BankingGuide GmbH

BankingGuide ZV auf der VP

Arbeitshilfe zur Einschätzung des Tools hinsichtlich:

- MaRisk AT 8.1
- MaRisk AT 8.2
- MaRisk AT 9
- Datenschutzgrundverordnung – Art. 6 Absatz 1 a, f
- IT-Sicherheit

Stand: April 2021

Inhaltsverzeichnis

1 Ziel dieser Unterlage

Mit der vorliegenden Einschätzung des BankingGuide auf der Vertriebsplattform hinsichtlich:

- MaRisk AT 8.1,
- MaRisk AT 8.2,
- MaRisk AT 9,
- Datenschutzgrundverordnung – Art. 6 Absatz 1 a, f sowie
- IT-Sicherheit

erhalten Sie nachfolgend, im Rahmen der Einführung der Anwendung „BankingGuide“, eine Hilfestellung für den Umgang mit den o.g. Rechtsvorschriften in Ihrem Haus.

Bei dieser Hilfestellung handelt es sich um die Einschätzung anderer Volksbanken Raiffeisenbanken. Daher muss - **unabhängig von dieser Unterlage** - von Ihnen eigenverantwortlich entschieden werden welche Einschätzung Sie für Ihr Haus vornehmen. Diese Unterlage dient lediglich der Orientierung und ist rechtlich nicht bindend.

Aus diesem Grund wird seitens des Erstellers für die nachfolgenden Darstellungen keine Haftung gegenüber Dritten übernommen.

2 MaRisk AT 8.1

Die MaRisk AT 8.1 verlangt von einem Kreditinstitut, dass dieses die „von ihm betriebenen Geschäftsaktivitäten versteht. Für die Aufnahme von Geschäftsaktivitäten in neuen Produkten oder auf neuen Märkten (einschließlich neuer Vertriebswege) ist vorab ein Konzept auszuarbeiten."

Das Vorliegen neuer Geschäftsaktivitäten in neuen Produkten oder auf neuen Märkten (einschließlich neuer Vertriebswege) bei der Einführung des BankingGuide wurde anhand der nachfolgenden Kriterien geprüft:

- □ Es wurden bisher vergleichbare Geschäfte über vergleichbare Vertriebskanäle getätigt
- □ Die bisherige Tätigkeit bezieht sich auf vergleichbare Märkte bzw. Branchen
- □ Es sind keine auf dieses Produkt bezogene Ausführungen in den MaRisk-Dokumentationen festgelegt
- □ Die fachliche Qualifikation im Rahmen der erforderlichen Tätigkeiten ist in der vorhandenen Organisationseinheit vorhanden
- □ Die Methoden zur Messung, Steuerung, Überwachung und Analyse der aus diesem Produkt abzuleitenden Risiken sind festgelegt
- □ Die Methoden zur Bewertung und Bilanzierung sind festgelegt
- □ Die korrekte dv-technische Abbildung (IT-Prozesse und -systeme) ist gesichert
- □ Die bestehenden Kundenverträge und -rahmenverträge sind geeignet und anwendbar

Einschätzung

Der BankingGuide ist gemäß der o.g. Checkliste nebst der Definition in den MaRisk AT 8.1 eine neue „Geschäftsaktivität", da dieser einen neuen Vertriebskanal bedient. Die Bank nutzt zwar bereits die „Vertriebsplattform" der Fiducia & GAD als Vertriebskanal, dennoch wird die Durchführung eines Neu-Produkt-Prozesses empfohlen, da die Nutzung der Vertriebsplattform auf einen neuen fachlichen Bereich (ZV-Beratung) ausgeweitet wird.

Beiliegend finden Sie das Muster eines NPP inkl. Verweise auf die Risikobewertung sowie den Link zum Leitfaden des BankingGuide.

3 MaRisk AT 8.2

Die MaRisk AT 8.2 besagen, dass vor wesentlichen Veränderungen in der Aufbau- und Ablauforganisation sowie in den IT-Systemen das Institut die Auswirkungen der geplanten Veränderungen auf die Kontrollverfahren und die Kontrollintensität zu analysieren hat.

Es ist demnach zu prüfen, ob es sich bei der Einführung des BankingGuide um eine **wesentliche** Veränderung in den IT-Systemen handelt. Zur Beurteilung der Wesentlichkeit wurden die folgenden Kriterien herangezogen:

- □ Besteht ein Zusammenhang zu wesentlichen Geschäftsprozessen?
- □ Sind die Auswirkungen der Veränderung nicht ohne Weiteres abschätzbar (z.B. bereichsübergreifend)?
- □ Sind umfangreiche Schulungsmaßnahmen erforderlich?
- □ Bedarf die Veränderung eines großen Vorlaufs in der Vorbereitung?
- □ Besteht ein hoher Projektaufwand (Ressourcen, Kosten)?
- □ Besteht die Notwendigkeit einer externen Unterstützung?
- □ Haben die Veränderungen der IT-Systeme einen hohen Umfang und erhebliche Auswirkungen auf die betroffenen Geschäftsprozesse?

Einschätzung

Gemäß der o.g. Checkliste handelt es sich beim BankingGuide um keine wesentliche Veränderung in der Aufbau- und Ablauforganisation sowie in den IT-Systemen, da sämtliche Fragestellungen bereits im Rahmen der Einführung der Vertriebsplattform beantwortet und berücksichtigt wurden und der BankingGuide lediglich eine Anwendung auf der bereits geschaffenen Infrastruktur darstellt.

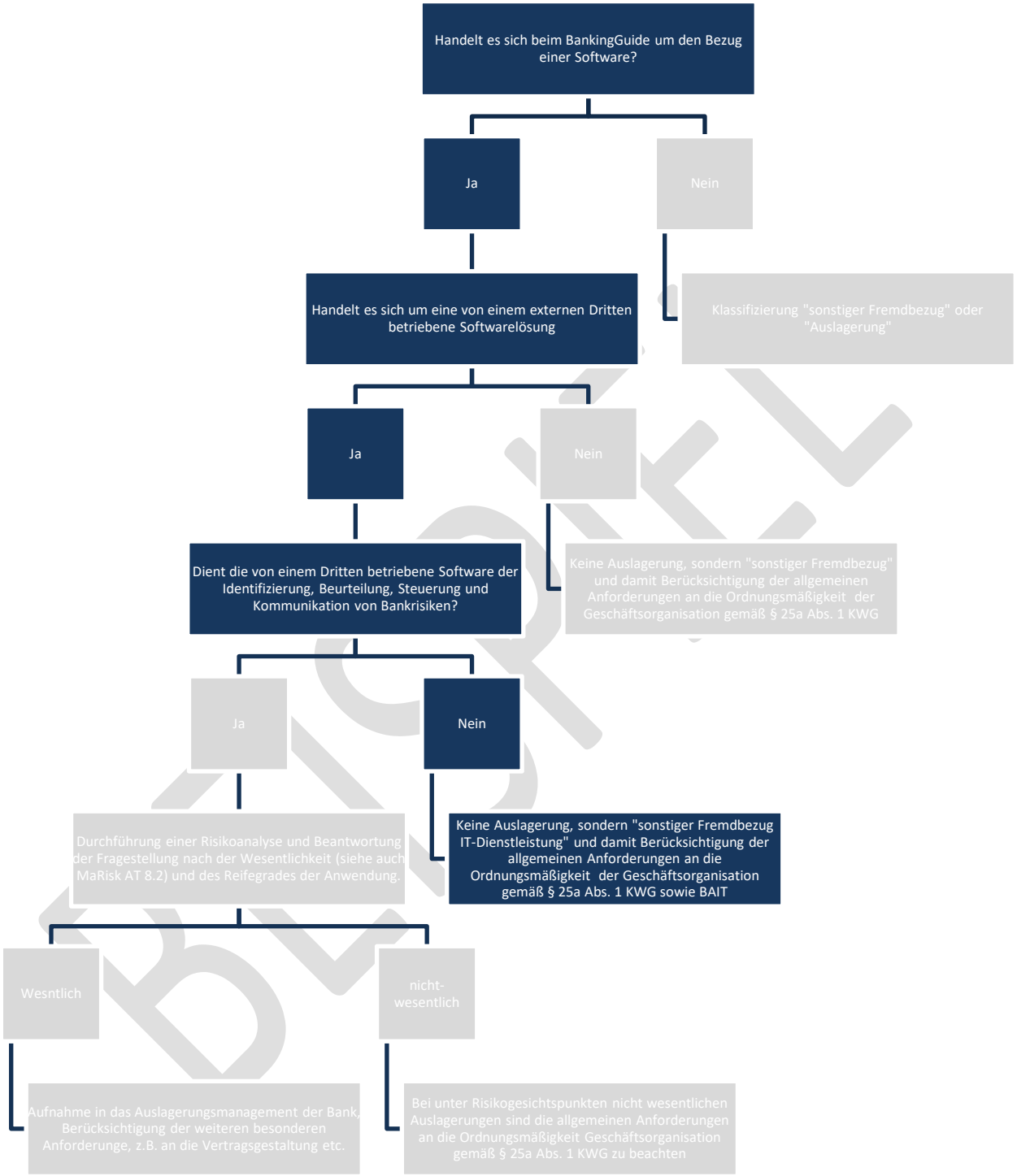
4 MaRisk AT 9

Die Aufsicht hat mit den Änderungen zur 5. Novelle im Oktober 2017 in Modul AT 9 eine Klarstellung der aufsichtsrechtlichen Praxis geschaffen, aber auch Grenzen der Auslagerbarkeit verdeutlicht:

Quelle:
https://tme-ag.de/wp-content/uploads/2018/11/AT9_%C3%84nderungen-%C3%9Cberblick-01.jpg

Auslagerungen werden seitdem klarer als in der Vergangenheit definiert und abgegrenzt. Eine weitere Neuerung betrifft die sogenannte fremdbezogene Software. Der isolierte Bezug von Software, einschließlich zugehöriger Unterstützungsleistungen, ist regelmäßig als sonstiger Fremdbezug zu klassifizieren. Dies gilt nicht für Software zum Risikomanagement und für Software mit wesentlicher Bedeutung für bankgeschäftliche Aufgaben; hier sind Unterstützungsleistungen in der Regel als Auslagerung anzusehen. Gleiches gilt für den Betrieb dieser Software durch Dritte.

Zu klären ist, ob es sich bei der Nutzung des BankingGuide um eine Auslagerung im Sinne von AT 9 Tz. 1 MaRisk handelt und ob diese unter Risikogesichtspunkten „wesentlich" ist. Daraus ergeben sich Implikationen für den Umfang der Risikoanalyse durch die Bank. Die Prüfung wurde in folgender Struktur vorgenommen (dunkelblauer Verlauf):



Einschätzung

Der BankingGuide wird als „sonstiger Fremdbezug IT-Dienstleitung“ eingestuft. Es handelt sich bei der Anwendung um eine Software, welche von einem Dritten (BankingGuide GmbH in Ver-

bindung mit der Fiducia & GAD) betrieben wird. Es sind keine bankrisikorelevanten Handlungsfelder in Verbindung mit der Software betroffen. Auch die Wesentlichkeit (vergleiche Ausführungen zu MaRisk AT 8.2) ist nicht gegeben.

Hinsichtlich der Erfordernisse des §25a Abs. 1 KWG sowie BAIT finden Sie beiliegend folgende Unterlagen:

- IT-Sicherheitskonzept BankingGuide
- Arbeitshilfe Risikobewertung Fremdbezug von IT-Dienstleistungen

5 Datenschutzgrundverordnung – Art. 6 Absatz 1 a, f

Artikel 6 der DSGVO beschäftigt sich mit der „Rechtmäßigkeit der Verarbeitung“. Die beiden relevanten Ziffern des Absatzes 1 besagen demnach folgendes:

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

1. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

2. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

3. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

4. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

5. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

6. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Einschätzung

Die Verarbeitung der personenbezogenen Daten durch den BankingGuide erfolgt ausschließlich auf der Vertriebsplattform der Fiducia & GAD. Externe haben, analog sämtlicher anderer Daten auf der Vertriebsplattform, keinen Zugriff auf die personenbezogenen Daten. Im Rahmen von Fernwartungen können Kundendaten sichtbar sein. Diesbezüglich wird eine Fernwartungsvereinbarung gem. Art. 28 Abs. 3 DSGVO mit der BankingGuide GmbH geschlossen.

Der Zugriff auf den BankingGuide erfolgt ausschließlich aus der Beratungsanwendung Kunden-Beziehungs-Management (KBM) auf der Vertriebsplattform heraus. Im Rahmen dieser Anwendung erteilt der Kunde die Einverständniserklärungen für die Beratung. Dies erfolgt zum derzeitigen Zeitpunkt (Stand 04.2021) durch einen mündlichen Beratungsvertrag. Perspektivisch soll dieser mündliche Beratungsvertrag durch eine schriftliche / elektronische Lösung der Vertriebsplattform oder KBM abgelöst werden, worunter dann wiederum auch der BankingGuide subsummiert wird.

6 IT-Sicherheit

Die BankingGuide GmbH als Betreiberin der Anwendung BankingGuide und hat diverse IT-Sicherheitsmaßnahmen umgesetzt, welche im IT-Sicherheitskonzept detailliert beschrieben sind. Viele dieser Sicherheitsmaßnahmen beziehen sich auf die Vertriebsplattform, welche vom BankingGuide genutzt wird. Ein Verweis auf das IT-Sicherheitskonzept der Vertriebsplattform ist aus diesem Grund im IT-Sicherheitskonzept des BankingGuide enthalten.

BankingGuide GmbH