

Dora: Haben sich die Banken zu sicher gefühlt?

Im großen FinanzBusiness-Interview zeigen Norman Edelmann und Tino Nielsen von Awado auf, was die Banken bisher in Sachen Dora richtig gemacht haben und welche Herausforderungen noch vor ihnen liegen.



Bringt die Banken ins Schwitzen: Dora | Foto: FinanzBusiness / KI

[Hauke Rudolph](#)

Herr Nielsen, Herr Edelmann: Die Banken klagen über die hohe Komplexität von Dora. Was sind die Herausforderungen?

Tino Nielsen: "Wir begrüßen die europaweite Harmonisierung der Anforderungen und die klaren, verbindlichen Vorgaben von Dora. Gleichzeitig birgt dies Herausforderungen: Das deutsche Drei-Säulen-Modell stellt im europäischen Vergleich eine Besonderheit dar. Einheitliche Vorschriften für sehr unterschiedliche Geschäftsmodelle führen daher faktisch zu Ungleichbehandlungen. Zudem entsteht durch das Fortbestehen der MaRisk eine Doppelregulierung, die zusätzliche Unsicherheiten schafft.

Damit Regulierung wirksam ist, muss sie für Finanzunternehmen handhabbar bleiben. Während die BAIT rund 30 Seiten umfassten, bringt Dora über 500 Seiten mit sich - der reine Befassungsaufwand hat sich somit vervielfacht. Die in Art. 16 Dora vorgesehenen Erleichterungen greifen für keine mir bekannte Genossenschaftsbank, da die

konservativen Schwellenwerte regelmäßig überschritten werden. Hier besteht Anpassungsbedarf.

Erschwerend kommt hinzu, dass der Markt für IT-Compliance-Experten bereits heute überzeichnet ist. Offene Stellen lassen sich selbst bei entsprechendem Willen nicht kurzfristig besetzen. Gleichzeitig generiert IT-Compliance keine Umsätze, sondern dient primär der Vermeidung ungeplanter Kosten und Haftungsrisiken.”

Norman Edelmann: ”Ein zusätzlicher Aspekt betrifft die Krisenkommunikation: Dora verlangt nicht nur robuste technische Resilienz, sondern auch eine strukturierte, zeitnahe und adressatenorientierte Kommunikation im Störfall. Die Anforderungen an Meldefristen, Abstimmungsprozesse und Eskalationswege sind hoch und erfordern klare interne Verantwortlichkeiten sowie verlässliche Kommunikationslinien zu Dienstleistern, Aufsichtsbehörden und Kunden. Viele Finanzunternehmen müssen dafür bestehende Krisenstäbe, Kommunikationsrichtlinien und Notfallprozesse grundlegend überarbeiten - sowohl organisatorisch als auch inhaltlich. Die Herausforderung liegt dabei weniger in der grundsätzlichen Bereitschaft als vielmehr in der operativen Umsetzung und der Synchronisation aller beteiligten Parteien.”

Welchen Herausforderungen sehen sich die Institute auf fachlicher Ebene ausgesetzt?

Tino Nielsen: ”Die Dora-Vorschriften gehen auf fachlicher Ebene in Teilen deutlich über bisherige Vorgaben hinaus oder verlangen ein verändertes, methodisch angepasstes Vorgehen. Besonders sichtbar wird dies im IKT-Drittparteienrisikomanagement, dessen Anforderungen nun stark denen des Auslagerungsmanagements nach AT 9 MaRisk ähneln und damit eine faktische Doppelregulierung schaffen. Zusätzlich führt die notwendige Identifizierung kritischer bzw. wichtiger Funktionen - als zentrale Steuerungsgröße im IKT-Risikomanagement - aufgrund methodischer Anpassungen zu spürbaren Unsicherheiten.”



Norman Edelmann | Foto: Jörn Strojny/Genoverband

Norman Edelmann: "Dora verschiebt die Krisenkommunikation von einem überwiegend internen Erfüllungsakt hin zu einem reputationssensitiven Führungsinstrument. Neben regulatorisch sauberen Meldungen, die Teil des IKT-Vorfallmeldewesens sind, erwarten Markt und Öffentlichkeit heute transparente, konsistente und vertrauensbildende Aussagen. Dora zentriert somit den reputationssichernden Faktor in einer Art und Weise, die Finanzdienstleister bisher nicht kannten. Professionell vorbereitete Kommunikationsprozesse - abgestimmt zwischen Fachbereich, Management und Kommunikation - werden damit zu einem entscheidenden Faktor, um Vertrauen zu erhalten und Reputationsschäden im Ernstfall zu vermeiden."



Tino Nielsen | Foto: Genoverband

Sie sprechen von Unsicherheiten aufgrund erforderlicher Anpassungen bei der Identifizierung kritischer oder wichtiger Funktionen. Wie meinen Sie das?

Tino Nielsen: "Bisher waren für zeitkritische Prozesse und Aktivitäten Notfallvorkehrungen zu treffen, wenn die Auswirkungen einer Nicht-Verfügbarkeit den eigenen Risikoappetit überschritten haben. Vielfach wurde die Methode der Business Impact Analyse (BIA) genutzt, mit der z.B. die finanziellen Auswirkungen der Nicht-Verfügbarkeit von Prozessen und Systemen bewertet wurden.

Der Ausdruck ´kritische oder wichtige Funktion´ umfasst mehr und fordert, dass nicht nur Auswirkungen einer Nicht-Verfügbarkeit, sondern auch verletzter Integrität, Authentizität und Vertraulichkeit zu bewerten sind. Die bisher genutzte BIA ist dafür nicht vollständig geeignet. In dieser Klarheit ist uns dies erst seit der BaFin-Jahresveranstaltung zu Dora aus dem Dezember 2025 klar. Mit den erforderlichen Anpassungen wird ein erheblicher Arbeitsaufwand auf die Institute zukommen."

Norman Edelmann: "Die europäischen Regulatoren haben erkannt, dass ein Dora-relevantes Ereignis bei Missmanagement der Kommunikation einen Reputationsschaden für das europäische Finanzsystem mit sich bringt. Daher fordern sie von den Banken, sich in kommunikativen Belangen so aufzustellen, dass die eigene Reputation, aber auch die des Finanzsystems insgesamt gewährleistet wird. Diese Aufgabe mündet darin, dass Banken frühzeitig Szenarien adaptieren und kommunikative Maßnahmen entwickeln müssen, um alle relevanten Stakeholdergruppen schnellstmöglich zu informieren. Dieser Ansatz ist für die Banken neu und führt in der Implementierung zu Unsicherheiten darüber, in welchem Umfang sie die Kommunikationsmittel zu erfüllen haben."

Kann es sein, dass die Banken sich zu sicher gefühlt haben?

Tino Nielsen: "Rückblickend ist es immer leicht, eine Bewertung vorzunehmen. Mit Blick auf kritische oder wichtige Funktionen würde ich jedoch nicht sagen, dass die Institute Fehler gemacht haben. Bei neuen Vorschriften ist es vielmehr typisch, dass zunächst unterschiedliche Verständnisse bestehen. Und bei begrenzten Ressourcen müssen Leitungsorgane entscheiden, wie sie diese einsetzen. Solange unklar war, wie die finalen Vorschriften aussehen und welche Unterstützungsleistungen bereitstehen, ist es nachvollziehbar, dass nicht sofort ´All-In´ gegangen wurde. Auch die Aufsicht hat das so gesehen: Für erst im Verlauf 2025 umgesetzte Dora-Vorschriften ist Transparenz wichtig, eine Beanstandung aber nicht erforderlich.

Unser Appell bleibt dennoch: Offene Punkte jetzt entschlossen schließen und eine gesamthafte Bewertung der Maßnahmen vornehmen - nicht nur für die

Aufsichtskonformität, sondern weil die Anforderungen sinnvoll sind und die digitale Resilienz stärken.”

Norman Edelmann: ”In ihren Notfallkonzepten hatten die Institute kommunikative Aspekte selbstverständlich schon berücksichtigt; bislang lag es jedoch in ihrem Ermessen, ob und in welchem Umfang sie jenseits der Meldepflichten nach außen kommunizieren. Diese Flexibilität ist mit Dora nun deutlich eingeschränkt. Die neuen Vorgaben verlangen eine strukturiertere, verbindliche und nachvollziehbar dokumentierte Kommunikationsplanung - sowohl gegenüber der Aufsicht als Teil des Notfallmanagements als auch gegenüber Kunden und weiteren Stakeholdern - als Teil der Krisenkommunikation. Für viele Institute bedeutet das, bestehende Prozesse gezielt auszubauen, statt sie völlig neu erfinden zu müssen.”

Kommen wir zurück auf die Dora-Implementierung. Wie haben sich die Institute nach Ihrer Erkenntnis auf die Dora-Umsetzung vorbereitet?

Tino Nielsen: ”Einige Institute haben ab Ende 2023 oder Anfang 2024 mit der Vorbereitung auf Dora begonnen, während andere - wie bereits erwähnt - zunächst auf externe Unterstützungsangebote gewartet haben. Sowohl interne Projekte als auch Angebote Dritter haben meist die Dora-Vorschriften mit den bestehenden BAIT-Anforderungen abgeglichen, den Umsetzungsstand erhoben, Lücken identifiziert und daraus Maßnahmen abgeleitet, die anschließend strukturiert in Projekten bearbeitet wurden. Das war vielerorts eine echte Sisyphusarbeit, die zahlreiche Bereiche betraf und weiterhin betrifft.

Dabei zeigt sich, dass es deutschen Instituten im Vergleich zu anderen Ländern oft schwerer fällt. Während man andernorts quasi auf der grünen Wiese beginnen kann, müssen hiesige Institute zunächst analysieren, in welchen Bereichen die bereits umgesetzten BAIT-Anforderungen für Dora nicht ausreichen.”

Norman Edelmann: ”Die Implementierung krisenkommunikativer Maßnahmen wird stets als Teil der Gesamtstrategie betrachtet, in der Umsetzung jedoch richtigerweise hintenangestellt. Dies ist schon deswegen geboten, weil die in den Kommunikationsrichtlinien enthaltenen Prozesse nahtlos ins gesamte Krisenmanagement integriert werden müssen. Nichtsdestotrotz ist Eile geboten, auch weil der Druck durch die Aufsicht, sich mit den Reputationsrisiken auseinanderzusetzen, groß ist.”

Wie unterstützen Sie die Institute? Wo erkennen Sie den höchsten Nachholbedarf?

Tino Nielsen: "Ganz allgemein unterstützen wir in vielen Bereichen wie z.B. der Durchführung interner Revisionen, Compliance-Checks und Vorbereitungen auf Sonderprüfungen.

Im Rahmen der Dora-Einführung haben wir insbesondere Genossenschaftsbanken in 70 bis 80 Implementierungsprojekten unterstützt. Angefangen bei der Identifizierung von Umsetzungslücken, bis hin zur Unterstützung bei der Umsetzung abgeleiteter Maßnahmen. Und das immer im engen Austausch mit unseren Kunden.

Gegenwärtig beraten wir Institute vielfach bei der Entwicklung von Notfallvorkehrungen oder auch der Erhebung des Umsetzungsstands bankindividueller Sicherheitsanforderungen.

Speziell in der genossenschaftlichen FinanzGruppe werden die Mitgliedsinstitute ergänzend durch zentrale Leistungen unterstützt. Dazu zählen z.B. die Bereitstellung von Leitfäden zur Strategieerstellung, Interpretationshilfen zu den Dora-Anforderungen und auch eine zentrale Dienstleistersteuerung. Seit kurzem wird das Modell zentraler Verfahrenslieferanten forciert."

Norman Edelmann: "Als Fachleute für Krisenkommunikation haben wir im Schulterschluss mit den Beraterinnen und Beratern der Awado ein Dora-konformes Krisenkommunikationshandbuch entwickelt, das Banken mit wenigen Handgriffen die Anpassung an das eigene Management erlaubt. Dieses Handbuch hilft dabei die regulatorischen Anforderungen zu erfüllen und bietet zugleich Mustermittelungen und Checklisten, die während der Krise helfen werden. Zugleich prüfen wir Krisenstäbe im Rahmen von Krisensimulation auf ihre Krisenresilienz, sodass die Organisation im Ernstfall handlungsfähig ist."

Was ist ein zentraler Verfahrenslieferant, und wie profitieren Institute der genossenschaftlichen FinanzGruppe davon?

Tino Nielsen: "Ein zentraler Verfahrenslieferant stellt für eine Vielzahl gleichartiger Institute, die ähnliche Leistungen beziehen, auf Basis anerkannter Verfahren und Werkzeuge Unterstützungsleistungen bereit. Dazu zählen Verfahrensbeschreibungen, Vorschläge für Schutzbedarfsfeststellungen, die Ableitung eines zentralen Sicherheitsanforderungskatalogs, allgemeine Risikobewertungen und ähnliches. Ansonsten müsste dies jedes Institut vollständig selbst machen. So obliegt es den Instituten insbesondere, die bereitgestellten Informationen und vorgelagerten Bewertungen zu validieren und zu individualisieren. Dies ist effizient.

Dies ist aber kein Allheilmittel. Aktuell sehen wir in den Bereichen Testen der digitalen operationalen Resilienz, dem IKT-Geschäftsfortführungsmanagement und der Überführung aller neuen Aktivitäten in den Regelbetrieb große Herausforderungen.”

Können Sie das Thema „Risiko-Orientierung“ noch einmal näher erläutern?

Verstehen wir das richtig - Dora verpflichtet die Finanzunternehmen zu weniger, als sie annehmen?

Tino Nielsen: ”Dora ermöglicht es, ihre Anforderungen risikoorientiert und damit verhältnismäßig umzusetzen. Art. 4 Dora stellt klar, dass Umfang und Tiefe der Maßnahmen u. a. von Größe, Risikoprofil und den angebotenen Dienstleistungen eines Instituts abhängen.

Ein Beispiel: Jedes Institut muss ein Testprogramm für die digitale operationale Resilienz entwickeln, um Schwachstellen in IKT-Systemen aufzudecken. Betreibt ein Institut jedoch ein vollständig physisch getrenntes Kunden-WLAN, ist das Risiko eines Schadens deutlich geringer als bei nur logisch getrennter Infrastruktur. Wenn dies nachvollziehbar dokumentiert wird, kann auf entsprechende Tests verzichtet werden.

Dieser Grundsatz lässt sich auf viele Dora-Vorschriften übertragen. Häufig fehlen jedoch Erfahrung, Mut oder eine saubere Herleitung - und Institute machen sich dadurch mehr Arbeit als nötig.

Das Prinzip ist nicht neu: Auch MaRisk und BAIT kennen diese ´doppelte Proportionalität´.”

Im Zusammenhang mit Dora war vor dem Inkrafttreten und ist immer noch viel vom Einsatz von Technologie die Rede, beispielsweise von KI und Robotic Process Automation. Inwiefern ist der Einsatz hilfreich? Und wenn er es ist, verfügen die Institute über die notwendige Kompetenz?

Norman Edelmann: ”Dora wird oft als Innovationsbremse wahrgenommen - dabei kann sie sogar Innovationsräume öffnen. In der Kommunikation kann sie beispielsweise zum Einsatz kommen, um Tonalitäten zu analysieren und die eigene Krisenkommunikation im laufenden Krisenprozess anzupassen. Dabei spielt DSGVO-Konformität und Datensicherheit - also das Arbeiten und Teilen von Daten in geschützten Umgebungen - natürlich genauso eine Rolle wie bei allen anderen relevanten KI-Projekten.”

Tino Nielsen: ”KI und RPA bieten gemeinsam große Effizienzpotenziale, und die Institute verfügen grundsätzlich über die nötigen Kompetenzen. Dennoch hakt die Digitalisierung oft - vor allem aus Sorge vor Datenschutzverstößen. Dem begegnen wir durch ein Rundum-Sorglos-Modell: Ein Partner stellt die technische Plattform, ein weiterer

übernimmt Konfiguration, Betriebskonzepte und Bündelung der Einkaufskraft. Ergänzt wird dies durch ein Rechtsgutachten zur DSGVO-Konformität sowie unseren Compliance-Check während der Einführung.

Im Kern geht es darum, Informationen aus Dokumenten auszulesen, strukturiert bereitzustellen und an Roboter zu übergeben, die standardisierte Prozessschritte ausführen - etwa bei Legitimationen, Freistellungsaufträgen oder Pfändungen. So steigern wir die Datenqualität und entlasten Mitarbeitende zugunsten anspruchsvollerer Aufgaben. Ganz im Sinne von: „Was einer alleine nicht schafft, das schaffen viele.“

Zu den Personen:

Norman Edelman ist Senior Manager der Awado Kommunikationsberatung mit Schwerpunkt Krisenkommunikation und Krisenprävention.

Tino Nielsen ist Senior Manager und Prokurist in der Awado GmbH Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft mit den Schwerpunkten Interne Revision IT und Compliance-Checks.