aba Arbeitsgemeinschaft für
betriebliche Altersversorgung e.V.

Bundesanstalt für Finanzdienstleistungsaufsicht
Versicherungs- und Pensionsfondsaufsicht
Graurheindorfer Straße 108
53117 Bonn

Per E-Mail an: Konsultation-17-21@bafin.de

030 3385811-0
info@aba-online.de

17.09.2021 ZA/SD

Konsultation 17/2021: Novellierung des Rundschreibens „Versicherungsaufsichtliche Anforderungen an die IT“ (VAIT) – aba-Stellungnahme

Sehr geehrte Damen und Herren,

wir bedanken uns für die Gelegenheit zur Stellungnahme zum Entwurf für eine Novellierung des VAIT-Rundschreibens 10/2018.

Die aba betrachtet die mit der vorgesehenen Überarbeitung des VAIT-Rundschreibens einhergehende Erhöhung der Anforderungen in Summe als problematisch in Bezug auf ihre Anwendung auf und Umsetzung in Einrichtungen der betrieblichen Altersversorgung (EbAV).

Bereits in unserer Stellungnahme anlässlich der Konsultation über die Erstfassung des VAIT-Rundschreibens haben wir im April 2018 darauf hingewiesen, dass sich die damalige Ausformulierung der versicherungsaufsichtlichen Anforderungen an die IT in ihrem Regelungsumfang und ihrer Regelungsdichte – trotz Proportionalitätsprinzip – unserem Eindruck nach in erster Linie an großen Versicherungsunternehmen mit weitreichenden Organisationsstrukturen, u.a. eigenständigen IT-Abteilungen, orientieren.

Die Größe und die interne Organisation der EbAV[1] sowie Art, Umfang und Komplexität ihrer Tätigkeiten unterscheiden sich u.E. erheblich von Finanzdienstleistungsunternehmen. So hat z.B. ein Teil der EbAV weder eigene Mitarbeiter noch eine eigenständig verwaltete IT-Infrastruktur. Diesen Unterschieden wurde im VAIT-Rundschreiben vom Juli 2018 leider nicht in angemessener Weise Rechnung getragen.

Die bisherigen Erfahrungen mit der Umsetzung haben die damaligen Befürchtungen bestätigt, dass der geforderte Gesamtaufwand für sehr viele EbAV erheblich ist und praxisnahe Lösungen einen hohen Ressourcenaufwand, insbesondere zur Dokumentation und Überwachung, verursachen.

[1] EbAV sind laut Richtlinie 2016/2341 über die Tätigkeiten und die Beaufsichtigung von Einrichtungen der betrieblichen Altersversorgung (sog. EbAV-II-RL) *„Altersversorgungseinrichtungen mit einem sozialen Zweck, die Finanzdienstleistungen erbringen. Sie sind für die Auszahlung von Leistungen der betrieblichen Altersversorgung verantwortlich und sollten deshalb bestimmte Mindestaufsichtsstandards bezüglich ihrer Tätigkeit und ihrer Betriebsbedingungen erfüllen, wobei sie nationalen Vorschriften und Gepflogenheiten Rechnung tragen sollten. Diese Einrichtungen sollten jedoch nicht wie reine Finanzdienstleister behandelt werden. Ihre soziale Funktion und die Dreiecksbeziehung zwischen dem Arbeitnehmer, dem Arbeitgeber und der EbAV sollten in angemessener Weise anerkannt und als grundlegende Prinzipien dieser Richtlinie gestärkt werden.“* (EW 32 EbAV-II-RL)

Wir befürchten, dass die vorgesehene Überarbeitung des VAIT-Rundschreibens dieses Grundproblem deutlich verschärfen wird und dies ohne Not:

- **EIOPA-Leitlinien für Versicherungsunternehmen**: Einen maßgeblichen Anteil für die drohende Verschärfung des Grundproblems sind die EIOPA-Leitlinien „zu Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologie“ (BoS-20/600). Diese werden in der Konsultationsankündigung als zentrale Begründung für die Überarbeitung bzw. als inhaltliche Vorlage für die Änderungen herangezogen. Allerdings entstammen sie der Regulierung von Versicherungsunternehmen (Solvency II). Dementsprechend weist EIOPA in ihren einleitenden Ausführungen („Hintergrund“, Ziffer 3) insbesondere auf die sich aus Art. 41 und 44 der Solvency II Richtlinie (RL 2009/138/EG) ergebende Verpflichtung von Versicherungsunternehmen hin, spezifische Leitlinien zu Fragen wie Risikomanagement, interne Kontrolle, interne Revision und gegebenenfalls Outsourcing auszuarbeiten.
- Diese Leitlinie nach Art. 16 EIOPA-Verordnung richtet sich an die BaFin und die beaufsichtigten Unternehmen im Hinblick auf Versicherungs- und Rückversicherungsunternehmen – nicht aber im Hinblick auf EbAV! Aus gutem Grund richtet sich EIOPA mit Erwartungen bezüglich der Beaufsichtigung von EbAV mit dem Instrument der *Stellungnahmen* gem. Art. 29 Abs. 1 EIOPA-VO 1094/2010 (ausschließlich) an die zuständigen Behörden in den Mitgliedstaaten (z.B. EIOPA-opinions on governance and risk management of pension funds von Juli 2019).

Die vorgenannten Themen (u.a. Risikomanagement, interne Kontrolle …) sind in der EbAV-II- Richtlinie den Besonderheiten von EbAV Rechnung tragend und in bestimmten Fragen (Outsourcing) auch detaillierter ausformuliert. Dies zeigt sich u.E. auch im BaFin-Rundschreiben MaGo für EbAV. Hier hat die BaFin erkennbar versucht, den Unterschieden von Lebensversicherungsunternehmen und EbAV und ihrer Vielfalt in der Ausgestaltung Rechnung zu tragen und den Unternehmen durch typische Beispiele die Umsetzung zu erleichtern.

Die in den EIOPA-Leitlinien formulierten Anforderungen an Versicherungsunternehmen sind u.E. auf viele EbAV, insbesondere kleine EbAV und Unternehmenseinrichtungen, nicht unterschiedslos übertragbar. Wie bereits in unserer Stellungnahme zu dem am 01.06.2021 in Kraft getretenen Rundschreiben MaGo für EbAV geäußert, haben wir auch hier Zweifel daran, ob die der Versicherungsregulierung entlehnte Vorstellung von Geschäftsorganisation, Berichtswegen und Verantwortlichkeiten noch mit dem Leitbild einer schlanken, effizienten Organisation einer EbAV vereinbar sein wird.

Die BaFin hat in der Meldung auf ihrer Homepage vom 28.06.2021 angekündigt, diese EIOPA-Leitlinien in ihrer Aufsichtspraxis anzuwenden. Gegenüber EIOPA hat die BaFin (über die EIOPA-Internet-Seite, wo neben dem Text der Guidelines auch die Tabelle mit den Antworten der BaFin in der Rubrik „Overview of replies and compliance tables“ veröffentlicht ist) gemeldet, dass sie alle neuen Leitlinieninhalte im Wege der Überarbeitung des VAIT-Rundschreibens voll umzusetzen gedenkt.

Ohne eine ausreichende Differenzierung zwischen Versicherungsunternehmen und EbAV droht durch die VAIT-Novelle unter dem Strich eine Fülle weiterer Anforderungen, die von vielen EbAV praktisch kaum erfüllt werden könnten. Es existieren Altersversorgungseinrichtungen, die in die IT-Strukturen ihrer Trägerunternehmen ganz oder teilweise eingebunden sind und daher keine eigenständige IT-Struktur haben. Diesen Einrichtungen droht ein hohes Maß an Rechtsunsicherheit und erheblicher Zusatzaufwand infolge der fehlenden Berücksichtigung der bereits bestehenden IT-Sicherheitsstandards der Trägerunternehmen. Durch die Fehlallokation begrenzter interner Ressourcen zur Umsetzung für diese Einrichtungen unangemessener VAIT-Anforderungen drohen auch Schäden, die letztlich von den Begünstigten in Form geringerer Altersversorgung zu tragen sind.

Ungeachtet des neu aufgenommenen Hinweises auf das für EbAV maßgebliche Proportionalitätsprinzip[2] sind die konkreten aufsichtsrechtlichen Erwartungen in vielen Konstellationen (z.B. EbAV ohne eigene Mitarbeiter oder EbAV, die die IT von Trägerunternehmen nutzen) nicht hinreichend klar bestimmbar.

Im Ergebnis sollte auch im Aufsichtsrecht der Grundsatz gelten, dass Unmögliches nicht verlangt werden kann. Das VAIT-Rundschreiben sollte daher so gefasst werden, dass die Anforderungen auch für EbAV unter Berücksichtigung ihrer Vielfalt in der Praxis umsetzbar sind.

Außerdem betrachten wir den Detaillierungsgrad bestimmter Anforderungen im Konsultationstext kritisch, etwa in Bezug auf die Position des im VAG nicht explizit geregelten Informationssicherheitsbeauftragten, dessen Position und Befugnisse im VAG gesetzlich nicht geregelt sind, und nun durch die VAIT-Novelle deutlich ausgebaut werden, und zwar in Richtung der einer gesetzlich geregelten Schlüsselfunktion.

- **Insgesamt bitten wir darum, bereits in der Vorbemerkung des Rundschreibens und, darauf aufbauend, auch in einzelnen Kapiteln, mehr EbAV-spezifische Ausführungen und Beispiele in das Rundschreiben aufzunehmen und andere, für EbAV nicht erfüllbare Anforderungen in der Formulierung entsprechend anzupassen. Hierzu finden Sie in der beiliegenden Tabelle konkrete Vorschläge, die wir gern mit Ihnen diskutieren möchten (Anlage).**
- **EbAV ohne eigene IT-Infrastruktur sollten sich darauf beschränken können, angemessene Ausgliederungsvereinbarungen zu schließen und im Weiteren das Outsourcing-Risiko gemäß den Bestimmungen des Kapitels 12 der MaGo für EbAV (und auch im Sinne des VAIT-Rundschreibens) angemessen zu steuern. Dabei sollten insbesondere vorhandene IT-Sicherheitsstandards der Trägerunternehmen angemessen anerkannt werden, um unverhältnismäßige und v.a. unnötige Zusatzaufwendungen zu vermeiden.**

In Bezug auf das Datum des Inkrafttretens der Überarbeitung empfehlen wir, eine ausreichend lange Umsetzungsfrist vorzusehen. Auf diese Weise sollen alle Unternehmen die Gelegenheit erhalten, ihre Prozesse und Strukturen an die neu in das VAIT-Rundschreiben aufgenommene und mit detaillierten Anforderungen hinterlegten Inhalte anzupassen, wie z.B. zum IT-Notfallmanagement.

Wir würden uns freuen, wenn Sie unsere Anliegen und Vorschläge zum Konsultationsentwurf des VAIT-Rundschreibens berücksichtigten würden. Für konstruktive Diskussionen und Rückfragen stehen wir Ihnen gern zur Verfügung.

Mit freundlichen Grüßen

aba Arbeitsgemeinschaft für
betriebliche Altersversorgung e.V.

[2] Konkretisiert durch die MaGo für EbAV; vgl. Fußnote 1 zur Vorbemerkung 6 im Konsultationsentwurf des VAIT-Rundschreibens