Die **DSGVO** bietet Banken auch **Chancen**

Von Rüdiger Giebichenstein und Holger Junghanns

Quelle: pixabay

Die Datenschutz-Grundverordnung wird in mancher Hinsicht eine Anpassung bisheriger Geschäftsprozesse und eine effizientere Zusammenarbeit zwischen den beteiligten Funktionen erfordern, wissen die Autoren. Sowohl auf der Ertrags- als auch auf der Kostenseite sehen sie aber auch Chancen. Wichtig dabei ist es, die Einverständniserklärung des Kunden zum richtigen Zeitpunkt einzuholen und sie mit Mehrwerten zu verknüpfen. So lässt sich die Kundenansprache verbessern und zugleich ein Teil der Datenpflege auf den Kunden übertragen werden. Red.

In einer Zeit, in der die Einsatzgebiete der Informationstechnologie immer vielfältiger werden, ist es für Unternehmen zwingend erforderlich, sich mit den aktuellen rechtlichen und organisatorischen Anforderungen zu befassen.

Gerade vor dem Hintergrund der umfangreichen Herausforderungen der Digitalisierung (Big Data, Cloud Computing, Industrie 4.0, künstliche Intelligenz) und der damit einhergehenden, immer größer werdenden Mengen an personenbezogenen Daten ist speziell den Anforderungen des Datenschutzrechts ein besonderer Stellenwert einzuräumen. Es gilt, diese Anforderungen aktiv anzunehmen.

Hieraus ergeben sich auch für den Bankensektor neue Herausforderungen, wie zum Beispiel eine deutlich höhere Kundeninteraktion im Online-Bereich (zum Beispiel Self-Service-Portale, Apps). Insbesondere werden durch die erhöhten Interaktionen individuelle und maßgeschneiderte persönliche Umgebungen dem Kunden in einem agilen Umfeld zur Verfügung gestellt.

Banken müssen nun in jedem Schritt des Verfahrens sicherstellen, dass die erhöhten datenschutzrechtlichen Anforderungen erfüllt sind. Dies erfordert eine ganzheitliche Ende-zu-Ende-Betrachtung der relevanten Prozesse und somit eine deutlich effizientere Zusammenarbeit zwischen den verschiedenen beteiligten Funktionen, wie zum Beispiel dem Kundenservice und dem Backoffice.

Ziel muss es sein, intuitive digitale Services für die Bankkunden bereit zu stellen und gleichzeitig die erforderliche Transparenz und Rechtssicherheit zu gewährleisten. Der Datenschutz hat somit einen nicht zu unterschätzenden Einfluss auf die zukünftigen und sich im Rahmen der Digitalisierung verändernden Geschäftsmodelle im Bankengeschäft.

Zu den Autoren

Rüdiger Giebichenstein, Köln, und **Holger Junghanns,** Frankfurt am Main, beide Partner, PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft

Datenschutz neu definiert

Die am 25. Mai 2018 in Kraft getretene europäische Datenschutz-Grundverordnung (EU-DSGVO) bringt weitreichende Veränderungen mit sich und hat Auswirkungen auf die gesamte Organisation der Unternehmen (unter anderem auf die Geschäftsmodelle, die Dienstleistungs- und Produktgestaltung, die Aufbau- und Ablauforganisation, die IT-Systeme, die Vertragsgestaltung und auch die Mitarbeiter). Zusätzlich zum europäischen Recht bildet das Bundesdatenschutzgesetz (BDSG) aus deutscher Sicht eine weitere wesentliche gesetzliche Grundlage.

Neben diversen, teilweise komplexen Einzelanforderungen kommt insbesondere der Dokumentation als Grundlage der Rechenschaftspflicht eine besondere Bedeutung zu. Unternehmen müssen gemäß Art. 5 Abs. 2, Abs. 1 DSGVO i.V.m. Art. 24 Abs. 1, 30 Abs. 1, 32 Abs. 1 DSGVO die Angemessenheit und Wirksamkeit der ergriffenen technischen und organisatorischen Maßnahmen zum Datenschutz sowie die Einhaltung der Grundsätze der DSGVO für sich und gegebenenfalls ihre Dienstleister nachweisen können. Darüber hinaus wurde der Bußgeldrahmen im Fall eines Verstoßes gegen die datenschutz-

rechtlichen Anforderungen (bis zu 20 Millionen Euro oder 4 Prozent des weltweit erzielten Jahresumsatzes gemäß Art. 83 Abs. 2, Abs. 5, Abs. 6 DSGVO) deutlich erhöht.

Geschäftsorganisation anpassen

Zur Bewältigung dieser Aufgabe und als Grundlage der Rechenschaftspflicht ist eine wirkungsvolle Methodik zur systematischen Planung, Organisation, Steuerung und Kontrolle des Datenschutzes in der Unternehmenslandschaft zu verankern. Aus diesem Anlass empfiehlt sich der Aufbau eines Datenschutz-Management-Systems (DSMS), dessen Implementierung auch dazu beiträgt, die Datenschutzorganisation der Unternehmen aus ihrer reagierenden Haltung zu locken und zu einem aktiven, das Geschäft unterstützenden, Sparringspartner zu entwickeln.

Obwohl die aufsichtsrechtlichen Anforderungen in den unterschiedlichen Branchen (zum Beispiel die MaRisk und BAIT für die Finanzindustrie oder das IT-Sicherheitsgesetz) bereits ein hohes Schutzniveau fordern, sind die Auswirkungen der DSGVO individuell für jedes Unternehmen zu beurteilen und bedürfen in den meisten Fällen einer Anpassung der bisherigen Geschäftsorganisation.

Datenschutz-Management-System – das Herz der DSGVO-Implementierung

Da typischerweise Unternehmen Erfahrungen beim Betreiben eines Managementsystems haben und es weder einen etablierten Standard zum Aufbau und Betrieb eines DSMS gibt, noch die DSGVO operative sowie explizite Anforderungen an die Ausgestaltung eines DSMS beschreibt, sollte der Datenschutz analog nach IDW PS 980 ausgerichtet werden, um Synergien und Schnittstellen nutzen zu können.

Des Weiteren hat sich in der Praxis eine Verzahnung mit dem Informationssicherheits-Management-System (ISMS gemäß dem ISO-Standard 27001) und dem Business-Continuity-Management-System (BCMS gemäß dem ISO Standard ISO 22301) als zielführend herausgestellt. Für die Ausgestaltung eines integrierten Datenschutz-Management-Systems schlagen wir in Anlehnung an den IDW PS 980 folgendes Zielbild vor:

- **Datenschutzkultur und -strategie (Werte/Ziele)** gemäß IDW PS 980 „Compliance-Kultur" und „Compliance-Ziele". Die Datenschutzkultur und -strategie wird durch die Grundeinstellungen und Verhaltensweisen des Managements sowie die Rolle des Aufsichtsorgans („tone at the top") geformt. Sie stellt das Grundfundament für das Datenschutzmanagement dar, verkörpert die Kultur im Unternehmen und prägt die eigenen Mitarbeiter. Die Ziele des eingerichteten Datenschutz-Management-Systems sind von der Geschäftsleitung zu definieren und bilden die Basis für die Bewertung der Risiken eines Datenschutzverstoßes.

- **Datenschutz-Risikomanagement** nach IDW PS 980 „Compliance-Risiken". Im Rahmen des Datenschutz-Risikomanagements sind die Risiken aus möglichen Datenschutzverstößen (nach DSGVO insbesondere die Risiken aus Sicht des Betroffenen) durch ein geregeltes Verfahren zu erheben, zu bewerten und zu berichten. Es obliegt der Geschäftsleitung, eine Risikoanalyse durchzuführen.

- **Maßnahmen zur Einhaltung des Datenschutzes (Datenschutz-IKS)** nach IDW PS 980 „Compliance-Programm". Auf der Grundlage der Beurteilung der Datenschutzrisiken sind zugehörige Maßnahmen (zum Beispiel Kontrollen) einzuführen, die auf die Mitigation der identifizierten Risiken und auf die Vermeidung von Datenschutzverstößen ausgerichtet sind oder als Handlung bei Datenschutzverstößen (zum Beispiel Prozesse zur Reaktion oder Eskalation sowie Berichtswesen) dienen. Das eingeführte IKS beziehungsweise Programm ist zu dokumentieren und bildet den Grundstein für den erforderlichen Nachweis der Angemessenheit und Wirksamkeit der im Sinne von Art. 24 Abs. 1 S. 1 DSGVO durch den Verantwortlichen ergriffenen Schutzmaßnahmen.

- **Umsetzung der Maßnahmen in einer zentralen und dezentralen Datenschutzorganisation** nach IDW PS 980 „Compliance-Organisation". Die Datenschutzorganisation (Aufbau- und Ablauforganisation) ist als integraler Bestandteil in die bestehende Unternehmensorganisation einzubinden und mit dieser zu verzahnen, um die Effizienz und Wirksamkeit des Datenschutz-Management-Systems zu erhöhen. Es ist eine schriftlich fixierte Ordnung (Dokumentenpyramide) für den Datenschutz aufzusetzen, über den Grad der Zentralisierung der Datenschutzorganisation zu entscheiden sowie die Rollen und Verantwortlichkeiten (Rollenmodell) festzulegen.

- **Fortlaufende Kommunikation und Sensibilisierung aller Beteiligter (zentral/dezentral)** nach IDW PS 980 „Compliance-Kommunikation". Die Grundprinzipien und Maßnahmen des Datenschutz-Management-Systems sind adressatenorientiert zu kommunizieren (zum Beispiel über ein Kommunikations- und Schulungskonzept), um Transparenz über die Datenschutzorganisation sowie den Schutz von personenbezogenen Daten herzustellen. Die Kommunikation und Sensibilisierung hat maßgeblichen Einfluss auf die Wirksamkeit der Umsetzung und die gelebte Praxis im Arbeitsalltag.

- **Regelmäßige Überwachung und Verbesserung des DSMS** nach IDW PS 980 „Compliance-Überwachung und Verbesserung". Die Angemessenheit und Wirksamkeit des eingerichteten Datenschutz-Management-Systems ist auf veränderte Anforderungen oder Risiken zu überwachen und regelmäßig auf Verbesserungen zu überprüfen, um den Reifegrad kontinuierlich zu erhöhen (zum Beispiel durch Verankerung im Managementprozess oder unabhängige Überprüfung durch Revision oder Dritte).

Wir empfehlen, dem Datenschutzmanagement das in der Praxis im Rahmen anderer Managementsysteme etablierte Verfahren nach dem PDCA-Zyklus zugrunde zu legen, um die Aktualität und Wirksamkeit der Datenschutzmaßnahmen regelmäßig zu überprüfen. Außerdem ist dieses Verfahren besonders vor dem Hintergrund zukünftig neuer gesetzlicher Anforderungen sinnvoll, da diese über den Zyklus mit abgebildet werden würden. Das Verfahren ist dabei auf alle zuvor benannten Kernelemente anzuwenden.

Inhalt und Aufbau eines Informationssicherheits-Management-Systems

Ähnlich wie das beschriebene Datenschutz-Management-System stellt das Informationssicherheits-Management-System (ISMS) nach ISO/IEC 27001 einen Managementansatz dar. Während das DSMS dem Schutz personenbezogener beziehungsweise personenbeziehbarer Daten gewidmet ist, verfolgt das ISMS die Zielsetzung, insbesondere die Vertraulichkeit, Verfügbarkeit und die Integrität aller Arten von (geschäftskritischen) Informationen zu schützen. Dies bedeutet, dass personenbezogene Daten, neben weiteren geschäftskritischen Daten, eine Teilmenge der schutzbedürftigen Daten innerhalb eines ISMS darstellen.

Auch personenbezogene Daten treten im ISMS-Kontext folglich nur als eines von vielen Information Assets in Erscheinung. Dies weist bereits auf die thematischen Schnittmengen und praktischen Schnittstellen mit dem Datenschutz hin.

Genau wie im DSMS werden im ISMS Richtlinien beziehungsweise Kontrollen zur Adressierung konkreter Risiken definiert, Rollen und Prozesse zur Steuerung und Überwachung der Einhaltung der Anforderungen definiert (Aufbau- und Ablauforganisation) und ein kontinuierlicher Verbesserungsprozess gelebt. Weiterhin sind im ISMS Awareness-Maßnahmen und Metriken zur Messung der Leistungsfähigkeit des Managementsystems zu implementieren.

Datenschutzfolgeabschätzung bei risikoreichen Verarbeitungsprozessen

Eine beispielhafte operative Schnittstelle bildet die Datenschutzfolgenabschätzung (DSFA) nach Art. 35 DSGVO, die als neue Anforderung aufgenommen wurde, und das Informationssicherheits-Risikomanagement nach Kap. 6 der ISO/IEC 27001. Die DSFA muss bei besonders risikoreichen Verarbeitungsprozessen durchgeführt werden. Risikoreich sind unter anderem Prozesse, die sensible Daten verarbeiten oder wenn die Verarbeitung eine neue Technologie, wie etwa Cloud-Lösungen, nutzt.

Weitere risikoreiche Prozesse lassen sich aus einer Risikokarte ablesen, welche in der Regel einen Ergebnistyp des Sicherheitsrisikomanagementprozesses im Rahmen des ISMS darstellt. In der Risikolandkarte werden mögliche Risiken erhoben und gemäß ihren Eintrittswahrscheinlichkeiten und Schadenspotentialen bewertet. Da in dieser Risikolandkarte nicht nur Risiken rund um die Verarbeitung personenbezogener Daten, sondern alle geschäftsrelevanten Informationen bewertet werden, sollten Unternehmen bei der Umsetzung der DSGVO die aus Sicht des Datenschutzes relevanten Risiken konkret als solche kennzeichnen. Dies hat später den Vorteil, dass die Datenschutzorganisation sich auf die für sie relevanten Risiken, zum Beispiel im Rahmen eines Berichtes zur Datenschutzsituation, fokussieren und auf Veränderungen rasch reagieren kann.

Ein weiterer Schnittpunkt ist die Risikobehandlung. Die bereits dokumentierten Behandlungspläne können in die DSFA übernommen werden beziehungsweise die in der DSFA identifizierten Maßnahmen können in den Behandlungsplan übernommen und Maßnahmen um gegebenenfalls konkrete Datenschutzanforderungen ergänzt werden. Ein weiterer, leicht zu realisierender Ansatz ist es, im Rahmen des

ISMS datenschutzrelevante Information Assets entsprechend zu kennzeichnen, um datenschutzspezifische Blickwinkel zu ermöglichen inklusive Sichtweisen auf die Risiken beziehungsweise Schutzbedürfnisse und Schutzniveaus. Hinweise zur konkreten Integration der Datenschutzaspekte für eine Datenschutzfolgenabschätzung in einen Sicherheitsrisikomanagementansatz liefert u. a. die Ende 2017 erschienene ISO/IEC 29134.

Strategic EU-DSGVO – besseres Kundenwissen trotz DSGVO

Neben den Risiken, die mit der Verarbeitung personenbezogener Daten einhergehen, gibt es auch zahlreiche Chancen für Finanzinstitute, die aus einer „intelligenten" Umsetzung der DSGVO erwachsen können. Die Chancen sind sowohl auf der Ertrags- als auch auf der Kostenseite zu finden.

Auf der Ertragsseite spielt das künftige Wissen über den Kunden eine zentrale Rolle. Nur mit erweiterter Kenntnis über den Kunden können Angebote und Kommunikationsinhalte auf dessen Bedürfnisse zugeschnitten werden. Zwei wesentliche Hebel sind hier anwendbar: Opt-in und Mehrwertservices.

Opt-in vom Kunden her gedacht

Beim Einholen des Einverständnisses des Kunden zur Datenverarbeitung (Opt-in) machen viele Finanzdienstleister auch nach der Umsetzung der DSGVO fundamentale Fehler. Sie vergessen zum einen, einen relevanten Mehrwert für den Kunden herauszustellen und zum anderen, dass die Einverständniseinholung aus Kundesicht oftmals eine komplexe und unbeliebte Entscheidung ist. Folgende Regeln sollten beachtet werden:

1. Mehrwerte für den Kunden klar und deutlich formulieren: Entscheider und Projektverantwortliche sollten sich bei Opt-in-Prozeduren die Frage stellen, ob sie persönlich den „Haken" für eine Zustimmung zur Datenverarbeitung setzen würden. Eine „individuelle werbliche Ansprache" als vielerorts verwendeter Ausdruck auf Opt-in-Formularen reicht als Kundennutzen eben nicht aus – welcher Kunden will denn noch mehr Werbung erhalten? Finanzdienstleister sollten auf Basis wirklicher Kundenmehrwerte (zum Beispiel bessere Anlagealternativen, Transparenz über Marktentwicklungen, mögliche Lebensrisiken) entsprechend verständliche Argumente formulieren.

2. Schritt für Schritt und zur richtigen Zeit: Erfahrungsgemäß zögern Kunden bei der Abgabe einer generellen Einwilligung zur Datenverarbeitung zu Beginn einer Kundenbeziehung. Der geforderte Umfang an freizugebenden Informationen überfordert viele Kunden, da diese „gefühlt" zu viele Informationen von sich preisgeben. Finanzdienstleister sollten die Einwilligung des Kunden daher als Prozess im Zuge des Aufbaus einer vertrauensvollen Kundenbeziehung verstehen und „Schritt für Schritt" die notwendigen Opt-ins vom Kunden einholen. Dabei ist entscheidend, den richtigen Zeitpunkt für das Opt-in zu treffen. Erst wenn der Kunde vor dem Hintergrund eines konkreten Anliegens nachvollziehen kann, warum sein Opt-in erforderlich ist, wird er es auch erteilen.

Etablierung von Mehrwertservices

Die DSGVO ermöglicht die Verarbeitung personenbezogener Daten nicht nur bei Vorliegen eines Einverständnisses seitens des Kunden, sondern auch wenn diese gemäß Art. 6 Abs. 1 S. 1 lit. b) DSGVO für einen „Vertragsabschluss erforderlich" ist. Dieser Anforderung folgend, könnten Finanzdienstleister entweder ihre Produkte in Services „verpacken" oder zusätzliche (digitale) Services etablieren.

Letzteres hat eine deutsche Bank vor einiger Zeit unter dem Titel „Infoservices" erfolgreich vollzogen. Kunden können Zusatzinformationen rund um ihre Produkte oder den Markt „abonnieren". Rechtlich kann dies als neuer Vertragsabschluss gewertet werden. Weiterführende Informationen können auf dieser Basis vom Kunden eingeholt und verarbeitet werden. Ebenso kann damit die Kommunikation mit dem Kunden auf neue Füße gestellt werden.

Produkte nicht isoliert vermarkten

Warum aber vermarkten beispielsweise Banken nach wie vor Girokonten oder Sofortkredite als isolierte Produkte? Warum könnte ein Girokonto in Verbindung mit einem Depot nicht in einen neuen Service namens „Besser Geld sparen und vermehren" einfließen oder Bauspar- und Baufinanzierungsprodukte nicht in den Service „Besser wohnen und schneller ins eigene Haus"?

Auf dieser Basis wären die Finanzdienstleister in der Lage, mit ihrem Kunden in einen deutlich intensiveren Dialog zu treten und neue Ertragsquellen zu erschließen.

Chancen auf der Kostenseite

Die Chancen einer richtigen DSGVO-Umsetzung liegen auch auf der Kostenseite. Beispielhaft sind die erweiterten Kundenrechte wie „Berichtigung" und „Auskunftsrecht" zu nennen. Diese können in Verbindung mit einem Kundendatenportal dazu genutzt werden, um Aktivitäten der Datenpflege auf den Kunden zu verlagern. Kunden werden beispielsweise über personalisierte Ansprachehinweise dazu motiviert, ihre Daten zu überprüfen oder zu vervollständigen. Wertvolle interne Ressourcen zur Kundendatenpflege können damit eingespart werden.

Hierbei können Finanzdienstleister von Social-Media-Plattformen lernen, die es sehr gut verstehen, Nutzer zu mobilisieren und zu motivieren, ihre Daten richtig und vollständig zu hinterlegen.

Die strategische General Data Protection Regulation (GDPR; deutsch DSGVO) bietet also nicht nur Hürden und Risiken, sondern auch klare Chancen, in einen besseren Dialog mit dem Kunden zu treten und sogar komplett neue Geschäftsmodelle aufzubauen. Bedarfsorientierte und anlassbezogene Kontaktaufnahmen können pauschale und häufig falsche Kundenansprachen über unscharfe Kampagnen ersetzen.

Dem Kunden können zielgerichtete, zu seinem Lebensstil und -abschnitt passende und über das typische Spektrum einer Bank hinausgehende Mehrwertservices angeboten werden, um damit neue Erträge zu generieren. Die unterschiedlichen Möglichkeiten zur Steigerung der Effizienz und entsprechender Kosteneinsparungen sollten ebenso berücksichtigt werden.

Prüfung durch unabhängige Dritte

Obwohl der 25. Mai 2018 schon der Vergangenheit angehört, sind viele DSGVO-Implementierungen in ihrer ersten Phase noch nicht abgeschlossen. Unabhängig hiervon gilt es in Zukunft ein Datenschutz-IKS aufzubauen, um die Effektivität der EU-DSGVO nachweisen zu können. Des Weiteren gibt es mit der E-Privacy-Verordnung (ePR) schon eine neue regulatorische Anforderung, welche voraussichtlich Anfang 2019 in Kraft tritt.

Als Nachweis über die Wirksamkeit der gesamten Datenschutzorganisation werden neben einer Auditierung durch die interne Revision künftig auch externe Prüfungen sowie Zertifizierungen durch unabhängige Dritte in Betracht kommen (zum Beispiel die Prüfung des Datenschutz-IKS gemäß ISAE 3402 oder ISAE 3000).

Diese Nachweise werden auch in Outsourcing-Beziehungen eine steigende Relevanz bekommen, da sich der Auftraggeber im Sinne seiner Überwachungsfunktion von der Angemessenheit und Wirksamkeit der Datenschutzorganisation seiner Dienstleister überzeugen muss und dies in der Regel nicht durch eigene Vor-ort-Prüfungen abdecken kann.

Neue Herausforderungen für Banken durch die E-Privacy-Verordnung

Mit der E-Privacy-Verordnung werden in Ergänzung zur Datenschutz-Grundverordnung (DSGVO) spezielle Datenschutzregeln für die elektronische Kommunikation geschaffen. Zusammen mit der DSGVO soll die E-Privacy-Verordnung einen einheitlichen und verbindlichen Rechtsrahmen für den Datenschutz in Europa ab Mai 2018 bilden. Die Billigung der E-Privacy-Verordnung durch den Europäischen Rat steht noch aus und wird für Ende 2018 / Anfang 2019 erwartet.

Da der Anwendungsbereich von ePR im Vergleich zur EU-DSGVO gestiegen ist, müssen die Banken die Analyse der bestehenden Prozesse, die sie in Bezug auf die DSGVO abgeschlossen haben, auf alle Prozesse ausdehnen. Dies betrifft die elektronische Kommunikation in jedweder Form mit ihren Kunden, Mitarbeitern und allen anderen Arten von Datensubjekten.

Darunter sollen neben klassischen Kommunikationsdiensten, wie E-Mail oder Telefon, insbesondere auch OTT-Dienste (Over-the-Top-Services), wie zum Beispiel Whatsapp, fallen. Die bisherige unterschiedliche Handhabe von herkömmlichen Diensten wie SMS und OTT-Diensten soll damit beendet werden. Unter den Begriff der elektronischen Kommunikation fasst die Verordnung jedoch nicht nur das Interagieren von Menschen, sondern auch die Einbindung von Maschinen, beispielsweise mittels Chat-Bots, die Machine-to-Machine-Kommunikation sowie jedwede vernetzten Gegenstände.

Die DSGVO beschränkt sich auf den Schutz personenbezogener Daten, während im Rahmen der ePR der gesamte Inhalt der elektronischen Kommunikation geschützt wird.