aba Arbeitsgemeinschaft für
betriebliche Altersversorgung e.V.

aba e.V. | Wilhelmstraße 138 | 10963 Berlin

Bundesanstalt für Finanzdienstleistungsaufsicht
Referat VA 36
Graurheindorfer Str. 108
D-53117 Bonn

Per Mail: Konsultation-04-18@bafin.de

info@aba-online.de

20.04.2018

aba-Stn: 008-BaFin-2018

Betreff: Stellungnahme der aba im Rahmen der Konsultation 04-2018
Geschäftszeichen: VA 36-I 2802-2018/0001

Sehr geehrte Damen und Herren,

zum Konsultationsentwurf für das Rundschreiben „Versicherungsaufsichtliche Anforderungen an die IT (VAIT)“ haben wir folgende Anmerkungen:

Der VAIT-Entwurf orientiert sich in seinem Regelungsumfang und seiner Regelungsdichte – trotz Proportionalitätsprinzip – u.E. an großen Versicherungsunternehmen mit weitreichenden Organisationsstrukturen, u.a. eigenständigen IT-Abteilungen. 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. Dieser Unterschied sollte in angemessener Weise in der VAIT berücksichtigt werden. Der VAIT-Entwurf ist u.E. noch weit von einem praxisnahen Rahmen für Altersversorgungseinrichtungen entfernt (siehe Ziff. 1 der Vorbemerkung).

Der geforderte Gesamtaufwand dürfte für sehr viele EbAV erheblich und unverhältnismäßig sein. Die VAIT sollten sich in Fällen von EbAV, die über keinerlei Angestellte verfügen, alle Funktionen und Versicherungstätigkeiten auf Spezialdienstleister ausgegliedert haben und daher natürlich auch nicht über eine eigene IT-Infrastruktur verfügen, darauf beschränken, versicherungsaufsichtliche Anforderungen an die technisch organisatorische Ausstattung und Prozesse der Funktionsausgliederungspartner dieser EbAV zu definieren, die in den entsprechenden Funktionsausgliederungsverträgen und dementsprechend konsequent in der Steuerung des Outsourcing-Risikos zu berücksichtigen wären. Zudem muss gewährleistet werden, dass Unternehmenseinrichtungen die IT des Trägerunternehmens weiterhin ohne unverhältnismäßige und v.a. unnötige Zusatzaufwendungen nutzen können. Wir schlagen hierzu konkret vor:

[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)

Vorbemerkung, TZ 7:

⇨ „Proportionalität wirkt sich darauf aus, wie Anforderungen erfüllt werden können. So können bei Unternehmen mit schwächer ausgeprägtem Risikoprofil – z.B. weniger komplexe Geschäftsmodelle wie bei Einrichtungen der betrieblichen Altersversorgung (EbAV) - einfachere Strukturen und Prozesse ausreichend sein. Umgekehrt kann das Proportionalitätsprinzip bei Unternehmen mit stärker ausgeprägtem Risikoprofil aufwändigere Strukturen und Prozesse erfordern. Bei der Beurteilung, wie Anforderungen erfüllt werden, kann auch eine beim Trägerunternehmen oder Dienstleister vorliegende Zertifizierung berücksichtigt werden."

Grundanliegen: Diese Ergänzungen könnten für mehr Sicherheit sowohl bei den Altersversorgungseinrichtungen als auch bei den Prüfern führen. Unnötiger Doppelaufwand würde verhindert und der Abstimmungsaufwand mit den Prüfern begrenzt.

3. Informationsrisikomanagement, TZ 23, rechte Spalte:

⇨ „IT-Risikokriterien enthalten bspw. mögliche Bedrohungen, das Schadenspotenzial, die Schadenshäufigkeit sowie den Risikoappetit.
Die Risikoanalyse kann u. a. auch auf Grundlage eines Vergleichs der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen und im Rahmen der (im Unternehmen etablierten) Risikomanagements ~~zu~~ erfolgen."

Grundanliegen: Ergänzung zur Klarstellung, dass hier kein eigenständiges Informationsrisikomanagement aufgebaut werden muss.

8. Ausgliederungen von IT-Dienstleistungen (…), TZ 66, rechte Spalte:

⇨ „Art und Umfang einer Risikoanalyse kann das Unternehmen unter Proportionalitätsgesichtspunkten festlegen. Z.B. kann aufgrund vorliegender Zertifizierungsnachweise von Trägerunternehmen oder Dienstleistern eine vereinfachte Risikoanalyse ausreichend sein".

Grundanliegen: Beim Bezug von IT von Trägerunternehmen und/oder Dienstleister, die bspw. eine ISO 27001 Zertifizierung nachweisen, sollte sich u.E. der Prüf- und Dokumentationsaufwand für die EbAV deutlich reduzieren. Eine Doppelung von Dokumentation, Prüfungen und Aufwendungen sollte durch Anerkennung vorhandener ISO-Zertifizierung der Trägerunternehmen und Dienstleister vermieden werden. Unter Ziff. 5 der Vorbemerkung wird im VAIT-Konsultationsentwurf gefordert, „bei der Ausgestaltung der IT-Systeme (Hardware- und Software-Komponenten) und der dazugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. …"

Mit freundlichen Grüßen

aba Arbeitsgemeinschaft für
betriebliche Altersversorgung e.V.

(Klaus Stiefermann, Geschäftsführer) (Dr. Cornelia Schmid)

aba Arbeitsgemeinschaft für betriebliche Altersversorgung e.V. Wilhelmstraße 138, 10963 Berlin
Telefon: 030 33 858 11-0 ▪ Fax: 030 33 858 11-21 ▪ info@aba-online.de ▪ www.aba-online.de

Vertretungsberechtigter Vorstand: Heribert Karch (Vorsitzender), Joachim Schwind (stellv. Vorsitzender), Dr. Georg Thurnes (stellv. Vorsitzender)
Registergericht: Amtsgericht Charlottenburg (Berlin) ▪ Registernummer: VR 32127 B ▪ Umsatzsteuer-Identifikationsnummer: DE 143293297