Softwareunterstützung für den **Datenschutz** – gewappnet für die DSGVO

Von Olaf Pulwey und Stephan Schollmeyer

Ob der deutsche Gesetzgeber es schafft, das Datenschutzanpassungs- und -umsetzungsgesetz, mit dem die europäische Datenschutzgrundverordnung (DSGVO) in nationales Recht umgesetzt werden soll, rechtzeitig zu verabschieden, scheint aktuell alles andere als gewiss. Dennoch raten die Autoren Kreditinstituten, sich rechtzeitig mit den zu erwartenden Änderungen vertraut zu machen und zu entscheiden, ob sie die Anpassungen in Eigenregie mir ihrem Rechenzentrum umsetzen oder auf eine externe Softwarelösung setzen wollen. Wichtig dabei sind vor allem Rechts- und Zukunftssicherheit. Red.

Jedes deutsche Unternehmen ist gemäß Bundesdatenschutzgesetz (BDSG) zum Datenschutz verpflichtet – auch die Kreditwirtschaft. Die EU-Richtlinien (EU-DSGV) gehen bezüglich der Auflagen noch einen Schritt weiter und würden greifen, wenn sich die Bundesregierung auf keinen nationalen Standard einigen könnte. Dem Kabinettsentwurf zum Datenschutzanpassungs-Umsetzungsgesetz (DSAnpUG-EU) fehlen zwar nur noch die Zustimmung von Bundesrat und Bundestag, doch erste kritische Stimmen am Gesetzesentwurf lassen an einem rechtzeitigen Beschluss zweifeln. Gelingen muss es dennoch, da die Zeit drängt: Liegt bis zum 25. Mai 2018 national keine finale Regelung vor, wird die EU-DSGV automatisch zur Grundlage – mit allen erdenklichen Konsequenzen.

Datenschutzbeauftragte unter Zugzwang

Unter anderem ist es genau diese Perspektive, die Datenschutzbeauftragte zunehmend unter Druck setzt. Denn die Anpassung und Einhaltung von Dokumentationspflichten oder der eigenen Compliance-Maßnahmen sind in jedem Falle aufwendig und kosten Zeit. Abhilfe können Softwarelösungen wie ein elektronisches Datenschutzmanagement schaffen, das bei der täglichen Arbeit maßgeblich unterstützt.

Neben den bekannten Regelungen schafft das Bundesdatenschutzgesetz einige neue Rahmenbedingungen. Einen besonderen Aspekt nimmt beispielsweise die Anpassung der Regelungen des Datenschutzbeauftragten nach § 38 ein. Nach den bisherigen Entwürfen übernimmt dieser eine reine Überwachungsfunktion für die durchzuführenden Aufgaben – insbesondere auch hinsichtlich der Begleitung und Unterstützung der Datenschutz-Folgenabschätzung – eine weitere Neuigkeit mit besonderem Stellenwert.

Zu den Autoren

Olaf Pulwey, Vorstand, FOCONIS AG, Köln, **Stephan Schollmeyer**, externer Datenschutzbeauftragter für Kreditinstitute, genoBIT GmbH, Oldenburg

Auch der Umsetzungsleitfaden zur Bewältigung der neuen Anforderungen, welche sich aus den Artikeln der EU-Vorgabe ergeben, ist ein zentraler Bestandteil des Gesetzentwurfs. Nicht zuletzt stellt die Vorlage beziehungsweise Dokumentation für die Aufsichtsbehörden einen wesentlichen Punkt des Bundesdatenschutzgesetzes dar. Ein Blick in all diese Ausführungen verdeutlicht, dass Datenschutzbeauftragte auch hier im Zugzwang sind und im Vergleich zur letzten Aktualisierung des BDSG vor allem in Bezug auf die Anforderungen zur Vollständigkeit und Nachvollziehbarkeit große Veränderungen vollziehen müssen.

Der Aufwand steigt

Finanzinstitute sind angesichts der bevorstehenden Neuerungen gefordert, bestehende Regelungen zu überarbeiten und Prozesse neu zu implementieren. Auch die Handlungsbefugnisse der Verantwortlichen bedürfen in diesem Zusammenhang einer Überprüfung und Angleichung gemäß den gesetzlichen Regelungen.

Keinesfalls verwunderlich ist, dass die Umsetzung der im Gesetzentwurf festge-

legten Neuregelungen entsprechend dem DSAnpUG-EU [1)] zunächst zu höherem Aufwand und damit auch zu höheren finanziellen Belastungen führen kann. So sind nach Schätzungen für die Erfüllung der Informationspflichten durch die Unternehmen einmalige Summen in Höhe von rund 58,9 Millionen Euro und eine jährlich wiederkehrende Belastung von rund 17,2 Millionen Euro notwendig.

Vor dem Hintergrund der wirtschaftlichen Gesamtsituation, wie beispielsweise niedriger Zinsmargen, stellt die Bereitstellung dieser Mittel für viele Banken und Sparkassen eine große Herausforderung dar und fordert zwangsläufig Sparmaßnahmen in anderen Bereichen. Eine Wahl haben sie allerdings nicht: Denn die hohen Bußgeldvorschriften nach dem EU-Entwurf wurden durch mögliche Strafverfahren erweitert. Der Business Case, die neuen Regelungen auszusitzen und sich mit der Umsetzung der geforderten Maßnahmen Zeit zu lassen, ist also denkbar instabil.

EDV zu Fuß oder digitalisiert?

Dass sie also etwas tun müssen, haben die meisten Kreditinstitute längst erkannt. Die Frage lautet aktuell also längst nicht mehr „Ob?" oder „Wann?", sondern eher „Wie?". Grundsätzlich haben Banken und Sparkassen die altbekannten Optionen: Einerseits können sie die Herausforderung auf eigene Faust intern und maximal mit der Hilfe ihres ausgewählten Rechenzentrums lösen. Andererseits haben sie die Chance, sich der Kompetenzen und Softwarelösungen externer Partner zu bedienen.

Während Ersteres mitunter mit vielen manuellen, papierhaften Tätigkeiten verbunden ist, punktet die Softwarevariante idealerweise mit einer standardisierten, rechtssicheren Umsetzung, schnellen, automatisierten Prozessen und Konformität im Ergebnis, weil Drittanbieter, dem Wettbewerb verpflichtet, den Anspruch verfolgen, in ihrem Themenfeld hinsichtlich Qualität und Beratungsstärke die Nase vorn zu haben.

Auch im Bereich „Softwarelösungen für den Datenschutz" werden Anwendungen entwickelt, die idealerweise so konzipiert sind, dass sie heute, vor allem jedoch morgen Bestand haben. Die Foconis AG etwa hat mit eDSMS bereits im Frühjahr 2016 eine Standardsoftware veröffentlicht, die zum Wohlgefallen geplagter Datenschutzbeauftragter auch die zukünftigen gesetzlichen Ansprüche rechtssicher abbilden wird.

Auch andere Hersteller haben es sich längst zur Aufgabe gemacht, die Rechtsprechung in puncto Datenschutz in revisionssichere Lösungen zu gießen. Entscheiden sich also die Institute für das Buy und gegen das Make, haben sie die Qual der Wahl, welche der marktgängigen Lösungen sie im eigenen Hause ausrollen wollen. Dabei sind jedoch Argusaugen gefragt, denn längst erfüllen nicht alle Lösungen die notwendigen Standards und die beruhigende Zukunftssicherheit, auf die sich die Kreditwirtschaft dringend verlassen können muss.

Anforderungen an ein elektronisches Datenschutz-Management-System

Angesichts des Ausmaßes und des zeitlichen Umsetzungsdrucks der bevorstehenden Änderungen ist vielen Verantwortlichen längst bewusst, dass dies nur mit der Hilfe einer elektronisch gestützten Lösung möglich ist. Folgende Anforderungen sollten die Institute darum an ein professionelles System mindestens stellen:

- Vorgefertigte, fachlich korrekte Formularfelder zur schnellen Erfassung, fortlaufenden Dokumentation und Überprüfung der jährlichen und unterjährigen Tätigkeiten und Maßnahmen;
- Zuordnung der Maßnahmen und Tätigkeiten zu verschiedenen Perioden (Jahreszahlen) zwecks Auswertung und optimaler Unterstützung beim jährlich vorgeschriebenen Berichtswesen;
- fachlicher Content-Updateservice mit Inhaltsvergleich-Optionen zur schnellen Erfassung von Veränderungen innerhalb der notwendigen Wissensbereiche;
- Optionen zur Bestimmung von Wiedervorlagen/Prüfdaten;
- Kompetenzschutz: schnell und sicher zu administrierende Zugriffs-, Lese- und Schreibberechtigungseinstellungen;
- Kenntnisnahmefunktion und Erinnerung an die Kenntnisnahme sensibler oder wichtiger Informationen inklusive dokumentierter, ausstehender Kenntnisnahmen;
- vorgefertigte, erweiterbare und individuell erstellbare Verfahrensverzeichnisse;
- Möglichkeit zur Prüfung und Dokumentation der Aktivitäten von Auftragsdatenverarbeitern;
- Archivfunktion zur Berücksichtigung individuell festgelegter oder gesetzlich vorgeschriebener Fristen;
- Erleichterung bei der Erstellung des jährlichen Berichtswesens durch Zuordnung der entsprechenden Tätigkeiten und Maßnahmen zum jeweiligen Jahr (periodische Kategorisierung).

Wie für die meisten Softwareanwendungen, sollte auch bei der Auswahl einer Lösung für den Datenschutz ein besonderes Augenmerk auf einer breiten Funktionspalette, eine intuitive Bedienbarkeit, eine gute Prozessunterstützung und eine starke Verlässlichkeit des Partners liegen. Auch die Tatsache, ob der Datenschutzbeauftragte extern bestellt oder intern berufen ist, darf im System keine Rolle spielen und sollte als Option unterstützt werden. Der Fokus muss auf der vereinfachten Darstellung derzeitiger und zukünftiger Auflagen in Prozessen und Aufgabenstellungen lie-

gen, die zudem einem logischen Ablauf folgen. Nicht zuletzt sollte die Lösung mithilfe tiefgreifender Kenntnisse erfahrener Experten zukunftssicher weiterentwickelt werden – auch hinsichtlich der Standardisierung gegenwärtiger und zukünftiger komplexer Datenschutzprozesse.

Während Datenschutzbeauftragte zuvor ein nicht selten komplexes Ordnersystem, individuelle Archivsortierungen und Sammlungen mit Fachinformationen pflegten, ermöglicht eine durchdachte Software neben der Implementierung eines praktischen Standards die Digitalisierung der gesamten Dokumentation umgesetzter Pflichten aus dem Datenschutz.

Ob von Mitarbeitern im Rahmen der Thematik gegenzuzeichnende Vereinbarungen oder die Dokumentation regelmäßiger Tätigkeiten des Datenschutzbeauftragten: Ein elektronisches Datenschutz-Management-System bietet den Zuständigen eine Möglichkeit, das alljährliche Compliance-Berichtswesen durch Kategorisierung in Perioden (Jahre) und schlussendlich gefilterte Anzeigen der Einträge erheblich zu beschleunigen.

Zudem sollten Banken und Sparkassen darauf achten, dass darüber hinaus dem jeweiligen Kernbanksystem entsprechende, vorgefertigte Verfahrensverzeichnisse vorliegen, die auch die Möglichkeit bieten, individuelle Verfahren hinzuzufügen. Und: Gut beraten ist jene Bank und Sparkasse, die sich im Rahmen der Softwarewartung auf automatisierte Softwareupdates und Content-Updates bei gesetzlichen Veränderungen in den Bestimmungen verlassen kann.

In Sachen Datenschutz sind in Zukunft deutliche Veränderungen zu erwarten, deren Umsetzung erheblicher Anstrengungen bedarf. Gut beraten ist jene Bank oder Sparkasse, die sich frühestmöglich nach geeigneter Software umschaut und bei der Produktwahl die für sich streng definierten Mindestanforderungen ansetzt. Damit das gelingt, muss jedoch die rechtzeitige Auseinandersetzung mit der aktuellen Gesetzeslage und den bevorstehenden Änderungen – insbesondere auch mit den drohenden Konsequenzen bei Nichteinhaltung – eine Selbstverständlichkeit sein. Nur wer die Thematik sach- und fachgerecht anpackt sowie die richtigen Partner im Boot hat, ist auf der sicheren Seite.

Fußnote

1) Quelle: Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EZU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) Seite 74

Sicherheit

Cyberkriminelle hacken vermehrt unstrukturierte Daten

2016 war ein alarmierendes Jahr mit massiven Hackerangriffen und Datenverletzungen. Um rekordverdächtige 566 Prozent stieg die Zahl der gestohlenen Datensätze weltweit an: von 600 Millionen auf über vier Milliarden. Das geht aus dem „IBM X-Force Threat Intelligence Index 2017" hervor, der IT-Sicherheitsdaten von rund 8000 IBM Kunden in mehr als 100 Ländern und Daten aus anderen Quellen wie Spam-Sensoren und Honeypots/-netzen analysiert.

Besonders Finanzinstitutionen sind dem Report zufolge im Visier der Cyberkriminellen. Die Finanzbranche führte 2016 die Liste der am stärksten von Vorfällen betroffenen Branchen an, nachdem sie im Vorjahr nur den dritten Rang belegt hatte. Neben personenbezogenen Angriffszielen wie Kreditkarteninformationen wurden 2016 auch vermehrt unstrukturierte Daten gehackt. E-Mail-Archive, Geschäftsdokumente, gestohlenes geistiges Eigentum oder Quellcodes eröffnen Kriminellen neue Möglichkeiten, etwa für den Insiderhandel, und setzen die Unternehmen weiter unter Druck.

Investitionen in die Cybersicherheit führten jedoch dazu, dass der Finanzsektor trotz der hohen Anzahl an Angriffen letztlich nur der am drittstärksten betroffene Bereich war, was die Zahl der kompromittierten Datensätze angeht. Am schlimmsten von Sicherheitsvorfällen und Datenpannen betroffen sind die Informations- und Kommunikationsbranche (IKT) und der öffentliche Sektor. Mit Blick auf die Finanzbranche bedenklich scheint jedoch der hohe Anteil versehentlicher Vorfälle, die von Akteuren innerhalb der jeweiligen Organisation verursacht werden: Sie machten in der Finanzbranche laut X-Force im vergangenen Jahr 53 Prozent der Angriffsquellen aus.

Ein besonders lohnendes Geschäft für kriminelle Hacker waren 2016 Erpressertrojaner, auch „Ransomware" genannt. Dabei verschlüsseln infizierte Anhänge in Spam-Mails Daten auf Servern von Unternehmen und Privatpersonen. Erst nach hohen Lösegeldzahlungen werden die Daten wieder entsperrt. Kriminelle Hacker erbeuteten alleine im ersten Quartal des vergangenen Jahres damit 209 Millionen US-Dollar. Durch die Bereitschaft von Unternehmen, Lösegeldforderungen Folge zu leisten, wächst die Beliebtheit von Ransomware weiter. Rund 70 Prozent aller betroffenen Unternehmen bezahlten IBM zufolge jeweils über 10000 US-Dollar an Lösegeld, um wieder Zugang zu ihren Geschäftsdaten und -systemen zu bekommen. IBM Security identifizierte daraus auch einen 400-prozentigen Anstieg von Spam-Mails als häufiger Träger von Malware. 44 Prozent der beobachteten Spam-Mails waren mit den Erpressertrojanern infiziert. Ransomware machte bis zu 85 Prozent dieser bösartigen Dateianhänge aus. **Red.**