

„Jetzt gilt es, Erfahrungen mit den neuen Vorschriften zu sammeln“

Interview mit Frank Trojahn



Quelle: pixabay

Die Sparkassen sind bestens für die DSGVO vorbereitet, so Frank Trojahn. Jetzt gilt es erst einmal, Erfahrungen zu sammeln. So wird sich auch erst mit der Zeit zeigen, bei welchen Aufgaben ein Outsourcing sinnvoll sein wird. In der Praxis rechnet Trojahn darüber hinaus mit etlichen Auslegungsfragen, die – anders als bisher – auf europäischer Ebene geklärt werden müssen. Die größte Herausforderung sieht er bei der technischen Weiterentwicklung, die in der DSGVO noch nicht vollständig berücksichtigt wurde. Red.

In bestimmten Fällen können auch Einwilligungserklärungen zur Nutzung persönlicher Kundendaten dazu dienen, den Kunden Transparenz über die Nutzung ihrer Daten zu verschaffen. Dabei steht die „Datensouveränität“ des Kunden im Vordergrund. Der Kunde soll entscheiden können, was außerhalb der Vertragserfüllung und Erfüllung gesetzlicher Pflichten durch das Kreditinstitut mit seinen Daten geschieht. Und dazu muss er verstehen, wofür diese Daten genutzt werden. Das Bankgeschäft ist zumeist ein Dauerschuldverhältnis, das heißt in einer häufig über Jahre währenden Geschäftsbeziehung

bedient das Kreditinstitut seine Kunden und muss sich hierbei auf ändernde Bedürfnisse seiner Kunden fortlaufend ausrichten.

bm Umfragen zufolge vertrauen die Deutschen in Sachen Datenschutz Banken und Sparkassen in besonderem Maße – weit mehr als zum Beispiel den Internetunternehmen. Warum ist das so? Was machen Kreditinstitute anders, um sich dieses Vertrauen zu verdienen?

Datenschutz ist seit jeher im Bankgeschäft eine zentrale Aufgabe (Stichwort „Bankgeheimnis“) und hat daher für Kreditinstitute eine sehr hohe Priorität. Aufgrund ihrer Geschäftstätigkeit müssen Kreditinstitute über viele persönliche Daten ihrer Kunden verfügen. Deshalb hat Transparenz mittels der neuen Datenschutzhinweise eine hohe Bedeutung.



Quelle: DSGVO

Frank Trojahn, Leiter des zentralen Projekts DSGVO, Deutscher Sparkassen- und Giroverband e.V. (DSGV), Berlin

bm Für die Banken war Datenschutz schon immer ein wichtiges Thema. Und das deutsche Datenschutzrecht galt immer als vergleichsweise streng. Wie gut waren und sind die Sparkassen in Deutschland damit für die Datenschutzverordnung gerüstet?

Die Deutsche Kreditwirtschaft hatte bereits in 2016 mit der Umsetzung der DSGVO begonnen. Auf Ebene der Verbände und/oder der jeweiligen Kreditinstitute wurden Projekte zur Umsetzung der DSGVO aufgesetzt, um den notwendigen rechtlichen, technischen und organisatorischen Anpassungen gerecht zu werden. Im Jahr 2017 wurden hierzu Leitfäden und sonstige Umsetzungshilfen zum Umgang mit der DSGVO in allen Themenbereichen erarbeitet und die IT-Systeme entsprechend angepasst.

bm An welchen Stellen bestand dennoch Handlungsbedarf?

Schutz und Sicherheit der Kundendaten hat für die Banken und Sparkassen stets eine herausragende Rolle gespielt. Deshalb hält sich der Anpassungsbedarf in den Sparkassen in Grenzen. Insbesondere die Vor-

schriften, die die Zulässigkeit der Datenverarbeitung regeln, sind weitgehend unverändert. Allerdings sind verstärkte Informations- und Dokumentationspflichten zu verzeichnen.

Die Verbände haben zur Erfüllung der Informationspflichten der Kreditinstitute Muster für Datenschutzhinweise erstellt und mit den Datenschutzaufsichtsbehörden besprochen. Damit kann Kunden transparent dargelegt werden, zu welchen Zwecken personenbezogene Daten verwendet werden und in welcher Form diese verarbeitet werden.

bm **Wie sieht das inzwischen aus? Sind die Sparkassen DSGVO-fit? Oder gibt es noch Baustellen?**

Die DSGVO betrifft die Sparkassen, wie alle anderen Unternehmen auch. Selbstverständlich haben wir uns schon seit 2015, als die Regelung angekündigt wurde, auf das Inkrafttreten vorbereitet.

In einem zentralen Projekt des DSGVO wurden die notwendigen technischen und organisatorischen Umsetzungen erarbeitet – dies zeigt auch die Relevanz des Themas für uns. Das war auch wichtig, weil es viele Fragen zu klären galt. Die Sparkassen sind also bestens vorbereitet.

Die über 130 000 Berater der 385 deutschen Sparkassen sind angehalten und geschult, ihre Kunden über die Inhalte der DSGVO zu informieren und die Datenschutzhinweise zu erläutern und auszuhandigen. Weiterhin informieren die Berater ihre Kunden über die Vorteile für eine ganzheitliche und passgenaue Beratung durch die Abgabe einer entsprechenden Einwilligungserklärung.

bm **Was denken Sie: Droht den Sparkassen eine „Abmahnwelle“, über die jetzt viel spekuliert wird?**

Die DSGVO hat zwar ein recht strenges Sanktionsregime etabliert, aber die Rahmenbedingungen des bisherigen Bundesdatenschutzgesetzes gelten im Grunde genommen fort. Nach den Regelungen der DSGVO ist die Verarbeitung personenbezogener Daten grundsätzlich verboten, es sei denn, sie ist durch einen Erlaubnistatbestand erlaubt. Alle Datenverarbeitungen, die auf gesetzlichen Vorgaben oder vertraglichen Pflichten beruhen, sind unter der DSGVO weiterhin zulässig. Hierzu zählen alle Aktivitäten im Kundengeschäft, die auf vertraglichen Kundenbeziehungen beruhen, wie beispielsweise Giro-, Kredit- und Wertpapiergeschäft inklusive Kundenberatung, Terminvorbereitung und gesetzlich zulässiger Werbung.

„Die Rahmenbedingungen des bisherigen Bundesdatenschutzgesetzes gelten im Grunde genommen fort.“

„Da die DSGVO einen recht hohen Abstraktionsgrad hat, wird es etliche zu klärende Auslegungsfragen geben.“

„Es gilt, das Datenschutzrecht funktions- und interessengerecht fortzuentwickeln.“

Neben diesen gesetzlichen und vertraglichen Grundlagen kann auch eine Einwilligung des Kunden zur Verarbeitung personenbezogener Daten eingeholt werden. Die eingesetzten Formulare und Prozesse wurden dabei natürlich umfassend datenschutzjuristisch geprüft. Darüber hinaus hat die Kreditwirtschaft schon frühzeitig den Kontakt zu den Datenschutzaufsichtsbehörden gesucht, um Umsetzungsfragen von grundsätzlicher Bedeutung frühzeitig zu klären.

bm **An welchen Stellen sehen Sie die größten Herausforderungen oder auch noch Baustellen?**

Wie alle Unternehmen haben sich die Sparkassen vor dem Hintergrund der DSGVO in den vergangenen Jahren noch einmal explizit und mit großem Aufwand dem Thema Datenschutz gewidmet. Das ist auch der Sinn der neuen Verordnung.

Die DSGVO ist erst seit wenigen Wochen wirksam. Nun gilt es, zunächst Erfahrungen mit den neuen Vorschriften zu sammeln. Dabei ist neu, dass diese letztendlich EU-weit geklärt werden müssen. Hier wird der neue Europäische Datenschutzausschuss gefragt sein, Belange von Verbrauchern und Unternehmen gleichermaßen zu berücksichtigen.

Eine besondere Herausforderung dürfte auch die rasch fortschreitende technologische Entwicklung sein, die die DSGVO nicht in jeder Nuance voraussehen konnte. Auch hier gilt es, sachgerechte Antworten zu finden und das Datenschutzrecht funktions- und interessengerecht fortzuentwickeln.

bm **Lässt sich der mit der Umsetzung der Datenschutzgrundverordnung verbundene Aufwand für die Sparkassenorganisation beziffern?**

Aufgrund der deutlich ausgeweiteten Pflichten zur Information und Dokumentation ist der bürokratische Aufwand bei allen Unternehmen erheblich gestiegen. Der Aufwand für die Anpassung der IT-Systeme, Formulare und Prozesse war in der Sparkassenorganisation insgesamt sehr hoch.

bm **Bietet das Thema Datenschutz auch Möglichkeiten für neue geschäftliche Ansätze – etwa indem sich Sparkassen als sicherer Datenspeicher positionieren? Oder ist im Grund-**

de wieder einmal außer Spesen nichts gewesen?

Ein Vorteil der DSGVO besteht zunächst darin, dass für Unternehmen in der EU die gleichen Rechtsvorschriften gelten. Das sorgt für gleiche Wettbewerbsbedingungen im EU-Binnenmarkt.

„Ob sich in Teilbereichen Outsourcingperspektiven ergeben, wird zu einem späteren Zeitpunkt zu beurteilen sein.“

Die DSGVO bietet zudem die Chance, den eigenen Datenbestand neu zu beurteilen, gegebenenfalls Verbesserungen vorzunehmen und auch über die Weiterentwicklung der Datennutzung und neue Geschäftsmodelle zugunsten der Kunden nachzudenken.

bm Können kleinere Sparkassen die Umsetzung allein stemmen? Oder welche Unterstützung gibt es im Verbund?

Die Sparkassen wurden durch die Regionalverbände und durch ein zentrales Projekt des DSGV mit 15 Expertengruppen aus dem ganzen Bundesgebiet umfangreich unterstützt. Die notwendigen technischen und organisatorischen Umsetzungen wurden zentral erarbeitet und den Sparkassen rechtzeitig vor Inkrafttreten der DSGVO bereitgestellt. Zur Schulung der Mitarbeiter stehen umfangreiche Schulungsmaterialien zur Verfügung und über die Regionalverbände und Akademien wird auf Fachtagungen und Seminaren über das Thema informiert.

„Die DSGVO-Umsetzung hat die frühzeitige Einbeziehung der IT-Dienstleister erforderlich gemacht.“

bm An welchen Stellen kann das Rechenzentrum helfen – etwa bei der Beaufskunftung oder der Datenlöschung nach der gesetzlichen Aufbewahrungsfrist? Lässt sich das automatisieren, gibt es hierzu Lösungen?

Die DSGVO-Umsetzung hat die frühzeitige Einbeziehung der zentralen IT-Dienstleister erforderlich gemacht. Neben der datenschutzkonformen Verarbeitung von personenbezogenen Daten stand bei der Anpassung der IT-Systeme vor allem ein hohes Maß an IT-Sicherheit im Fokus.

bm Ist das Thema Datenportabilität mit dem bereits realisierten Kontowechselservice bereits erledigt? Oder hängt mehr daran?

Das ist nur ein Baustein. Für Sparkassenkunden bestehen viele Möglichkeiten, Informationen zu Personen- und Kontodaten selbstständig über die Internetfiliale abzurufen. Darüber hinaus erhalten Kunden auf Wunsch eine Datenauskunft nach Art. 15 DSGVO in standardisierter Form.

„Die DSGVO bietet die Chance, den eigenen Datenbestand neu zu beurteilen.“

bm Wie hat sich die Position des Datenschutzbeauftragten in der Sparkasse verändert? Welche Aufgaben sind hinzugekommen?

Die Qualifizierung der Mitarbeiter ist ein wesentlicher Baustein der DSGVO-Umsetzung in Banken und Sparkassen. Es steht regelmäßig umfangreiches Schulungsmaterial zur Verfügung. Die Schulungsinhalte können vom Erlernen der gesetzlichen Rahmenbedingungen über das Handling in der IT bis hin zur Beantwortung von möglichen Kundenanfragen reichen. Wichtig ist, nicht nur Datenschutzbeauftragte in die Schulungen einzubeziehen, sondern eine breite Akzeptanz bei Führungskräften und Beratern zu schaffen.

Die Rolle und die Aufgaben des Datenschutzbeauftragten sind in Art. 39 der DSGVO geregelt. Seine Aufgaben umfassen die Beratung, Unterrichtung und Überwachung der Datenschutzorganisation. Damit hat sich die Rolle von operativen Aufgaben hin zur koordinieren Funktion verändert.

bm Lassen sich einige der DSGVO-bedingten Aufgaben outsourcen? Wenn ja welche und welche nicht?

Das Outsourcing DSGVO-bedingter Aufgaben stand nicht im Mittelpunkt der bisherigen Projektarbeit. Im Moment ist ganz überwiegend davon auszugehen, dass die zentralen Herausforderungen in der Eigenverantwortung der Sparkasse zu bewältigen sind. Ob sich in Teilbereichen Outsourcingperspektiven ergeben, wird zu einem späteren Zeitpunkt zu beurteilen sein.

bm Gibt es ein Spannungsfeld zwischen Compliance und Datenschutz? Compliance setzt ja auch relativ weitgehende Einsichts- und Auskunftsrechte voraus ...

Die Compliance-Funktion ist für Kreditinstitute im KWG beziehungsweise den MaRisk geregelt. Nach MaRisk ist den bisherigen Compliance-Strukturen beziehungsweise anderen Beauftragten weder über- noch untergeordnet. Insofern werden die Regelungsfelder anderer Compliance-Bereiche auch nicht von der Compliance-Funktion nach MaRisk überlagert und bleiben unberührt.

bm Welche „Datenpannen“ unterliegen jetzt der Meldepflicht? Geht es da nur um echte Datenlecks oder um mehr?

Die Meldepflicht von Datenschutzverletzungen ist in Art. 33 der DSGVO geregelt. Danach sind Datenschutzverletzungen meldepflichtig, wenn diese zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen.

Neben „Datenlecks“ in zentralen Systemen zählt dazu beispielsweise bereits das Abhandenkommen eines mobilen Rechners mit unverschlüsselter Festplatte, auf der lokal Kundendaten für Auswertungszwecke gespeichert sind.

bm Mit Big Data war die Kreditwirtschaft bisher sehr zurückhaltend. Hat sich das Thema durch die DSGVO erledigt? Oder was ist noch möglich?

Die DSGVO bietet die Chance, den eigenen Datenbestand neu zu beurteilen und auch über die Weiterentwicklung der Datennutzung und neue Geschäftsmodelle zugunsten der Kunden nachzudenken. So stellt die Einwilligung des Kunden einen in der DSGVO explizit vorgesehenen rechtssicheren Weg für die Analyse personenbezogener Daten dar. Mit einer freiwilligen Kundeneinwilligung ist es möglich, die Kunden über die reine Vertragserfüllung hinaus individuell in Finanzfragen noch passgenauer beraten zu können.

bm Wie hoch ist die Bereitschaft der Kunden, ihrer Sparkasse Daten zur Verfügung zu stellen, um dafür wirklich passende Angebote zu erhalten? Oder gibt es künftig wieder Marketing mit der Gießkanne, weil es an personenbezogenen Daten fehlt?

Den Sparkassen ist die persönliche Beratung ihrer Kunden sehr wichtig. Daher sprechen die Berater ihre Kunden persönlich an und informieren sie über die Hintergründe, Rechten und Pflichten aus der Datenschutzgrundverordnung. Weiterhin informieren die Berater ihre Kunden über

die Vorteile für eine ganzheitliche und passgenaue Beratung durch die Abgabe einer entsprechenden Einwilligungserklärung. Es ist nicht so, dass sich die Kunden Sorgen machen müssen, mit Wer-

bung bombardiert zu werden, weil sie in die Nutzung ihrer Daten eingewilligt haben. Im Gegenteil: Angebote können zielgerichtet an die Bedürfnisse des Kunden angepasst werden. ■