Bundesverband Deutscher
Kapitalbeteiligungsgesellschaften

Bundesanstalt für Finanzdienstleistungsaufsicht
[redacted]
Referat WA 46 - Investmentaufsicht
Marie-Curie-Straße 24-28
60439 Frankfurt am Main

16.05.2019

Stellungnahme „Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT)"

Sehr geehrte [redacted],

anbei übersende ich Ihnen als stellvertretende Geschäftsführerin des Bundesverbandes Deutscher Kapitalbeteiligungsgesellschaften BVK folgende Stellungnahme unseres Rechtsbeirates, Vorsitz Dr. Andreas Rodin, P+P Pöllath & Partners, zur Konsultation des Entwurfes des Rundschreibens „Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT)" mit der freundlichen Bitte um Kenntnisnahme.

Anmerkungen P+P zur Konsultation 07/2019 (KAIT):

Grundsätzlich ist es zwar wichtig, IT-sicherheitsrechtliche Belange auch für Kapitalverwaltungsgesellschaften in den Fokus zu rücken. Die genaue Ausgestaltung der Anforderungen nach dem Entwurf bleibt häufig aber unklar, d.h. die Formulierungen sind sehr weit und gleichzeitig unbestimmt. Bei der Umsetzung der KAIT nach dem Entwurf des Rundschreibens würde es daher u.E. zu Unsicherheit kommen, was genau in welchem Maße gefordert ist.

Bundesverband Deutscher
Kapitalbeteiligungsgesellschaften –
German Private Equity and Venture
Capital Association e.V. (BVK)

Residenz am Deutschen Theater
Reinhardtstraße 29 b
10117 Berlin
Telefon +49 30 306982-0
Telefax +49 30 306982-20
bvk@bvkap.de
www.bvkap.de

Deutsche Bank AG
IBAN DE34 1007 0024 0012 1251 00
BIC DEUTDEDBBER
Commerzbank AG
IBAN DE81 1008 0000 0930 1100 00
BIC DRESDEFF100

Sitz/Vereinsregister
Berlin, Amtsgericht
Charlottenburg 9378 NZ

Geschäftsführendes Vorstandsmitglied:
Ulrike Hinrichs

Im Einzelnen:

1. IT-Strategie (S. 6):

- Die Geschäftsleitung soll eine nachhaltige IT-Strategie festlegen, hierfür werden Mindestinhalte für die IT-Strategie vorgegeben. Es ist zunächst nach Nr. 2 (a) für die strategische Entwicklung der IT-Aufbau und IT-Ablauforganisation der KVG sowie der Auslagerung von IT-Dienstleistern Sorge zu tragen. Gemeint ist hiermit die Beschreibung der Rolle, der Positionierung und des Selbstverständnisses der IT im Hinblick auf Personaleinsatz und Budget der IT-Aufbau und IT-Ablauforganisation sowie die Darstellung und strategische Einordnung der IT-Dienstleistungen. Ebenso wird die strategische Entwicklung der IT-Architektur gefordert (Nr. 2 (d)), wonach die Darstellung des Zielbilds der IT-Architektur in Form eines Überblicks über die Anwendungslandschaft gemeint ist. **à Anmerkung**: Nicht deutlich wird, worin der genaue Unterschied zu Nr. 2 (a) besteht, da im Rahmen der Aufbau und Ablauforganisation auch die entsprechenden Anwendungsbereiche festgelegt werden (müssen).

- Zudem sollen nach Nr. 2 (e) / (f) Aussagen zum Notfallmanagement unter Berücksichtigung der IT-Belange und Aussagen zu den in den Fachbereichen selbst betriebenen bzw. entwickelten IT-Systemen erbracht werden. **à Anmerkung**: Welche Art von Aussagen getroffen werden und welchen Zweck diese Aussagen mit sich bringen sollen bleibt gänzlich unklar, an Erläuterungen (wie bei den anderen Buchstaben) fehlt es hier.

2. IT-Governance (S. 9):

- Zur Steuerung sowie Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme soll die KVG unter anderem sicherstellen, dass die IT-bezogenen Geschäftsaktivitäten auf der Grundlage von Arbeitsablaufbeschreibungen (Organisationsrichtlinien) betrieben werden. **à Anmerkung**: Die Anforderung an den Entwurf eines Richtlinienkatalogs scheint überzogen, insbesondere weil die KVG angehalten ist, geeignete Ablaufprozesse festzulegen. Hierbei sollte nach m.E. aber ein gewisser Spielraum verbleiben, um den Arbeitsaufwand nicht unnötig zu erhöhen.

3. Informationsrisikomanagement (S. 11):

- Die Informationsverarbeitung und -weitergabe in Geschäfts- und Serviceprozessen wird typischerweise durch datenverarbeitende IT-Systeme unterstützt. Daher sollen insbesondere IT-Risikokriterien und der notwendige Schutzbedarf festgelegt werden. Auch hierfür wird gefordert, dass ein sog. Sollmaßnahmekatalog zur Umsetzung der Schutzziele und Dokumentation des Schutzbedarfs bereitgestellt werden soll. **à Anmerkung**: Wie bei den Organisationsrichtlinien scheint auch hier die Anfertigung eines Sollmaßnahmekatalog etwas zu weitgehend, da es vermutlich nicht für jedes IT-Risiko von der KVG vorher festgelegte Schutzmaßnahmen geben kann. Zudem ist in bestimmten (IT-Risiko-) Situationen auch ein gewisser Spielraum nötig, der durch die Festlegung eines Sollmaßnahmekatalog zur Inflexibilität führen kann.

- Für das Informationsrisikomanagement soll die Geschäftsleitung angehalten werden, mindestens vierteljährlich einen Risikostatusbericht zu erstellen. **à Anmerkung**: Das geforderte Intervall bedeutet enormen Arbeitsaufwand und bleibt hinter dem nicht deutlich werdenden Sinn und Zweck einer so häufigen Berichterstattung zurück. Eine (halb-)jährliche Revision des Informationsrisikomanagements erscheint ausreichend.

4. Informationssicherheitsmanagement (S. 12):

- Zur Informationssicherheit sollen Prozesse definiert und deren Umsetzung gesteuert werden. Hierzu sollen wiederum zusätzlich Informationssicherheitsrichtlinien festgelegt werden. **à Anmerkung**: Nicht ganz klar wird hierbei, inwieweit diese Informationssicherheitsrichtlinien einen Mehrwert im Verhältnis zu den schon geforderten Organisationsrichtlinien und dem Sollmaßnahmekatalog darstellen. Es kommt zu inhaltlichen Überschneidungen in den jeweiligen Dokumenten. Sinnvoller erscheint es daher, ein einzelnes Dokument zur IT-Sicherheit zu erstellen.

Bundesverband Deutscher
Kapitalbeteiligungsgesellschaften

- Zudem soll ein Informationssicherheitsbeauftragter eingesetzt werden. **à Anmerkung**: Die Schaffung einer neuen Position als Informationssicherheitsbeauftragter kann ggf. mit größeren Kosten verbunden sein; der Nutzen einer solchen (grundsätzlich intern zu schaffenden Position) erscheint aber nicht klar, da die Geschäftsleitung der KVG insgesamt für die Informationssicherheit verantwortlich ist. Auch wird eine Berichterstattung des Informationssicherheitsbeauftragten an die Geschäftsleitung mit dem Intervall von mindestens vierteljährlicher Berichterstattung festgelegt, wobei auch hier die Notwendigkeit einer so häufigen Berichterstattung unklar bleibt.

Mit freundlichen Grüßen

Swantje Freifrau von Massenbach
stellv. Geschäftsführerin BVK
Leiterin politische Kommunikation