# „Nicht jeder Regelungsraum sollte durch **staatliche Regelungen** belegt werden“

Interview mit Jens Saenger

**Seit jeher identifizieren sich Kreditinstitute mit dem Datenschutz als Kernaufgabe des Bankgeschäfts, so Jens Saenger. Dennoch wurde der Datenschutz lange gewissermaßen nebenbei erledigt. Spätestens mit der Digitalisierung ist das Themenfeld Datenschutz und Datensicherheit jedoch sehr komplex geworden, weshalb vor allem kleinere Institute die Aufgaben auslagern. In Sachen Regulierung mahnt Jens Saenger zweierlei an: Nicht alles, was reguliert werden kann, sollte auch reguliert werden. Aber es braucht mehr „Waffengleichheit“ zwischen Banken und Fintechs. Red.**

**bm Wenn es um ihr Geld geht, sind die Menschen sensibel. Stehen Kreditinstitute in Deutschland in Sachen Datenschutz und Datensicherheit im Vergleich zu anderen Branchen unter besonderer Beobachtung? Oder würden die Kunden Datenauswertungen, die sie zum Beispiel bei Online-Händlern schätzen, seitens ihrer Bank oder Sparkasse gar nicht akzeptieren?**

Natürlich stehen Kreditinstitute – und zwar in vielen Bereichen auch aus gutem Grund – unter besonderer Beobachtung. Wer würde schon gerne bei jeder Dispoüberziehung erfahren, wie andere Menschen in ähnlichen Situationen gehandelt haben? Wer würde in dieser Situation gleich Werbepost mit Kreditangeboten haben wollen? Oder anderes Beispiel: Wer würde wollen, dass seine Überweisungsträger in öffentlich zugänglichen Papierkörben entsorgt werden? Banken haben schon seit jeher ein ausgeprägtes Verständnis von Geheimhaltungsverpflichtungen. Das Bankgeheimnis ist in der DNA eines jeden „Bankers“.

**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?**

**Jens Saenger, Sprecher der Geschäftsführung, GenoTec GmbH, Neu-Isenburg/ Zeppelinheim Ost**

Allein schon durch das Bankgeheimnis unterlagen und unterliegen Kreditinstitute im Hinblick auf den Schutz von Daten einer besonderen Geheimhaltungspflicht.

Darüber hinaus sind gerade die Volks- und Raiffeisenbanken Unternehmen, die in ihrem Markenkern die Förderung der Mitglieder und Kunden tragen. Ihre historische Spitzenleistung ist doch, dass sie sich seit über 150 Jahren ihrer Region und deren Bürgern verpflichtet haben – über die reine Gewinnmaximierung hinaus. Die solidarische Verpflichtung bedingt einen respektvollen und achtsamen Umgang miteinander, insbesondere mit dem Wissen, um die Belange seines Nachbarn. Dies gilt im Übrigen auch für Sparkassen.

Damit haben diese Kreditinstitute die schweren Zeiten der Weltwirtschaftskrise, zweier Weltkriege, dem Nachkriegsdeutschland, aber auch den jüngeren Finanzkrisen sicher getrotzt. Der über viele Jahrzehnte sorgsam gepflegte Umgang miteinander, hat sich auf das heute von Ihnen geschilderte Vertrauen, bezahlt gemacht.

Die Identifikation mit dem Datenschutz als Kernaufgabe des Bankgeschäfts bedeutet

auch, dass sich Kreditinstitute nicht auf dem Erreichten ausruhen. Neue Technologien schaffen neue Bedrohungssituationen, und neue Bedrohungssituationen bedürfen neuer Abwehrmechanismen. Dem trägt im Übrigen auch die Bankenaufsicht Rechnung. Auch das neue IT-Sicherheitsgesetz und die zu erwartenden „Bankenaufsichtsrechtlichen Anforderungen an die IT" (BAIT) werden neben der Selbstverpflichtung der meisten Banken(gruppen) auch gehörigen aufsichtsrechtlichen Druck ausüben. Ein Druck, der bei anderen nicht – jedenfalls nicht in der Ausprägung gilt. Auch nicht bei den sogenannten Fintechs.

Internetunternehmen kommen und gehen. Wenn sie älter als fünf Jahre sind, dann gelten sie schon als Dinosaurier des Internets. Allein aus ihrer Start-up-Position heraus agieren sie risikofreudiger. Sie müssen mehr ausprobieren und setzen natürlich andere Prioritäten. Sicherheit gehört naturgemäß – und auch gar nicht abwertend gemeint – sicherlich nicht dazu.

**bum: Welche Selbstbeschränkungen bei dem, was sich mit den vorhandenen Daten anfangen ließe, sind mit der besonderen Verantwortung von Banken in Sachen Datenschutz verbunden – etwa im Bereich Big Data oder Marketingautomation?**

Wenn der sorgsame Umgang miteinander das Handeln bestimmt, dann ist jede Datennutzung außerhalb dieses dienenden Charakters schädlich.

In ihrer Aufgabe als Finanzintermediäre kommen Banken allerdings nur dann adäquat nach, wenn sie die Kundenbedürfnisse umfassend begreifen und alternative Lösungsangebote vorschlagen können. Wer sich gegen Risiken des Lebens finanziell absichern will – etwa gegen Berufsunfähigkeit – kann dies tun, indem er spart oder aber auch indem er sich versichert. Beides schützt gegen die finanziellen Bedrohungen. Hier ist Datenaustausch sicherlich sinnvoll.

**bum: Kann ein hohes Datenschutzniveau auch zum Wettbewerbsnachteil im Vergleich zu neuen Wettbewerbern werden?**

Wer sich seinen Kunden verpflichtet fühlt und nachhaltig agiert, wird langfristig bestehen. Aber nicht jeder Regelungsraum sollte durch staatliche Regelungen belegt werden. Manches kann und sollte man dem Bürger zutrauen – auch im Bereich des Datenschutzes.

**„Dem Datenschutzbeauftragten kommt neben der mahnenden auch eine beratende Funktion zu."**

Unabhängig davon: Wenn die Datenschutzregelungen für alle gleich sind, wie soll dann für den einzelnen ein Wettbewerbsnachteil entstehen? Was ich meine: Wenn Regelungen erlassen werden, dann sollte auf eine einheitliche Geltung und Umsetzung gedrungen werden.

Gerade die neue EU-DSGVO, die eine Harmonisierung des europäischen Datenschutzniveaus mit sich bringt, scheint zumindest regulativ diese Gleichheit herbeiführen zu wollen. Allerdings bliebe noch sicherzustellen, dass sie auch immer gleich umgesetzt wird. Ein Wettbewerbsnachteil wäre dann idealtypisch ausgeschlossen – die Mehrkosten des Datenschutzes wären dann für alle gleichermaßen in der Preisstellung umzusetzen (oder anderweitig zu kompensieren).

**bum: Wie sehen Sie die Position eines Datenschutzbeauftragten in einer Bank oder Sparkasse? Ist der Datenschutzbeauftragte mitunter der „Bremser", der Ideen aus anderen Abteilungen wie dem Marketing eine Absage erteilen muss?**

Natürlich wird der Datenschutzbeauftragte als „Bremser" empfunden. Es gehört zu seinen Aufgaben, Einhalt zu gebieten. Datenschutz ist ein hohes Gut, das selbstverständlich gegen andere legitime Interessen, wie zum Beispiel Ertragssteigerung, abzuwägen und im Zweifelsfall auch durchzusetzen ist. Wir alle brauchen hin und wieder jemanden, der uns bremst und fragt: „Ist das noch vereinbar mit unseren Werten?"

Wir würden aber bei der Frage nicht innehalten und den Geschäftszweck – Kundenbedarf, Ertragschance – verstehen wollen, um dann Datenschutz- beziehungsweise normenkonforme, neudeutsch „compliante" Wege zur Erreichung der Geschäftsziele aufzuzeigen.

Damit kommt dem Datenschutzbeauftragten neben der mahnenden Funktion auch eine beratende Funktion zu. In diesem Sinne bremst der Datenschutzbeauftragte nicht nur, sondern er befördert gleichzeitig konstruktiv die Strategieentscheidungen der Geschäftsführung.

**bum: Wie komplex ist die Arbeit des Datenschutzbeauftragten in einem Kreditinstitut. Ist das eine Aufgabe, die sich „nebenbei" erledigen lässt, oder eine Hauptaufgabe?**

Dies hängt grundsätzlich von der Größe des Kreditinstitutes, der eingesetzten Verfahren oder den beauftragten Auftragsdatenverarbeitern ab.

**„Faktisch wurde bei vielen Instituten der Datenschutz lange nebenbei erledigt."**

Faktisch wurde bei vielen Instituten der Datenschutz lange „nebenbei" erledigt. Dies hat sich inzwischen grundsätzlich verändert. Die Anforderungen an das Spezialwissen sind über die Jahre enorm gestiegen: Spätestens mit der Digitalisierung

unser Gesellschaft ist der Untersuchungsgegenstand wesentlich komplexer geworden. Die neuen gesetzlichen Regelungen sind (nur) Ausdruck dieser Entwicklung und tragen ihr Rechnung.

Nicht zuletzt durch die neue EU-Datenschutzgrundverordnung wird sich auch der Aufwand bei vielen Instituten deutlich erhöhen. Schon jetzt sollte man sich hier vorbereiten, um für den Umsetzungstermin am 25. Mai 2018 gewappnet zu sein.

„Nicht zuletzt durch die neue EU-Datenschutzgrundverordnung wird sich der Aufwand bei vielen Instituten deutlich erhöhen."

**bum Wo lauern zum Beispiel Fallstricke in Sachen IT-Sicherheitsmanagement oder Datenschutz, die man ohne spezielle Fachkenntnis vielleicht gar nicht erkennt?**

IT-Sicherheit und Datenschutz setzen notwendig ein umfangreiches Fachwissen voraus. Aber das allein macht noch keinen guten Beauftragten.

In der Praxis leitet sowohl den IT-Sicherheitsbeauftragten als auch den Datenschutzbeauftragten seine Erfahrung: Die Erfahrung lässt ihn – bankindividuell – geeignete Monitoringsysteme aufsetzen. Sie identifiziert die eigentliche Gefahrenlage in der konkreten Situation, und sie lässt ihn auch die angemessenen, wirksamen Gegenmaßnahmen wählen.

Ein Beispiel: Nach § 9 des Bundesdatenschutzgesetzes (BDSG) in Verbindung mit der Anlage zu § 9 Satz 1 BDSG sind alle Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten oder nutzen wollen, verpflichtet, die erforderlichen und angemessenen technischen und organisatorischen Maßnahmen zum Erzielen und Aufrechterhalten der Datensicherheit zu treffen. Es geht dabei um die Gewährleistung der Verfügbarkeit, Authentizität und Integrität der Daten. Hierfür bedarf es vorab der Durchführung einer Schutzbedarfsanalyse, um zu ermitteln, welcher Schutz zur Einhaltung der drei Ziele sowie die dafür einzusetzende Technik erforderlich und angemessen ist. Dies erfordert fundierte Kenntnisse und eine laufende Informationsbeschaffung zur aktuellen Gesetzeslage und Technik.

Dabei ist es wichtig, dass sich der Beauftragte vernetzt und so auch auf die Erfahrungen anderer zurückgreifen kann. Es ist ein entscheidender Vorsprung, von einem Hackerangriff im anderen Teil der Republik oder einer Datenschutzpanne in einem anderen Unternehmen zu wissen.

Das ist im Übrigen auch der Vorteil eines spezialisierten Mehrmandantenanbieters: Hier laufen die Fäden zusammen: der Einzelne profitiert von dem Wissen der Gemeinschaft.

**bum Wann ist es sinnvoll, bei diesen Aufgaben auf Outsourcing zu setzen?**

Wenn man der Komplexität selber nicht oder nur zu unverhältnismäßig hohen Kosten gerecht werden kann, ist es sinnvoll auszulagern. Die Ausbildung, Sicherung und Fortentwicklung des erforderlichen Know-hows ist in Anbetracht der komplexen Materie nicht trivial und sehr zeit- und kostenintensiv. Man sollte auch nicht vergessen, dass es neben dem akademischen Wissen der Erfahrungen bedarf, um möglichen Fehlentwicklungen schnell und pragmatisch begegnen zu können.

„Die Ausbildung, Sicherung und Fortentwicklung des erforderlichen Know-hows ist sehr zeit- und kostenintensiv."

Auslagerung an einen spezialisierten Dienstleister ist dann der beste Weg, wenn das Geschäftsmodell eine Bereitstellung eigener, erfahrener Spezialisten organisatorisch oder betriebswirtschaftlich nicht hergibt. Ein spezialisierter Experte wird – bei ausreichender Erfahrung (überregional und hinreichender Kundenbasis) und hinreichender Transparenz seiner Dienstleistung – den Schutzzweck der Informationssicherheit und des Datenschutzes am besten befördern können.

**bum Welche Aufgaben genau lassen sich outsourcen – was verbleibt auch dann noch in der Verantwortung des jeweiligen Instituts?**

Die Verantwortung lässt sich grundsätzlich nicht auslagern. Diese bleibt den Organen einer jeden Gesellschaft (Bank oder Nicht-Bank) vorbehalten. Und um es mit Wowereit zu sagen: Das ist auch gut so! Denn Datenschutz und Informationssicherheit sind ein hohes Gut.

Dies setzt sich auf der persönlichen Ebene fort. Mittlerweile produziert und verarbeitet jeder Mitarbeiter im Unternehmen Daten und arbeitet an einer IT-basierten Schnittstelle – und sei es nur die Zugangskontrolle oder die Zeiterfassung. Damit trägt auch jeder Einzelne Verantwortung, die auch er grundsätzlich nicht delegieren kann: Jeder ist gefordert, darauf zu achten, dass er mit „seinen" Daten sorgsam umgeht und Gefährdungssituationen in der Informationssicherheit erst gar nicht entstehen lässt.

Alles andere – beispielsweise die systematische Erfassung und Analyse möglicher Schwachstellen, die Ableitung entsprechender Kontrollhandlungen, die Empfehlung geeigneter Gegenmaßnahmen oder auch die Sensibilisierung der Mitarbeiter für Risikolagen – kann in die Hände von Spezialisten gegeben werden.

**Wie viele Genossenschaftsbanken zählen Sie aktuell zu Ihren Kunden? Sind das eher größere oder kleinere Häuser?**

Wir haben bundesweit im genossenschaftlichen Bankensektor aktuell weit über 200 Auslagerungsmandate im Bereich des Datenschutzbeauftragten und des Informationssicherheitsbeauftragten. Dabei ist fast jede Bilanzsumme vertreten, von ganz kleinen Häusern bis zu den ganz großen Volks- und Raiffeisenbanken.

**„Wir erlebten es bisher als hemmend, dass es im Datenschutz unterschiedliche Positionierungen der Landesdatenschutzbeauftragten zu spezifischen Themen gab."**

Bitte bedenken Sie, dass die größeren Häuser der Volks- und Raiffeisenbanken mit Bilanzsummen von drei bis fünf Milliarden Euro sind, also im nationalen und internationalen Bereich eher als klein einzustufen sind. Daher ist auch die Vollauslagerung bei größeren Verbundunternehmen nicht nur sicher möglich, sondern auch zielführend zur Erhöhung der Informations- und Datensicherheit.

Naturgemäß übernehmen wir bei den kleinen und kleineren eher die gesamte Funktion im Rahmen von Auslagerungen, während die großen Häuser uns eher beratend und unterstützend hinzuziehen.

**Gibt es in Sachen Datenschutzrecht „Waffengleichheit" zwischen Kreditinstituten und Fintechs beziehungsweise Wettbewerbern aus anderen Branchen?**

Nein. Hier gibt es sowohl regulativ als auch in der Umsetzung und Kontrolle ein klares Ungleichgewicht.

**Was bedeutet die EU-Datenschutzgrundverordnung aus Sicht von Banken?**

Wir gehen davon aus, dass der Aufwand durch die impliziten Dokumentationspflichten erheblich anwachsen wird. Inhaltlich erfüllen die meisten Regionalbanken die Vorgaben schon heute.

Aber: Fakt ist, das alte BDSG wird ab 25. Mai 2018 in seiner jetzigen Form nicht mehr existieren. Der Gesetzgeber ist zurzeit damit beschäftigt, die in der EU-DSGVO eingebundenen Öffnungsklauseln für sich national zu nutzen. Das heißt, es wird zur neuen Verordnung ein begleitendes Ausführungsgesetz geben. Hierzu liegt bereits ein Regierungsentwurf vor. Die Banken sind also gut beraten, sich schon jetzt Gedanken über die organisatorische Umsetzung ab 2018 zu machen.

**Und wie ist das mit der PSD2: Welche Lücke reißen hier die Schnittstellen für Drittanbieter in Sachen Datenschutz oder Datensicherheit?**

Grundsätzlich besagt die „Zweite Zahlungsrichtlinie" PSD2, dass neben den Banken auch Drittdienstleister, beispielsweise Internetunternehmen wie Zahlungsauslöse- oder Kontoinformationsdienste, zur Ausführung ihrer Dienstleistungen über eine Schnittstelle der Bank Zugang zu Konten und Kontoumsätzen des Bankkunden erhalten dürfen. Diese Daten sind datenschutzrechtlich betrachtet sehr sensibel.

**„Mit der PSD2 steigt die Gefahr von Hackerangriffen oder auch eine eventuelle Zweckentfremdung der Daten durch Dritte."**

Dabei ist auch zu bedenken, dass der bisherige Aspekt des Bankgeheimnisses hier nicht greift. Deswegen ist eine saubere Umsetzung der „ausdrücklichen Zustimmung" der Zahlungsdienstenutzer nach Art. 94 Abs. 2 PSD2 im Kontext altes BDSG bis zum 25. Mai 2018 und neuer EU-DSGVO ab 25. Mai 2018 zu beachten. Die PSD2 wird bis zum 13. Januar 2018 in nationales Recht umzusetzen sein.

**Gibt es auch rechtliche Vorgaben, deren Sinn Sie infrage stellen? Und welche Änderungswünsche hätten Sie aus der Praxis heraus?**

Ich würde gar nicht bei den rechtlichen Vorgaben ansetzen wollen. Sie reagieren mal besser mal schlechter auf gesellschaftliche Entwicklungen. Wir erlebten es bisher als hemmend, dass es im Datenschutz zum Beispiel unterschiedliche Positionierungen der Landesdatenschutzbeauftragten zu spezifischen Themen gab. Dies erschwert die praktische Umsetzung und führt dazu, dass jeder versucht, sein eigenes Süppchen zu kochen.

Die Banken stehen im Hinblick auf die neue EU-DSGVO vor großen Herausforderungen. Sie stellen sich alle – ausnahmslos und aus einem inneren Antrieb heraus – ihrer datenschutzrechtlichen Verantwortung. Aber sie haben nur begrenzte Zeit. Sie sind angewiesen auf klare Rahmenbedingungen, damit sie schnell in die Umsetzung kommen und sich wieder dem Markt zuwenden können. Wenn ich einen Wunsch frei hätte, würde ich mir wünschen, dass die 16 Landesbehörden im Kontext der neuen EU-DSGVO schnell einen Prozess finden, der einen einheitlichen Konsens bei aktuellen Datenschutzproblemen möglich macht.