



BankingGuide

GmbH

BankingGuide ZV auf der OKP

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

Inhaltsverzeichnis

1	Ziel dieser Unterlage	1
2	MaRisk AT 8.1.....	2
3	MaRisk AT 8.2.....	3
4	MaRisk AT 9.....	4
5	Datenschutzgrundverordnung – Art. 6 Absatz 1 a, f	7
6	IT-Sicherheit	9

1 Ziel dieser Unterlage

Mit der vorliegenden Einschätzung der im VR Payment-Leistungspakets enthaltenen Anwendungen 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, 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 der (Kundenselbst-)Beratungsanwendungen 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

Die (Kundenselbst-)Beratungsanwendungen des VR Payment-Leistungspakets sind gemäß der o.g. Checkliste nebst der Definition in den MaRisk AT 8.1 eine neue „Geschäftsaktivität“, da diese einen neuen Vertriebskanal bedienen. Insbesondere gilt dies für die Kundenselbstberatung und den darauffolgenden Produktabschluss im Online-Banking (z.B. im Basis-Modul „Kundenselbstberatungslösung zum Abschluss von VR Pay Kompakt-Lösungen im Online-Banking“). Die Bank nutzt zwar die #webbank von VR-NetWorld sowie den BankingWorkspace und das Online-Banking von ATRUVIA als Vertriebskanal, dennoch wird die Durchführung eines Neu-Produkt-Prozesses empfohlen, da die Nutzung der genannten Plattformen um den Bereich „Kundenselbstberatung und -abschluss“ ausgeweitet wird.

Beiliegend finden Sie das Muster eines NPP inkl. Verweise auf die Risikobewertung. Weitere Informationen zu den Lösungen finden Sie in der in der Anwenderdokumentation „Self-Services für Firmenkunden mit BankingGuide Express“ im ATRUVIA Hub.

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 der Lösungen des VR Payment-Leistungspakets 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 bei den Lösungen des VR Payment-Leistungspakets um keine wesentliche Veränderung in der Aufbau- und Ablauforganisation sowie in den IT-Systemen, da sämtliche obenstehenden Fragestellungen bereits im Rahmen der Einführung der jeweiligen Plattformen (#webbank, Online-Banking, BankingWorkspace) beantwortet und berücksichtigt wurden und die Lösungen des Pakets lediglich Anwendungen auf der bereits geschaffenen Infrastruktur darstellen.

4 MaRisk AT 9

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

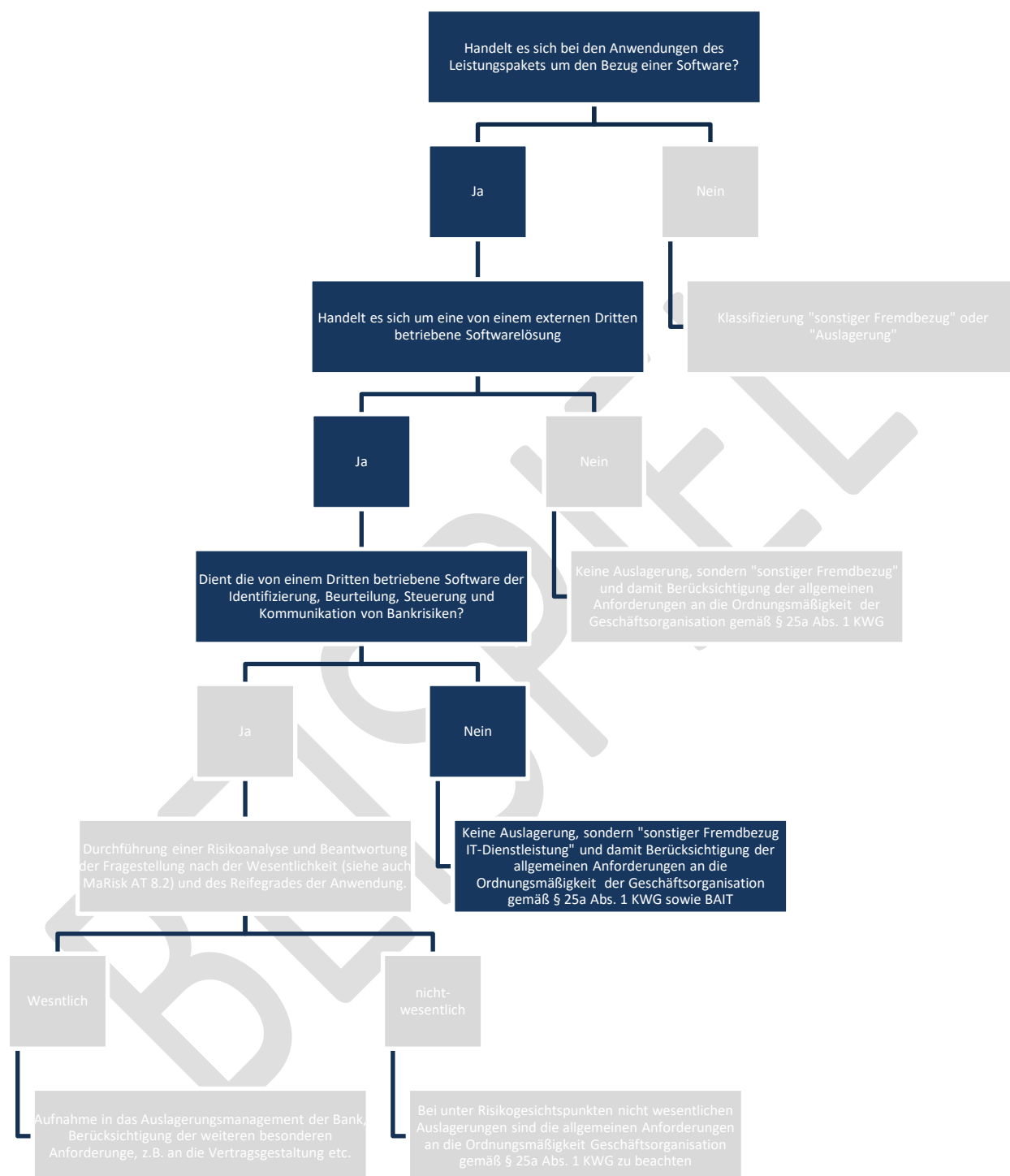
AT 9 Tz. 1	AT 9 Tz. 2	AT 9 Tz. 4, 5	AT 9 Tz. 6	AT 9 Tz. 8	AT 9 Tz. 12, 13
Auslagerungsdefinition; Abgrenzung „sonstiger Fremdbezug“	Risikoanalyse; Prüfung auf Wesentlichkeit	Auslagerbarkeit von Aktivitäten und Prozessen von Kontroll- und Kernbankbereichen	Neu: Ausstiegsstrategien bzw. Ausstiegsprozesse	Neu: Konkrete Vorgaben zu Weiterverlagerungen	Neu: Einrichtung eines zentralen Auslagerungsmanagements (ZAM)
Konkretisierung der Auslagerungsdefinition	Standardisierung der Risikoanalyse	Auslagerung Compliance- und Risikocontrolling / IR	Verabschiedung von Ausstiegsstrategien	Verankerung von Vorgaben in Auslagerungsverträgen	Einrichtung ZAM
Fremdbezogene Software und die ergänzende Unterstützungsleistung die zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation von Risiken genutzt wird, ist künftig als Auslagerung zu behandeln.	Die Risikoanalyse soll auf Basis gruppen- oder konzernweit gültiger Vorgaben regelmäßig als auch anlassbezogen durchgeführt werden.	Risikocontrolling und Kernbankbereiche sind unter Auflagen nun auslagerbar. Vor allem muss der ordnungsgemäße Betrieb auch im Falle einer Beendigung der Auslagerung gewährleistet sein (siehe auch AT 9 Tz. 6).	Für den Fall der beabsichtigten oder erwarteten sowie für die unbeabsichtigte und unerwartete Beendigung hat das Institut Ausstiegsstrategien festzulegen, zu verabschieden und diese zu überprüfen.	Weiterverlagerungsmodalitäten für das Auslagerungsunternehmen mit Subdienstleistern sind im Auslagerungsvertrag festzuhalten oder müssen zumindest mit diesem in Einklang stehen.	Institute haben ein ZAM mit entsprechenden Kontroll- und Überwachungsprozessen einzurichten. Das ZAM hat mindestens einmal jährlich an die Geschäftsleitung zu reporten.

Quelle:

https://tme-aq.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 der Lösungen des Leistungspakets um eine Auslagerung im Sinne von AT 9 Tz. 1 MaRisk handelt und ob diese unter Risikogesichtspunkten „wesentlich“ sind. Daraus ergeben sich Implikationen für den Umfang der Risikoanalyse durch die Bank. Die Prüfung wurde in folgender Struktur vorgenommen (dunkelblauer Verlauf):



Einschätzung

Die Anwendungen des Leistungspakets werden als „sonstiger Fremdbezug IT-Dienstleistung“ eingestuft. Die Anwendungen wurden auf Grundlage einer Software-Beratungstechnologie (BankingGuide) entwickelt, welche von einem Dritten (BankingGuide GmbH in Verbindung mit

der Atruvia AG) 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

BEISPIEL

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 die Anwendungen des Leistungspakets erfolgt – vor Abschluss der Bestellung in den folgenden gesicherten Bereichen

- Homepage (#webbank) der VR-NetWorld GmbH
- Online-Banking von ATRUVIA
- BankingWorkspace von ATRUVIA

Bank-Externe haben zu diesem Zeitpunkt 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.

Nach Bestellung einer Produktlösung, welche der Kunden per TAN und pflichtmäßiger Zustimmung zum untenstehenden Hinweistext (siehe Screenshot unten) ...

- ☐ Ich stimme hiermit zu, dass die VR Payment meine Daten von der Volksbank Test zum Zweck der Datenverarbeitung transformieren darf. Mir ist bewusst, dass diese Zustimmung freiwillig ist und ich sie jederzeit für die Zukunft widerrufen kann.

... bestätigt, werden die personenbezogenen Daten an die VR Payment GmbH per API-Schnittstelle weitergeleitet. Die Datenweiterleitung erfolgt gem. des oben genannten Punktes 2 gem. der Inhalte des Artikel 6 DSGVO.

BESPIEL

6 IT-Sicherheit

Die BankingGuide GmbH als Betreiberin der Anwendungen des Leistungspakets hat diverse IT-Sicherheitsmaßnahmen umgesetzt, welche im IT-Sicherheitskonzept detailliert beschrieben sind. Viele dieser Sicherheitsmaßnahmen beziehen sich auf die oben bereits mehrmals genannten Plattformen (#webbank, Online-Banking, BankingWorkspace, VR Payment Betriebssysteme), welche von den Anwendungen des Leistungspakets genutzt werden. Hinweise und Referenzen zu den IT-Sicherheitsstandards der genannten Plattformen und Systeme sind aus diesem Grund im IT-Sicherheitskonzept des Leistungspakets enthalten.

BEISPIEL

