auch Datenschutzverletzungen zu gewährleisten.

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Konsequenz: Das benötigte Datenschutzniveau fortwährend zu prüfen und dauerhaft sicherzustellen.

„Datenschutz und Datensicherheit sind äußerst lohnenswerte Ziele!“

Zusammenfassend kann man also feststellen, dass diese Anforderungen dauerhaft nur zu erfüllen sind, wenn die Unternehmen regelmäßig ihren SAP-Sicherheitsstatus ermitteln (SAP Security Audits) und ebenso Maßnahmen treffen, um Sicherheitsrisiken sehr zeitnah (SAP Security Monitoring) zu entdecken.

DSGVO-Konformität und umfassende IT-Sicherheit zu erlangen und natürlich auch beizubehalten sind zudem äußerst lohnenswerte, ja sogar notwendige Compliance-Ziele, denn sie helfen:

- Strafzahlungen bei DSGVO-Verfehlungen zu vermeiden
- Datenverluste und Betriebsausfälle zu minimieren
- wirtschaftliche Schäden und Imageschäden abzuwenden
- Vertrauensverluste wichtiger Stakeholder zu verhindern

Lassen Sie es nicht so weit kommen, nehmen Sie das Heft des Handelns aktiv in die Hand und senken Sie Ihre Unternehmensrisiken.

Werner Stangner, GF, exagon GmbH

exagon consulting & solutions GmbH
Reutherstrasse 3
53773 Hennef
Telefon: +49 2242 9202–0
info@exagon.de
exagon.de | sap-security.de

Datenschutz & Sicherheit nicht dem Zufall überlassen!
Systematische Analyse und Reduzierung Ihrer SAP-Sicherheitsrisiken.

- SAP Berechtigungen
- SAP Schnittstellen
- Patch-Level
- Plattform-Sicherheit (OS / DB)
- Quellcodeanalyse
- Log-Analyse

Software-gestützte Ermittlung Ihres SAP-Sicherheitsstatus.
Schnell, günstig und umfassend.
exagon

Datenschutz 2018 (DSGVO & BDSG-neu) – fachbereichsübergreifend interpretiert und umgesetzt mit SAP ILM oder anderen Tools

Oliver Greiner, Geschäftsführer entplexit GmbH, Eschborn
Prof. Dr. Daniel F. Abawi, entplexit GmbH, Eschborn
www.entplexit.com

Die Datenschutz-Grundverordnung (DSGVO) und das neue Bundesdatenschutzgesetz (BDSG-neu) treten bekanntlich zum 25. Mai 2018 in Kraft. Viele Unternehmen bereiten sich intensiv auf diesen Termin vor und denken auch darüber nach, ob spezialisierte Produkte wie beispielsweise SAP Information Lifecycle Management (SAP ILM) zum Einsatz kommen können.

Dabei stellen viele Unternehmen in der Diskussion fest, dass bei der technischen Umsetzung von zum Beispiel SAP ILM die notwendigen datenschutzrechtlichen Anforderungen im Vorfeld nicht umfassend geklärt sind. Zu den datenschutzrechtlichen Vorbedingungen zählen im Speziellen die juristische Herleitung für die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten (Personal- und Kundendaten), die daraus resultierenden Aufbewahrungsfristen und die abzuleitenden Löschfristen. Wir stellen in Unternehmen vermehrt fest, dass die juristische Abteilung eine andere Interpretation aus den Anforderungen DSGVO folgert als andere Fachabteilungen, einschließlich der IT-Abteilung. Dieser Beitrag will diese unterschiedlichen Sichtweisen in Einklang bringen und eine zielorientierte Vorgehensweise vorschlagen.

Erhöhter Bedarf nach Unterstützung bei der Umsetzung datenschutzrechtlicher Fragestellungen

Als ein Unternehmen, welches SAP-Technologieberatung anbietet und gleichzeitig im Bereich Compliance und Datenschutz spezialisiert ist, erhalten wir zahlreiche Anfragen, inwieweit und wie wir eine Unterstützung bei Umsetzung der neuen Verordnungen anbieten können. Dabei wollen viele der anfragenden Unternehmen im Kontext ihrer SAP-Systeme spezialisierte Zusatzprodukte einsetzen, häufig SAP ILM.

Erforderliche Vorarbeiten auf unterschiedlichen Ebenen

Die Einführung einer technischen Lösung zur Abbildung der Datenschutz-Grundverordnung – z. B. durch SAP ILM – erfordert Vorarbeiten auf unterschiedlichen Fachbereichsebenen, auch und insbesondere abseits der technischen Ebene.

Diese Vorarbeiten sind nach unseren Erfahrungen häufig nicht oder nur teilweise existent bzw. fehlen Kenntnisse und Informationen. Oftmals sind in den Unternehmen die rechtlichen Anforderungen aus der Datenschutz-Grundverordnung, BDSG-neu, HGB, AO und Arbeitsgesetzen zu bewerten und zu berücksichtigen. Zum Teil sind die jeweiligen Prozesse wie zum Beispiel ein Auskunftsanspruch nach Art. 15 DSGVO, Löschanspruch nach Art. 17 DSGVO oder Sperranspruch (Einschränkung der Verarbeitung) nach Art. 18 DSGVO seitens des Betroffenen im Unternehmen noch nicht etabliert und umgesetzt. Die genannten Rechte der Betroffenen gelten übrigens im Innenverhältnis (Mitarbeiterdaten) wie auch im Außenverhältnis (Kundendaten). Hierbei wird meist dem Thema Mitarbeiterdaten weniger Beachtung geschenkt. Aufgrund der rechtlichen Anforderungen (Arbeitsrecht, Zeiterfassung, Leistungsdatenerfassung, Beurteilungsmanagement etc.) ist die datenschutzrechtliche Bewertung von Mitarbeiterdaten für die Arbeitgeber komplexer und umfassender zu bewerten, um die entsprechenden Ableitungen zu treffen.

Diese Prozesse sind im Unternehmen ganzheitlich zu etablieren und zu verankern. Eine technische Umsetzung mittels SAP ILM ist im Anschluss die mögliche Konsequenz, zum Beispiel, um die Anforderungen einer Löschung von Daten aus datenschutzrechtlichen Gesichtspunkten umzusetzen.

Gesucht: Verfahren, die personenbezogene Daten verarbeiten

Dem bereits aus dem Bundesdatenschutzgesetz bekannten Verfahrensverzeichnis wurde in den vergangenen Jahren wenig Beachtung geschenkt. Aufgrund der Änderungen der Sanktionsmöglichkeiten in der DSGVO kommt dem Verzeichnis der Verarbeitungstätigkeiten (VVT) ein höherer Stellenwert zu. Das VVT bietet jedoch aus unserer Sicht die Möglichkeit, sich ein ganz gutes Bild im Unternehmen zu verschaffen, an welchen Stellen und bei welchen Geschäftsprozessen personenbezogene Daten verarbeitet werden. Die Detaillierung und die Granularität eines solchen Verzeichnisses können dabei von Unternehmen zu Unternehmen deutlich variieren. Wir empfehlen die Erstellung eines übersichtlichen und praktikablen Verzeichnisses. Mithilfe der identifizierten Datenkategorien (personenbezogene Daten) und der Zweckbestimmung kann eine juristische Herleitung der Verarbeitung relativ einfach vorgenommen werden. Im Zuge dessen sollten auch entsprechende Löschklassen und Löschfristen definiert und berücksichtigt werden, die bislang im Unternehmen noch nicht ganzheitlich vorhanden sind bzw. tatsächlich genutzt werden.

Wir empfehlen, dass die Verarbeitung von personenbezogenen Daten – soweit möglich – auf einer Rechtsgrundlage einer gesetzlichen Regelung (z. B. §26 BDSG-neu, Art. 6 DSGVO) beruht. Eine Einwilligung und der sich daraus resultierende mögliche Widerruf entzieht bekanntlich die notwendige Rechtsgrundlage. Eine Löschung der verarbeitenden Daten ist die logische Konsequenz.

Anhand unterschiedlicher datenschutzrechtlicher Projekte mit und ohne SAP-Bezug hat sich ein praxisnahes Vorgehen bei uns etabliert, welches wie folgt skizziert werden kann.

1. Identifikation des Verfahrens oder des Prozesses inkl. der Verarbeitung der personenbezogenen Daten
2. Rechtliche Herleitung bei der Verarbeitung personenbezogener Daten
3. Identifikation der entsprechenden Aufbewahrungsfristen
4. Eingruppierung der Daten in die entsprechenden Löschklassen
5. Anpassung oder Erstellung der entsprechenden Dokumentationen (Löschkonzept etc.)
6. Technische Umsetzung mit dem jeweiligen Tool, zum Beispiel SAP ILM

Der Erfolg solcher Projekte anhand des aufgezeigten Vorgehens zeigt, dass eine vorrangig technische Produktdiskussion im Kontext der DSGVO und des BDG-neu nicht ausreichend ist. Somit ist die Einbindung aller Fachabteilungen – inklusive Legal – notwendig, um eine einheitliche Umsetzung der Anforderungen zu ermöglichen.

Vorarbeiten führen zur beschleunigten und reibungslosen Umsetzung, mit und ohne SAP ILM

Die Einführung von SAP ILM oder anderen technischen Lösungen gelingt auf Basis der skizzierten Vorarbeiten deutlich beschleunigt und reibungsloser. Aus unserer Erfahrung heraus sind die entsprechenden Vorarbeiten zwingend erforderlich. Die jeweiligen Fachbereiche, bestehend aus Personal, Marketing, Legal, IT, Geschäftsleitung und Compliance (Datenschutzbeauftragter), sind in die Vorarbeiten einzubinden, jedoch ist deren Anteil (im Sinne von Arbeitsbelastung) als gering einzustufen. Sind die personenbezogenen Daten analysiert und die betroffenen Prozesse/Verfahren identifiziert, so steht mit SAP ILM eine leistungsfähige Lösung zur gezielten Sperrung oder Löschung von Daten zur Verfügung. Wichtig zu erwähnen ist, dass es auch ausreichend sein kann, die Standardfunktionalitäten eines SAP-Systems zu nutzen (SAP Datenarchivierung), um eine regelkonforme Umsetzung des Datenschutzes zu erreichen. Dies ist jedoch vom jeweiligen Verfahren abhängig, welches personenbezogene Daten verarbeitet. So kann beispielsweise das Ende des Vorgangs aus datenschutzrechtlicher Sicht unterschiedlich im SAP-Kontext gesehen werden. SAP ILM unterscheidet an dieser Stelle EOB und EOP. Hier muss gemeinsam mit der Fachabteilung eine konforme Lösung erarbeitet werden, damit der Aufsetzpunkt der Löschung – der z. B. auch für SAP ILM notwendig ist – korrekt definiert ist.

Werkzeuge und Vorgehensweisen

Aufgrund unserer Erfahrungen in zahlreichen Projekten zur dargestellten Umsetzung der datenschutzrechtlichen Anforderungen haben wir Werkzeuge und Vorgehensweisen entwickelt, mit denen wir bei der Einführung von SAP ILM und anderen technischen Lösungen beratend und praktisch zur Seite stehen.

Bei der Beratung helfen die von uns entwickelten Werkzeuge und Vorgehensweisen aus der DSGVO-Beratung, um eine Einführung von beispielsweise SAP ILM zu gewährleisten.

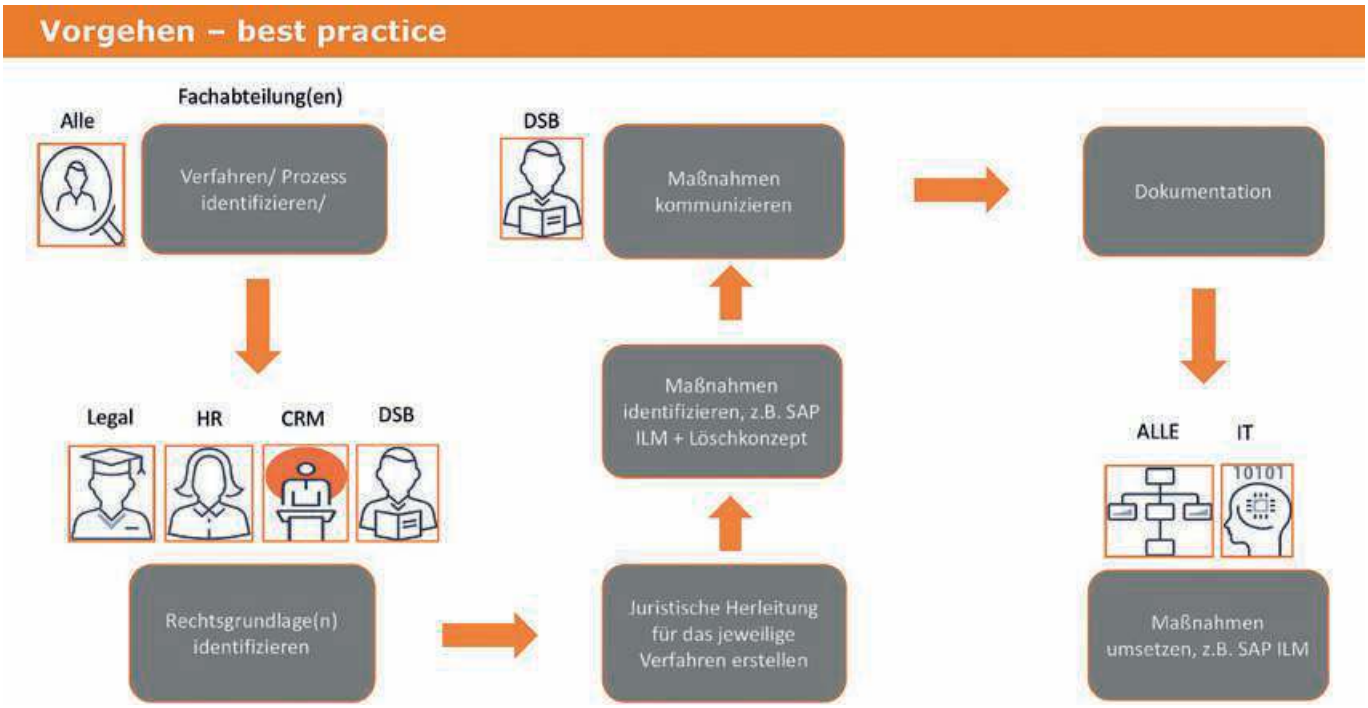
Wir empfehlen, die datenschutzrechtlichen Anforderungen durch ein schrittweises Vorgehen umzusetzen, welches sich aus unserer Sicht wie in der Abbildung unten dargestellt strukturiert.

Abschließend lässt sich festhalten, dass die Änderungen durch die DSGVO und das BDSG-neu auch eine gute Möglichkeit bieten, bestehende Prozesse zu hinterfragen, neu zu etablieren oder anzupassen. Die möglichen Sanktionsmöglichkeiten der Aufsichtsbehörden sollten nicht alleine im Vordergrund stehen, wenn technische und auch prozessuale/organisatorische Maßnahmen umgesetzt werden können bzw. werden müssen. Das Vermeiden von Risiken bekommt mit den Änderungen vom Mai 2018 nun auch im Datenschutzrecht einen anderen Stellenwert. Hierbei sollte die Vermeidung von Imageverlust, Schadensersatz und Haftung im Vordergrund stehen.

Und schließlich: Erwarten wir von anderen Unternehmen nicht auch, dass unsere persönlichen Daten sicher sind und dass damit bewusst umgegangen wird?

entplexit
make IT simple

entplexit GmbH
Kölner Straße 12
65760 Eschborn
Telefon: +49 6196 97344-00
information@entplexit.com
www.entplexit.com



Rückstellungen bilden ist nicht die einzige Option

Sofortmaßnahme Weitergabekontrolle

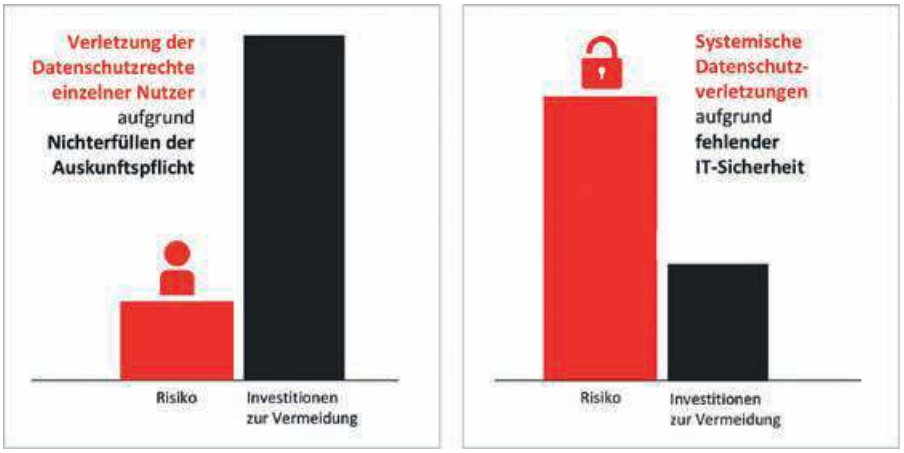
CIOs, die die Verbreitung von personenbezogenen SAP-Daten innerhalb des Unternehmens unter Kontrolle halten, reduzieren mit wenig Aufwand den größten Anteil des Risikos für Strafzahlungen und sparen Zeit und Kosten für das Lokalisieren, Sperren und Löschen sensibler Daten.

Holger Hügel ist Vice President Products & Services bei Secude.

In der SAP-Community kursieren die Anforderungen der EU-DSGVO schon seit geraumer Zeit. Im Kern geht es um die Identifizierung personenbezogener Daten in der SAP-Systemlandschaft, deren Pseudonymisierung in Kopien des Produktivsystems sowie das zeitnahe Beauskunften, das Sperren und schließlich das Löschen einzelner Nutzerdaten. Mit dem Ende der Übergangsfrist am 25. Mai 2018 wird die viel diskutierte Thematik nun zur Realität. Trotzdem stehen viele Unternehmen immer noch vor einem riesigen Aufgabenberg, dessen Abtragung laut der Mehrzahl der Berater mindestens ein Jahr dauern soll. Wer Anfang 2018 noch kein Projekt aufgesetzt hat, sollte besser Rückstellungen für den Fall eines grundsätzlichen Verstoßes bilden – so die durchaus ernst gemeinte Empfehlung der Experten.

Kein Datenschutz ohne Datensicherheit

Aber was macht die Projekte eigentlich so kompliziert? Die vorhergesagte Langwierigkeit des Vorhabens resultiert nicht nur aus der schwierigen Umsetzung einer zweckbestimmten Verarbeitung der personenbezogenen Daten, sondern auch aus der Komplexität der heutigen Unternehmensprozesse. Auch wenn SAP-Anwendungen eine zentrale Rolle spielen, verteilen sich die einzelnen Prozessschritte oft über mehrere Anwendungen. Daten werden aus SAP-Systemen exportiert und in anderen Non-SAP-Applikationen, wie zum Beispiel Microsoft Excel, weiterverarbeitet. Dadurch werden sie der Kontrolle des SAP-Berechtigungswesens und des Information Lifecycle Managements (ILM) entzogen. Das Sperren und Löschen von Daten ist in solchen Fällen sehr schwierig – wenn nicht sogar unmöglich. Trotzdem investieren die meisten Unternehmen derzeit hauptsächlich in Projekte zur Erfüllung ihrer Auskunfts- und Löschpflicht. Dabei birgt eine fehlende IT-Sicherheitsmaßnahme wie die Weitergabekontrolle von Daten ein weitaus schwerwiegenderes Risiko für grundsätzliche Verstöße gegen die DSGVO: Von Einzelfällen, in denen – auf Anfrage der betroffenen Person – keine umfängliche und unmittelbare Auskunft, Sperrung oder Löschung vorgenommen werden konnte, geht laut Expertenmeinung kaum ein Risiko für hohe Strafzahlungen aus. Ganz anders verhält es sich, wenn jedoch Aufsichtsbehörden systematische Verletzungen der DSGVO aufdecken, die sich aus fehlender technischer Datensicherheit ergeben. Ohne ein funktionierendes IT-Sicherheitskonzept fehlt die Basis für jegliche Datenschutzmaßnahmen.



Risikoeinschätzung und Investitionen stehen bei vielen SAP-Kunden noch nicht im richtigen Verhältnis.

Noch ist es nicht zu spät

Die Kontrolle der Datenexporte aus SAP-Anwendungen gehört damit zu den grundsätzlichen Maßnahmen für eine DSGVO-konforme Verarbeitung personenbezogener Daten. Mithilfe schnell einsetzbarer Sicherheitslösungen wie Secude Halocore und automatisierter Klassifikation der Downloads lassen sich unautorisierte Exporte wirksam verhindern. Gleichzeitig können Daten, die außerhalb von SAP benötigt werden, mit dem gleichen Schutzbedarf wie innerhalb der SAP- Anwendung versehen und dadurch wirksam geschützt werden. Für die Absicherung der SAP-Daten in unstrukturierten Dokumenten ist im Halocore-Konzept der De-facto-Standard von Microsoft zuständig. Mit Microsoft AIP/RMS lassen sich alle Dokumentenarten verschlüsseln und dadurch der Zugriff sowie die Verarbeitungsrechte granular kontrollieren. Das schützt personenbezogene Daten und senkt den entscheidenden Anteil des Risikos für Strafzahlungen aufgrund von DSGVO-Verletzungen. Gleichzeitig werden auch unternehmenskritische Daten, wie zum Beispiel geistiges Eigentum, vor Missbrauch und Verlust bewahrt.

Bitte beachten Sie auch den Community-Info-Eintrag Seite 108

SECUDE

Verarbeitungstätigkeiten dokumentieren, Maßnahmen ableiten

Prozessorientierte Methodik zur Umsetzung der EU-DSGVO

Die Bundesanstalt für Immobilienaufgaben (BImA) stellt sich mit konzeptioneller und technischer Unterstützung des IT-System- und Beratungshauses CONET in Prozessanalyse und Prozessdokumentation der Umsetzung der europäischen Datenschutz-Grundverordnung (EU-DSGVO).

Mit einem Portfolio von Grundstücken mit einer Gesamtfläche von rund 490.000 Hektar und 38.000 Wohnungen sowie etwa 6000 Mitarbeitern ist die BImA einer der größten Immobilieneigentümer Deutschlands und verarbeitet entsprechend große Mengen an personenbezogenen Daten (pbD) wie Mieter-, Käufer-, Verkäufer- und Interessentendaten. Daher begann die BImA bereits 2016 mit der Planung zur Umsetzung der Vorgaben der EU-DSGVO und des BDSG-neu.

Geschäftsprozessmanagement als Basis

Um alle Anforderungen lückenlos umzusetzen und erforderliche Maßnahmen ableiten zu können, bietet sich ein Vorgehen entlang einer prozessorientierten Methodik an: Im Geschäftsprozessmanagement sind bereits alle relevanten Abläufe und Abhängigkeiten definiert und dokumentiert. So lassen sich im Falle der BImA beispielsweise bei der Erstellung eines Mietvertrags auf einen Blick die beteiligten Vorlagen, Personengruppen, IT-Systeme und eben auch alle dort gegebenenfalls verarbeiteten pbD einfach identifizieren. Damit liegen weitreichende Informationen bereits vor. Es fehlen lediglich im Prozessmodell noch genaue Angaben dazu, welche pbD im Einzelnen verarbeitet werden, zu welcher Datenkategorie und zu welcher Personengruppe diese Daten gehören und ob besondere personenbezogene Daten erfasst werden. Diese Angaben lassen sich zusammen mit den relevanten Schutzbedarfskategorien und Sperr- und Löschfristen einfach im Prozessmodell ergänzen, womit dieses zu einem vollständigen Informationsträger für alle datenschutzrelevanten Details wird.

Verarbeitungstätigkeiten identifizieren

Auf dieser Basis lassen sich die einzelnen Verarbeitungstätigkeiten identifizieren, deren Inhalte sich aus allen Informationen, die sich an den Objekten (Fachbegriffen, Tätigkeiten, IT-Systemen, Prozessrollen) innerhalb der zugeordneten Prozesse befinden, bestimmen.

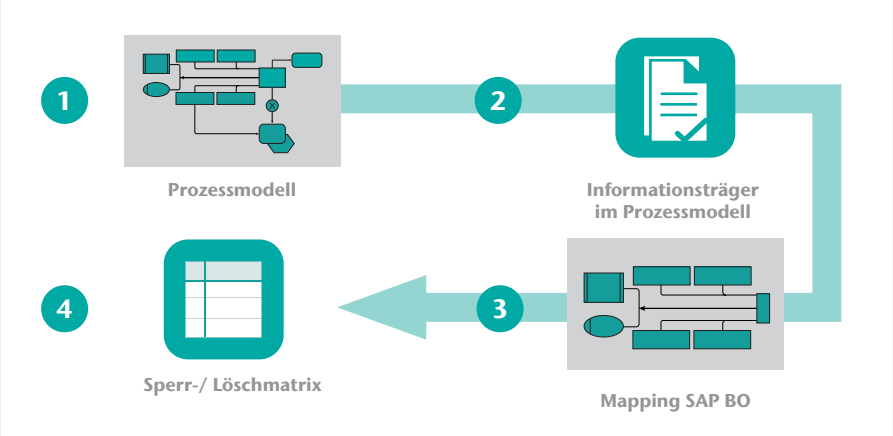
Eine Datenschutzfolgeabschätzung sowie eine dedizierte Risikobewertung dienen dann dazu, die Risiken für jede Verarbeitungstätigkeit zu bewerten und diese mithilfe geeigneter sogenannter technisch-organisatorischer Maßnahmen (TOM) zu minimieren. Dabei werden je Verfahren die Notwendigkeit, die Verhältnismäßigkeit sowie die Risiken für die Rechte und Freiheiten des betroffenen Individuums untersucht. Damit liegen dann alle Informationen vor, um die Verarbeitungstätigkeiten entsprechend den Vorgaben zu dokumentieren und jederzeit etwa bei einer Prüfung durch die Aufsichtsbehörden aktuelle Berichte aus den Geschäftsprozessmodellinformationen zu erzeugen.

Technische Umsetzung in SAP

Auf der SAP-Seite ergeben sich aus den definierten TOM wiederum verschiedene technische Umsetzungsaufgaben: So sind beispielsweise entsprechende Rollen- und Berechtigungskonzepte für die SAP-Systeme der BImA mitsamt dem Aufbau eines funktionierenden Systems zur Zugriffsprotokollierung und zur Meldung von Datenschutzvorfällen zu etablieren. Dazu gehört als Grundlage auch der Aufbau eines Datenschutzmanagementmodells mit festgelegten Verantwortlichkeiten.

Schließlich sind auch Konzepte und technische Lösungen zur zeitgerechten Erfüllung der umfangreichen Informations- und Reaktionspflichten gegenüber Betroffenen bezüglich ihrer gespeicherten Daten und eine entsprechende Auskunftsstruktur zu etablieren.

Um die Anforderungen zum Sperren und Löschen von Daten für ein SAP-System abzuleiten, wird auch wieder auf die Informationen des Geschäftsprozessmodells zurückgegriffen. Da im SAP-System ein Sperren und Löschen der pbD nur an den verwendeten Business-Objekten (BO) umgesetzt werden kann, erfolgt ein Mapping zwischen den SAP-Systemen mit ihren Business-Objekten und den Informationsträgern im Prozessmodell sowie die Fixierung entsprechender Regeln in einer Sperr- und Löschmatrix, die die Bezugsgrößen/Felder und Abhängigkeiten abbildet. Damit kann die technische Umsetzung im SAP-System erfolgen.



Schematische Darstellung der Umsetzung des Lösch- und Sperrkonzepts.

CONET

CONET Business Consultants GmbH

Humperdinckstraße 1
53773 Hennef
Telefon: +49 2242 939-0
info@conet.de
www.conet.de

Neue gesetzliche Anforderungen verlangen nach einer zertifizierten Archivierungslösung im Back-End

Ist Ihre SAP®-Datenarchivierung fit für die DSGVO?

Die EU-DSGVO kommt – und mit ihr neue Anforderungen an die Archivierung und Löschung personenbezogener Daten. Unternehmen sind gut beraten, ihre Prozesse und Systeme jetzt zu überprüfen.

Die zweijährige Übergangsfrist ist bald vorbei und die EU-Datenschutz-Grundverordnung (DSGVO) wirft nun nicht mehr nur ihre Schatten voraus – sondern sie tritt am 25. Mai 2018 tatsächlich in Kraft. Mit der DSGVO wird der Datenschutz jetzt erstmals auf europäischer Ebene einheitlich geregelt und somit stellt die Datenschutz-Grundverordnung besondere Anforderungen an die Speicherung und Verarbeitung personenbezogener Daten. Dies betrifft beispielsweise Datensicherheit, Datensparsamkeit, Zweckbindung, Richtigkeit, Vertraulichkeit und Dokumentation. Zudem gibt es Regeln für Speicherfristen und das Löschen von personenbezogenen Daten, die unter anderem in Artikel 17 „Recht auf Löschen" beschrieben sind. Auch Artikel 5 legt fest, dass „personenbezogene Daten grundsätzlich nur für einen bestimmten Verarbeitungszweck gespeichert werden dürfen, und nur so lange, wie es für den jeweiligen Zweck erforderlich ist".

Archivierungslösungen gehören auf den Prüfstand

Unternehmen aller Größen und Branchen sind jetzt also gefordert, ihre Prozesse schnellstens zu prüfen und DSGVO-compliant aufzusetzen. Betroffen sind jedoch nicht nur die „klassischen Systeme" zur Verarbeitung personenbezogener Daten wie HR- oder CRM-Anwendungen, sondern auch Archivierungsprozesse und -lösungen. Denn in diesen muss beispielsweise das „Recht auf Vergessen" prozess- und systemseitig umgesetzt werden.

Mit SAP® ILM und Columbus DW von Macro 4 können Unternehmen die DSGVO-Vorgaben hinsichtlich Datenarchivierung und -löschung erfüllen.

Für SAP®-Anwendungen steht mit SAP ArchiveLink® seit Langem eine Schnittstelle zu Archivierungslösungen mit Basisfunktionalität zur Verfügung. Diese war in der Vergangenheit für viele Anwender völlig ausreichend. Allerdings ist SAP ArchiveLink® den gestiegenen Anforderungen aus der DSGVO jetzt nicht mehr gewachsen. Für einen Großteil der Unternehmen könnte deshalb eine Erweiterung von SAP ArchiveLink® auf SAP® Information Lifecycle Management (ILM) anstehen.

Mit SAP® ILM werden die SAP®-Standardauslieferungen um die Fähigkeit ergänzt, den Lebenszyklus produktiver und archivierter Daten aufgrund von Regeln zu verwalten. SAP® ILM erfüllt bereits in der Basisversion alle rechtlichen Vorgaben der DSGVO. Doch damit allein ist es nicht getan: Anwender benötigen zusätzlich eine von SAP® zertifizierte Archivierungslösung als Back-End. Diese muss alle in SAP® ILM definierten Regeln und Funktionalitäten unterstützen und deren konkrete Anwendung auf Daten und Dokumente ermöglichen. Erst die Kombination aus SAP® ILM und zertifizierter Archivierungslösung ermöglicht Unternehmen den DSGVO-konformen Betrieb ihrer SAP®-Landschaft.

Revisionssichere Archivierungslösung als Back-End

Bereits seit der Einführung von SAP® ILM bietet Macro 4 mit Columbus DW ein von der SAP® zertifiziertes Online-Archivsystem für die revisionssichere Speicherung, Verarbeitung und Bereitstellung von Geschäftsdokumenten und Daten. Über Columbus DW können alle Funktionalitäten aus SAP® ILM optimal genutzt werden. So lassen sich beispielsweise Aufbewahrungsregeln zur Abbildung gesetzlicher Vorgaben und Anwendung dieser Vorgaben auf produktive und archivierte Daten definieren. Daten, die noch für Rechtsfälle relevant sind, können gegen vorzeitiges Vernichten gesperrt werden. Und gleichzeitig lässt sich die Vernichtung von Daten unter Berücksichtigung gesetzlicher Vorgaben und rechtsfallbedingter Sperren automatisiert regeln. Für alle Szenarien können Zugriffsbeschränkungen sowohl auf Datensatz- als auch auf Dokumentenebene vergeben werden.

Zwei Fliegen mit einer Klappe: DSGVO-compliant und kostenoptimiert

Mit der Kombination aus SAP® ILM und Columbus DW als zertifizierte Archivierungslösung sind Unternehmen in der Lage, die Anforderungen der EU-Datenschutz-Grundverordnung in puncto Archivierung und Löschung von Daten rechtskonform umzusetzen. Zusätzlich spart eine optimale Archivierung Speicherplatz und Kosten, wenn operativ nicht mehr benötigte Daten in ein kostengünstigeres Online-Speichermedium ausgelagert und Daten entsprechend den gesetzlichen Vorgaben vernichtet werden.

MACRO4
A Division of UNICOM® Global

Macro 4 GmbH
Humboldtstraße 10
85609 Aschheim
Telefon: +49 89 6100970
market.de@macro4.com
www.macro4.com

Kundendaten DSGVO-konform verwalten

Die EU-DSGVO wirft ihre Schatten voraus. Um die neuen Rechte der Klientel zu gewährleisten, müssen die entsprechenden Daten ganzheitlich und durchgängig verwaltet werden. Mit SAP Hybris Gigya können Unternehmen nicht nur einen Riesenschritt in Richtung DSGVO-Konformität gehen, sondern auch die Customer Experience entscheidend verbessern.

Am 25. Mai dieses Jahres wird es ernst: Bis dahin müssen Unternehmen jeglicher Größe die Vorschriften der neuen europäischen Datenschutz-Grundverordnung (EU-DSGVO) umsetzen. Verbraucher werden dadurch mit nie da gewesenen Rechten und Ansprüchen ausgestattet, was den Umgang mit ihren persönlichen Daten betrifft. In der Pflicht sind alle Organisationen, die personenbezogene Informationen erheben, speichern oder verarbeiten – unabhängig vom Umfang der gesammelten Daten und dem Speicherzweck. Das trifft so gut wie auf jedes Unternehmen zu. Denn um mit Kunden in Kontakt zu treten und zu interagieren, müssen die entsprechenden Daten in irgendeiner Weise in einer Datenbank oder einem CRM-System vorliegen.

Dabei gilt das im April 2016 beschlossene Regelwerk nicht nur für Firmen, die ihren Sitz in einem Mitgliedsland der EU haben. Betroffen sind auch Unternehmen, die lediglich mit Daten von EU-Bürgern arbeiten, auch wenn sie außerhalb der EU operieren – ganz gleich, ob Ein-Mann-Betrieb, Mittelständler oder Großkonzern. Mit den weitreichendsten Verpflichtungen konfrontiert sehen sich Institutionen, die eine große Menge von Nutzerdaten (Big Data) sammeln, wie etwa Internet-Konzerne, Suchmaschinen-Betreiber, Handelsportale, Vermittlungsplattformen, Online-Shops, Mobilfunkanbieter, Finanzinstitute oder Social-Media-Dienste. Aber auch klassische, stationäre Geschäftsmodelle sehen sich vor die enorme Herausforderung gestellt, die in jahrzehntelanger, akribischer Kleinarbeit gesammelten Kontaktdaten aufzufinden, zu konsolidieren und zu bereinigen. Denn für sie alle gilt: Sie müssen unter anderem auf Anfrage der Kunden detailliert über die erhobenen Daten und deren Verwendung Auskunft geben. Überdies dürfen die betroffenen Personen die Berichtigung und sogar die Löschung der jeweiligen Daten verlangen. So gewährleistet die DSGVO also erstmalig in der Geschichte der Datenverarbeitung ein „Recht auf Vergessenwerden“.

Heiko Jungholt, Principal KPS AG.

Hohe Strafen bei DSGVO-Verstoß

Bei nicht fristgerechter Umsetzung oder konkreten Verstößen gegen die Bestimmungen drohen empfindliche Strafen: Im Extremfall können Unternehmen zur Zahlung von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes verpflichtet werden. Dieses Strafmaß ist für kein Unternehmen zu vernachlässigen, insbesondere da die DSGVO auch eine persönliche Haftung der Geschäftsführung vorsieht. Gerade digitale Geschäftsmodelle sind in zunehmendem Maße datengetrieben und einige von ihnen werden daher in der Öffentlichkeit häufig als „Datenkraken" gebrandmarkt. Experten sehen nach Inkrafttreten der DSGVO eine übergreifende Klagewelle auf deutsche Unternehmen zurollen: Denn nimmt man analog zu den Beschwerden an, dass nur fünf Prozent der Betroffenen mit einem Problem ihr Recht gerichtlich durchsetzen würden, dann ergibt sich bereits ein beträchtliches Volumen – gerade vor dem Hintergrund aktueller Diskussionen zu sozialen Netzwerken. An eine künstliche Akzelerierung analog der Abmahnwelle rund um das Thema „fehlerhafte Website-Impressen" mag man erst gar nicht denken.

Da die Umsetzungsfrist bereits in wenigen Wochen verstreicht, müssen die betroffenen Unternehmen zeitnah reagieren. Der erste Schritt sollte das Aufstellen eines Prozesskatalogs sein, welcher immer organisatorisch von einem Datenschutzbeauftragten begleitet werden sollte, um sämtliche Prozesse rund um die Speicherung und Verwaltung personenbezogener Informationen auf sichere und DSGVO-konforme Beine zu stellen. Um dann notwendige Änderungen wirtschaftlich zu kanalisieren und zu automatisieren, ist der Einsatz einer zentralen Komponente für das Management von Kundendaten zu empfehlen. Besonders gut geeignet sind Systeme für das Consumer Identity und Access Management (CIAM), weil sie als Service einfach in Bestandsinfrastrukturen integriert werden können und Datensilos ersetzen. Sie unterstützen dabei, zu Kunden digitale Beziehungen aufzubauen und die Kundenbindung zu festigen. Mit den Systemen lassen sich gesammelte Daten mit dem Einverständnis der Klientel zu umfassenden Kundenprofilen zusammenführen und setzen somit den digitalen Grundsatz einer „Customer Centricity" systemisch um. Durch die nahtlose Integration der Daten in professionelle Commerce-, Marketing- und Serviceanwendungen erhält der Kunde personalisierte und passgenaue Empfehlungen auf der gesamten Customer Journey. Single- oder Cross-Channel-Unternehmen realisieren dadurch eine bessere Customer Experience.

Gewinnbringende Kundenbeziehungen aufbauen und festigen

Der Marktführer für CIAM-Lösungen ist die Firma Gigya, die mittlerweile zu SAP gehört. Deren ganzheitliche CIAM-Plattform, inzwischen SAP Hybris Gigya, trägt dazu bei, die Zahl der Registrierungen im Online-Umfeld zu erhöhen und dabei erlaubnisbasiert Kunden über verschiedene Geräte hinweg zu identifizieren. Unterstützt wird Gigya von der Unternehmensberatung KPS AG. Sie ist auf Strategie-, Prozess-, Applikations- und Technologie-Consulting im Handel und der Konsumgüterbranche spezialisiert und verfügt insbesondere über eine fundierte Erfahrung mit SAP Hybris. Mit ihrer gebündelten Kompetenz versetzen die beiden Partner Unternehmen in die Lage, gewinnbringende Kundenbeziehungen zum beiderseitigen Nutzen aufzubauen und langfristig zu festigen. Dabei bleibt der Schutz der Privatsphäre von Kunden auch in einem immer komplexeren regulatorischen Kontext immer gewahrt – vor allem im Hinblick auf die DSGVO.

Um Organisationen fit für die Umsetzung der neuen Richtlinien zu machen, müssen zunächst die Integrierten Prozessstrecken (IPS) rund um die Interaktion mit Kunden und den Umgang mit deren Daten betrachtet, analysiert und ausgewertet werden. Dabei treffen die Berater häufig auf ein bestimmtes Grundmuster: Zwar betreiben Unternehmen in ihrem digitalen Ökosystem meist umfassende Lösungen für das Informationsmanagement und die Marketing-Automation wie etwa CMS-, E-Commerce-, DMP- oder CRM-Systeme. Dennoch herrschen oftmals Silo-Architekturen mit fragmentierten Kundenidentitäten vor. Das bedeutet, die Daten sind in unterschiedlichen, häufig voneinander isolierten Systemwelten gespeichert. In einem solchen heterogenen Umfeld ist es nahezu unmöglich, den digitalen Anwendern eine End-to-End User Experience zu bieten und die strikten Anforderungen der DSGVO hinreichend umzusetzen.

In der Konsequenz mangelt es an der nötigen Transparenz und Kontrolle über Beziehungen und Zusammenhänge in der Interaktion zwischen Unternehmen und Kunden. Dies betrifft beispielsweise die Einsicht in Profildaten, die Ausgestaltung der Marketing-Kommunikation hinsichtlich Brands, Produkten und Interessen, die Wahl der einzelnen Marketing-Kanäle wie E-Mail, SMS oder Telefon, die Frequenz der Kundenansprache sowie die Einhaltung von allgemeinen Geschäftsbedingungen und Datenschutzrichtlinien. Ohne diese Transparenz wird es den Kunden schwerfallen, Vertrauen zum Unternehmen aufzubauen und der Speicherung sowie Verarbeitung der personenbezogenen Daten im Sinne der DSGVO vollumfänglich zuzustimmen. Erlangen Kunden jedoch die volle Kontrolle über ihre Daten und wissen genau, auf welche Weise diese genutzt werden, können sie Vertrauen schöpfen und sind eher zur Kooperation zum beiderseitigen Nutzen bereit.

Silo-Strukturen aufbrechen

Vonnöten ist vorab eine klar definierte Prozesslandschaft, die vorhandene, organisatorische Silo-Strukturen aufbricht und dabei hilft, Kundenidentitäten übergreifend zu integrieren – und zwar entlang der gesamten Customer Journey. Und genau hier greift die CIAM-Plattform SAP Hybris Gigya: Im Rahmen einer dreistufigen Funktionsarchitektur (Identity, Consent, Profile) macht die Lösung aus unbekannten Nutzern transparente, wertgeschätzte und loyale Kunden. In der ersten Stufe (Identity) wird geregelt, wie die Daten generiert werden. Es geht darum, über welche Touchpoints und Applikationen die Kunden ihre Daten eingeben und hinterlassen, sich also registrieren, anmelden oder einloggen. Dies kann beispielsweise über Online-Shops, Vermittlungsplattformen oder soziale Netzwerke erfolgen. Die zweite Stufe (Consent) bietet Funktionen für die Verwaltung der Daten und eröffnet Möglichkeiten, diese legal und rechtskonform zu nutzen. Verarbeitet werden unter anderem die Präferenzen der Kunden bezüglich der Kommunikationskanäle und das Opt-in-Management. Insbesondere hier müssen die Datenschutzregeln der DSGVO beachtet werden. Das dritte Funktionsmodul (Profile) integriert alle denkbaren Verwaltungsprozesse, um die Informationen anzureichern. Dadurch entstehen aussagekräftige Daten, die wertvolle Einblicke zu den Vorlieben und Wünschen der Kunden liefern. Selbstverständlich werden auch hierbei alle rechtlichen Vorgaben strikt eingehalten.

Um die Kundenbeziehung strukturiert und strategisch sinnvoll aufzubauen, nutzt die CIAM-Lösung eine Vorgehensweise in drei logischen Schritten: Connect – Collect – Convert. Dabei wird im ersten Schritt die Verbindung zwischen den Akteuren hergestellt. Unternehmen verwandeln anonyme Benutzer in bekannte Kunden und erfassen hierbei erlaubnisbasiert, sicher und umfassend deren Daten. Im zweiten Schritt wachsen mit Einverständnis des Kunden aussagekräftige, einheitliche Profile, die präzise Einblicke in dessen Bedürfnisse, Präferenzen und Wünsche ermöglichen. Im dritten Schritt schließlich vertieft das CIAM-System mittels einfacher Integration von Customer-Insights- und Analytics-Tools den Einblick in die Zielgruppe. Die erfassten Daten werden nahtlos in andere digitale Lösungen integriert und konsequent genutzt, um die Kunden langfristig zu binden. Die Lösung ermöglicht also genau das richtige Maß an Personalisierung und Vertraulichkeit – optimale Voraussetzungen für erfolgreiche Beziehungen im „Zeitalter des Kunden".

Kundendaten über alle Touchpoints hinweg verwalten

Die CIAM-Plattform implementiert dabei einen übergreifenden, cloudbasierten Layer, der sämtliche Kundendaten redundanzfrei in einem Gesamtsystem verwaltet. Ganz gleich, über welchen Touchpoint der Kunde mit dem Unternehmen interagiert – ob mobile App, Webshop oder Social-Media-Plattform: In allen Systembereichen stehen konsistent alle persönlichen Daten zur Verfügung. Somit lassen sich Informationen zur Beantwortung wichtiger Fragen besser verknüpfen, um den maximalen Nutzen aus der Kundenbeziehung zu generieren: Welche Produkte oder Dienstleistungen hat der Kunde bereits gekauft? Für welche Produkte hat der gleiche Kunde sich interessiert, aber noch keine Kaufentscheidung getroffen? Welche Rabatte wurden ihm bisher gewährt? Wie viele Retouren hat er veranlasst? Hat er schon Feedback über bestimmte Leistungen abgegeben? Mit welchem Tenor? Unternehmen sind dadurch in der Lage, über alle Vertriebskanäle hinweg bessere Services zu bieten und die Bedürfnisse der Kunden gezielter zu befriedigen.

Und wie kann nun der Kunde seine Rechte und Ansprüche aus der DSGVO mithilfe der CIAM-Lösung optimal durchsetzen? Hierfür stehen entweder ein Dashboard oder REST-Schnittstellen für die Integration in beliebige UIs zur Verfügung. Ein Kunde bekommt dadurch eine Übersicht über seine persönlichen Daten, die vom Unternehmen gespeichert und verarbeitet werden. Jederzeit kann er die Informationen nicht nur einsehen, sondern auch herunterladen, bearbeiten und verändern. Dies betrifft sowohl inhaltliche Daten wie Name, Telefonnummer, E-Mail-Adresse und Anschrift als auch Policies, Privatsphäre-Einstellungen, Kommunikations-Präferenzen sowie die Art der Datennutzung. Somit hat es der Kunde komplett selbst in der Hand, auf welche Weise das Unternehmen mit ihm interagiert. Dies erhöht sein Vertrauen und die Bereitschaft, sich an die Firma zu binden. Und schließlich kann der Kunde über das Dashboard seine persönlichen Daten sogar sperren und löschen. So bietet die Lösung einen soliden Beitrag für die Umsetzung der Vorschriften aus der DSGVO.

Fazit

Durch das Inkrafttreten der DSGVO sehen sich Unternehmen mit ganz neuen Herausforderungen konfrontiert, was die Erfassung, Speicherung und Verarbeitung personenbezogener Kundendaten betrifft. Wichtig ist dabei nicht nur, die Verwaltung der Informationen, sondern auch die Interaktion und den Umgang mit den Kunden auf den Prüfstand zu stellen und an die Anforderungen der neuen Datenschutzrichtlinie anzupassen. Optimale Unterstützung für die Umsetzung bietet eine Lösung für das Consumer Identity und Access Management (CIAM). Der führende Anbieter Gigya stellt in Zusammenarbeit mit der Unternehmensberatung KPS AG hierfür eine passgenaue Plattform bereit: SAP Hybris Gigya enthält praktikable Tools, mit denen sich Kundenidentitäten über Silo-Strukturen hinweg zusammenführen und durchgängig verwalten lassen. Dies erleichtert nicht nur die Einhaltung der DSGVO-Vorschriften. Auch erhält der Kunde dadurch die volle Kontrolle und Transparenz über seine Daten und kann mehr Vertrauen zum Unternehmen aufbauen.

KPS

KPS AG
Beta-Str. 10 H
85774 Unterföhring

DSGVO-Umsetzung

Ganzheitlich die dreidimensionale Vernetzung in SAP betrachten

SAP-Landschaften sind zu komplex, als dass es die eine Lösung gäbe, die Datenintegrität perfekt zu wahren. Vielmehr empfiehlt es sich, das große Ganze im Blick zu behalten und die strengen Datenschutzvorgaben der EU strukturiert umzusetzen. Auf diese Weise kann das nötige Verzahnen von Cloud, Geschäft und Recht gelingen.

Viele SAP-Anwendungen von Anbietern, die SAP-zertifiziert sind, versprechen dem Anwender, schnell agieren zu können, genau so, wie es die EU-Datenschutz-Grundverordnung (EU-DSGVO) vorschreibt. Das Regelwerk verschärft ab dem 25. Mai die Vorgaben für das Sammeln, den Zugriff, die Verwendung, das Speichern und die Weitergabe von personenbezogenen Daten. Wer Kundengeschäft mit EU-Bürgern betreibt, hat die Regelungen wie etwa „Privacy by Design und Default“, das „Recht auf Vergessenwerden“ und das Prinzip der Datensparsamkeit zu befolgen. Bei Verstößen gegen die DSGVO drohen Unternehmen Strafen bis zu 20 Millionen Euro oder bis zu vier Prozent ihres weltweit erzielten Jahresumsatzes. Der Wunsch, Aufwand und Kosten im Zaum zu halten und trotzdem Compliance herzustellen und solch drakonische Strafen zu verhindern, ist verständlich. Für viele SAP-Anwender erfüllt SAP NetWeaver Information Lifecycle Management (ILM) diese Anforderung, denn mit dem ILM lassen sich personenbezogene Daten sperren und löschen.

Allerdings kann es die eine, universelle und einfache Lösung, die für ein gesamtes SAP-Ökosystem die nötige DSGVO-Konformität herstellt, schlichtweg nicht geben. Die Vielfalt und Komplexität einer SAP-Landschaft stehen dem entgegen. Die ursprüngliche dreiteilige Systemlandschaft aus Entwicklung, Test und produktivem Betrieb besteht zwar im Grunde immer noch, aber Anwendungen von unterschiedlichen SAP-Partnern erweitern das Spektrum ständig, wobei aktuell Internet of Things (IoT), Blockchain oder maschinelles Lernen im Fokus stehen. Eine SAP-Umgebung weist daher heute wesentlich mehr Ebenen auf, inklusive der Abbildung von Prozessen, die personenbezogene Daten aufweisen. Deshalb reicht das Herstellen von Compliance auf Geschäftsprozessebene und im Human Capital Management (HCM) allein nicht mehr aus.

Thomas Herrmann,
Business Development Manager SAP bei NetApp.

Zirkulation von personenbezogenen Daten

So nutzen beispielsweise Anwendungen für das Gesundheitswesen kritische personenbezogene Informationen, die ein hohes Schutzniveau verlangen. Oder für E-Commerce besteht die Anforderung, Kreditkartendaten sicher zu verarbeiten. In einem SAP-System, das nur im eigenen Rechenzentrum betrieben wird, zirkulieren personenbezogene Daten aufgrund der Vernetzung von ERP, PLM, SCM, CRM und vielem mehr. Die Datenschutzherausforderung schließt zudem Test- und Entwicklungssysteme ein, wenn diese reelle Datensätze verwenden.

Mittlerweile setzen viele Firmen auf Geschäftsmodelle, die nur noch auf Daten basieren. In dem Fall muss die Datenverteilung automatisiert in der SAP-Landschaft und zu extern vernetzten Systemen erfolgen. Die Vernetzung erreicht auf diese Weise die zweite Dimension. Ihre dritte Ebene bilden hybride SAP-Umgebungen ab, die IaaS- und PaaS-Lösungen von SAP einbinden. Mit SAP Ariba, der cloudbasierten Netzwerklösung für Einkäufer und Lieferanten, steht eine Plattform bereit, um den Beschaffungsprozess zu automatisieren – datengesteuert. Ein anderes Beispiel ist SAP Hybris C4C (Hybris Cloud for Customer). Das cloudbasierte CRM-System vereinfacht Vertrieb, Service und Marketing. Das Datenmanagement in einer solchen Hybrid Cloud muss neben Effizienz nun auch End-to-End-Compliance bieten.

Strukturiertes Vorgehen beginnt mit DSGVO-Verständnis

Die mehrdimensionale Vernetzung verleitet Unternehmen dazu, sich allein auf technische Ansätze für einen gesetzeskonformen Datenumgang zu fokussieren. Jedoch liegt hier die Gefahr, vorschnell zu handeln. Nötig ist strukturiertes Vorgehen: Zunächst müssen alle Verantwortlichen im Unternehmen die DSGVO kennen und verstehen – das betrifft nicht nur den CIO, CDO und Datenschutzbeauftragten, sondern auch das Personal in den Abteilungen Legal, Einkauf und HR. Ansonsten wird der nächste Schritt scheitern: das De-

finieren des rechtlichen Rahmens, um abzustecken, wo und wie die DSGVO das eigene Geschäft beeinflusst. Erst danach ist es sinnvoll, sich mit der technischen Realisierung zu beschäftigen. Die beginnt mit der Datenklassifizierung, die transparent macht, wo sensible Informationen in der SAP-Umgebung verarbeitet und gespeichert werden und welche Anwendungen und Nutzer darauf zugreifen.

Klassifizierte Daten schaffen die Basis, Datenverarbeitungsprozesse anzupassen. Anonymisierung, Pseudonymisierung und Verschlüsselung von personenbezogenen Daten stuft der Gesetzgeber als geeignete Schutzmaßnahmen ein. Mit anonymisierten Daten halten Entwickler und Tester den Datenschutz ein. Das Übertragen von Kundendaten und Passwörtern muss stets verschlüsselt erfolgen. Bei Webapplikationen zum Datenteilen und zur Datenübertragung empfiehlt sich der Einsatz von SSL-Zertifikaten für die Verschlüsselung. Diese Sicherheitsmaßnahmen gilt es in ein Gesamtkonzept zu integrieren.

Unterstützung von SAP-Partnern

Das erfolgreiche Verzahnen von Cloud, Geschäft und Recht erfordert ein ganzheitliches Vorgehen, das die dreidimensionale Vernetzung im Blick hat. Unternehmen können sich mit SAP und/oder einem spezialisierten SAP-Partner wie dem Datenmanagementspezialisten NetApp den Weg zur gesetzeskonformen SAP-Landschaft erarbeiten. Dazu dienen beispielsweise Hybrid-Cloud-Readiness-Workshops, in denen Experten gemeinsam mit der SAP-Anwenderfirma die vertikale und horizontale Datenverteilung in deren SAP-System ermitteln. Auch wird beleuchtet, wie sich die Verlagerung von Services in die Cloud auf ein regelgerechtes Datenmanagement auswirkt: von der Datenerfassung über die Verarbeitung bis hin zur Haltung und Archivierung. Wenn das alles klar definiert ist, kann man die Technologien auswählen, um die DSGVO-Vorgaben im Detail umsetzen zu können.

Im SAP-Umfeld lässt sich diese Herausforderung beispielsweise mit dem Data-Fabric-Konzept von NetApp und dem cloudbasierten Speicherbetriebssystem ONTAP realisieren. Ein Anwender des Data-Fabric-Konzepts behält so die volle Kontrolle über seine Applikationen und Daten, egal wohin er sie schnell und einfach verschieben will.

Auf permanenten Prozess einstellen

Erst das Wissen, wie sich die DSGVO auf das eigene Geschäft auswirkt, schafft die Voraussetzung, den Compliance-Rahmen aufbauen und die nötigen technischen Verfahren in einer SAP-Umgebung implementieren zu können. Ein ganzheitlicher Ansatz ist prädestiniert, die Datenverteilung in einer dreidimensional vernetzten SAP-Landschaft verordnungsgemäß aufzusetzen. Methodisch führen Datenermittlung, unstrukturierte Datenanalyse, Analyse der Sicherungsdaten, Cloud-Datenanalyse, strukturierte Datenanalyse, Datenverlauf und Daten-Case-Management zur umfassenden Compliance, die zudem Unternehmen einen permanenten Prozess mit ständigem Überprüfen und Nachjustieren abverlangt. Nachhaltiges Handeln bedeutet für Unternehmen künftig aber auch, hinsichtlich der DSGVO mitzudenken, wenn sie neue Geschäftsfelder erschließen. Die moderne Datenstrategie muss heutzutage in eine Kultur des Datenschutzes im Unternehmen eingebettet sein. Das schafft Vertrauen bei Mitarbeitern und Kunden gleichermaßen und sichert den langfristigen Geschäftserfolg.

NetApp®
Data Driven

NetApp Deutschland GmbH
Sonnenallee 1
85551 Kirchheim bei München
Telefon: +49 89 9005940
info-de@netapp.com
www.netapp.de

SAP-Daten managen.
Perspektiven eröffnen.
www.NetApp.com/SAP

NetApp
Data Driven

Das SAP-Hochleistungsarchiv von KGS ist für alle unter der DSGVO relevanten Schnittstellen in der jeweils neuesten Version zertifiziert

SAP ILM 3.1 und KGS-Archiv – passendes Gespann für die DSGVO

Die DSGVO betrifft mehr Daten als die im SAP HCM verwalteten. Da die HCM-Daten und -Dokumente per definitionem personenbezogen sind, lohnt es sich, zunächst auf das HCM-System zu schauen – ohne aber die anderen Daten (zu Kunden, Interessenten, Lieferanten) aus den Augen zu verlieren. Mit SAP ILM steht bereits heute eine Softwarelösung bereit, die den kommenden Anforderungen gerecht wird – sofern ein ILM-fähiges Archiv- und Speichersystem vorhanden ist.

Winfried Althaus, KGS-Geschäftsführer.

SAP hat ILM ursprünglich entworfen, um Systemstilllegungen zu unterstützen und Retention Management im laufenden Betrieb umzusetzen. Wenn Stilllegungen funktionieren, warum nicht SAP ILM auch im laufenden Betrieb nutzen? Dagegen spricht technisch nichts, nur haben die SAP-Anwender dies in der Vergangenheit kaum praktiziert. Mit der EU-DSGVO eröffnet sich ein veritables Anwendungsfeld. SAP-Bestandskunden steht SAP ILM für Archivierungsobjekte ab Release EA-HR 604 zur Verfügung. Und da SAP ILM ab ERP 6.0 Enhancement Package 4 verfügbar und bereits in der ERP-Lizenz enthalten ist, wächst auch die Anwenderzahl stetig.

Erweiterter Ansatz innerhalb des SAP ILM

SAP ILM ergänzt den SAP-Standard um ein Regelwerk zur Verwaltung des Lebenszyklus produktiver und archivierter Daten und Dokumente. Diese können mit ILM revisionssicher auf einem zertifizierten WebDAV-Server abgelegt werden und sind so vor verfrühtem Löschen geschützt. Der SAP-Anwender kann Löschfristen aus dem ERP-System heraus setzen und den Löschvorgang steuern. Für die Nutzung von SAP ILM ist eine Datenarchivierung zwingende Voraussetzung, da sowohl die Inhalte der SAP-Datenbanken als auch die unstrukturierten Daten in Archiven betroffen sind. Die Objekte müssen aus der SAP-Datenbank herausgelöst und der Archivierung zugeführt werden, damit man sie zum gegebenen Zeitpunkt löschen kann.

Im Zuge der Unterstützung der Anforderungen des DSGVO-Regelwerks hat SAP die ILM-Schnittstelle funktional erweitert. Bewegungsdaten können durch Archivierung und eine entsprechende Zugriffskontrolle gesperrt werden. Ihre Aufbewahrung ist dadurch auch nach Ablauf der Zweckbindung gesichert, wenn das Löschen durch übergeordnete Gesetze nicht gestattet ist. Der Zugriff auf die Daten und ihre Verarbeitung lassen sich über erweiterte Berechtigungen einschränken. Gelöscht

werden sie dann nach Ablauf der gesetzlichen Fristen nach den in SAP ILM hinterlegten Regeln. Der Anwender kann über das Information Lifecycle Management prüfen, ob personenrelevante Daten entsprechend der Zweckbindung und Datensparsamkeit verarbeitet und gespeichert werden. Er kann Aufbewahrungsfristen und Sperrkennzeichen auf abgelegte SAP-Dokumente setzen, um ein späteres automatisches Löschen zu ermöglichen (Legal Hold), sowie User, Rollen und Zugriffsrechte einrichten und administrieren.

Um diese Funktionen zu unterstützen, muss das verwendete Archivsystem zusätzlich zur SAP-ArchiveLink-Schnittstelle die SAP-ILM-WebDAV-Schnittstelle unterstützen. Für mindestens eine der existierenden SAP-Archivschnittstellen sind fast alle Archivsysteme am Markt zertifiziert: Klassisch ArchiveLink ist der Standard, es folgen – schon dünner gesät – SAP ILM, ILM 3.1 und die ILM-Schnittstelle für SAP S/4HANA.

ILM-fähiges Archiv erforderlich

Bei SAP ArchiveLink und SAP ILM handelt es sich um zwei völlig getrennte Schnittstellen: ArchiveLink ist eine http-basierte Schnittstelle, die nur wenige Funktionen wie beispielsweise Anlegen, Ablegen, Zurückholen und Löschen unterstützt. SAP ILM hingegen als WEBDAV-Implementierung erlaubt es darüber hinaus, Eigenschaften von Dateien wie beispielsweise Aufbewahrungszeit, Löschverhinderung etc. zu pflegen.

SAP besteht im ILM-Zertifizierungsverfahren seit Version 3.0 darauf, dass alle Archive, die ILM unterstützen, auch für SAP ArchiveLink zertifiziert sind. Hintergrund: Auch bei der Nutzung von ILM ist ein ArchiveLink-Archiv für die unstrukturierten Dokumente (Originalbelege) nötig. Zu jedem über ArchiveLink verwalteten Objekt wird dann im ILM ein Metadatensatz gehalten, der die Eigenschaften „Aufbewahrungszeit“ und ggf. „Legal Hold“ abbildet. Insofern ergibt sich daraus bei der Nutzung von SAP ILM die Notwendigkeit, ein ILM-fähiges Archiv zu betreiben.

High-Performance-Archiv speziell für die SAP-Archivierung

Mit dem ILM-zertifizierten KGS ContentServer4Storage bietet die KGS ein High-Performance-Archiv, das speziell für die Bedürfnisse der SAP-Archivierung entwickelt wurde und höchste Performanceanforderungen erfüllt. Die schlanke Archivlösung ist für alle unter der DSGVO relevanten SAP-Archivschnittstellen in der jeweils neuesten Version zertifiziert (Archive-Link und ILM für ECC 6.0 und S/4HANA) und ermöglicht eine rechtssichere Dokumentenarchivierung, Datenarchivierung und Archivierung von Drucklisten. Die nahtlose Integration in den SAP-Standard macht aufwändige Rollouts von Client-Komponenten überflüssig. Um ein Dokument anzuzeigen, muss der Nutzer seine gewohnte Anwendungsumgebung nicht verlassen, sondern verwendet den vorhandenen SAP-Dokumentenviewer oder alternativ den KGS H5 Viewer, der serverbasiert eingesetzt werden kann.

Neben der tiefen Integration in die SAP-Landschaft stellt der KGS ContentServer4Storage als SAP-Archiv und -Dokumentenmanagementsystem auch eine vollständige Integration zu den unterschiedlichen, in den Unternehmen bereits befindlichen Speicher- und HSM-Lösungen her und ist auf einer Vielzahl von Betriebssystemen lauffähig. Unternehmen können damit ihre vorhandene Server- und Storage-Infrastruktur nutzen und sparen sich zusätzliche Investitionen für die Dokumenten- bzw. Daten-Archivierung.

Der KGS ContentServer4Storage wird immer als Unternehmenslizenz (Corporate License) lizenziert und es entstehen somit keine weiteren Folgekosten für zusätzliche User. Damit ist auch die betriebswirtschaftliche Planungssicherheit gewährleistet. In Kombination mit weiteren KGS-Komponenten bildet das Archiv die Basis für ein leistungsfähiges, modernes und SAP-nahes Enterprise Content Management System (ECM-System)/Dokumenten Management System (DMS). Im Einsatz ist es bei namhaften Unternehmen wie Döhler, Borsig, Loewe, RheinChemie oder der EnBW. Für deren Administratoren bedeutet die KGS-Lösung mit ihrer reduzierten Komplexität eine Zeitersparnis in ihrer täglichen Arbeit von bis zu 50 Prozent.

Fazit

SAP ILM in der neuesten Ausprägung bietet eine gute technische Basis, um den aus der DSGVO erwachsenen Ansprüchen zu genügen. Bestimmte Anforderungen, wie z. B. die Forderung nach Datenminimierung im Produktivsystem, die eingeschränkten Zugriffe auf personenbezogene Daten und die besonderen Forderungen im Zusammenspiel von Löschung und Aufbewahrungsfristen machen es notwendig, ein ILM-fähiges Archiv- und Speichersystem einzusetzen. Der KGS ContentServer4Storage ist als SAP-Archiv für die neuesten Versionen aller vier für die Umsetzung der DSGVO relevanten Archivschnittstellen zertifiziert: BC ILM 3.1, BC-AL 7.40, S/4-BC ILM 1.0 und S/4-BC-AL 7.40.

KGS
Document Integration for SAP®

KGS Software GmbH & Co. KG

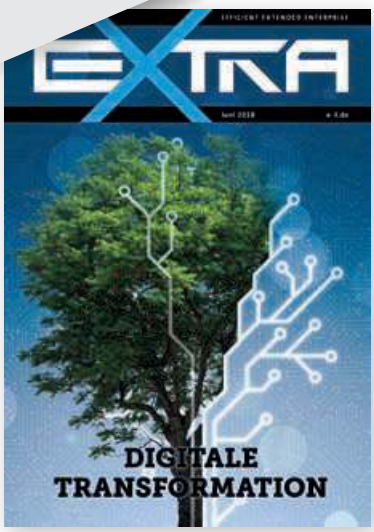
Dornhofstraße 38 A
63263 Neu-Isenburg
Telefon: +49 6102 8128522
info@kgs-software.com
www.kgs-software.com

EXTRA VORSCHAU

Juni 2018:
Digitale Transformation

Digitalisierung verändert alle Lebensbereiche und ist längst vom Hype-Thema zu einer der wichtigsten Zukunftsfragen im Wirtschaftsleben geworden. SAP sieht in S/4 einen wesentlichen Bestandteil der Transformation. Lesen Sie, wie Digitalisierungsprojekte zum Erfolg werden.

Druckunterlagenschluss:
14. Mai 2018



September 2018:
Künstliche Intelligenz

Jeder redet über künstliche Intelligenz. Doch die konkreten Angebote sind noch eher rar und unkonkret. Die Community braucht Klarheit darüber, wie sie mit KI und Machine Learning die nächste Stufe der Automatisierung erreichen kann. In diesem E-3 Extra erfahren Sie, wie Sie KI gewinnbringend für Ihr Unternehmen einsetzen.

Druckunterlagenschluss:
13. August 2018

November 2018:
Add-ons

Customize me! Agilität setzt Anpassungsfähigkeit voraus: Mit den Add-ons zum SAP-ERP-System wird es möglich. Früher waren es Abap-Add-ons, heute kommen Add-ons auch aus der Cloud. Ihr Unternehmen kann dies bieten? Know-how von Experten aus erster Hand finden Sie in diesem E-3 Extra.

Druckunterlagenschluss:
15. Oktober 2018

2018

Alles, was die SAP-Community wissen muss,
finden Sie monatlich im E-3 Magazin.

Ihr Wissensvorsprung im Web, auf iOS und Android
sowie PDF und Print: **e-3.de/abo**

www.e-3.de

SAP® ist eine eingetragene Marke der SAP AG in Deutschland und in den anderen Ländern weltweit.