

FINMA Rundschreiben 2018/3 Outsourcing

Zugestellt am: 01.04.2025

An: Baumer AG
Herr Daniel Jud, Lic. Oec. HSG – Geschäftsführer, VR Delegierter
Betreff: Einhaltung FINMA Rundschreiben durch die Baumer AG

Inhaltsverzeichnis

FINMA Rundschreiben 2018/3 Outsourcing	1
A. Management Summary	1
B. Auftrag	2
C. Ergebnis	2
1. Ausgangslage	2
2. Anwendbarkeit des FINMA-Rundschreibens 2018/3	3
3. Zulässigkeit des Outsourcings	3
4. Anforderungen und GoodPriv@cy®	3
5. Prüfung und Aufsicht	3
6. Rolle der SQS-Zertifizierungen bei der Prüfung	3
D. Fazit	4

A. Management Summary

Die Baumer AG ist nach den international anerkannten Zertifizierungen ISO 9001, ISO 27001 und GoodPriv@cy® zertifiziert.

Die Erfüllung der Anforderungen von ISO 9001, ISO 27001 und GoodPriv@cy®, deren Kernelemente der Betrieb eines den anerkannten Grundsätzen des Qualitätsmanagements entsprechenden Qualitätsmanagementsystems (QMS), Informationssicherheitsmanagementsystems (ISMS) sowie Datenschutzmanagementsystems (DSMS) sind, wird regelmässig durch die Schweizerische Vereinigung für Qualitäts- und Managementsysteme (SQS) überprüft. Diese ist durch die Schweizerische Akkreditierungsstelle SAS für die Zertifizierung von Qualitäts-, Informationssicherheits- und Datenschutz-Managementsystemen akkreditiert.

Mit der Zertifizierung auf der Grundlage von ISO 9001, ISO 27001 und GoodPriv@cy® erfüllt die Baumer AG die Anforderungen an einen Dienstleister gemäss FINMA-Rundschreiben 2018/3 "Outsourcing", insbesondere anlehnd an die frühere Praxis. Dies

umfasst insbesondere die Bereiche systematische Kontrolle, Informationssicherheit und Notfallkonzepte zur Geschäftskontinuität.

Die internen und externen Prüfstellen der auslagernden Unternehmen können die Tätigkeit der Schweizerischen Vereinigung für Qualitäts- und Managementsysteme (SQS) beziehen. Die fachspezifische Tiefe dieser Zertifizierungsprüfungen ermöglicht es der Prüfgesellschaft des auslagernden Unternehmens, ihre eigenen Prüfungshandlungen auf ergänzende Aspekte zu fokussieren und so eine fachlich fundierte, aber ressourcen-effiziente Gesamtprüfung sicherzustellen.

Wie weit die von den auslagernden Unternehmen mit der Baumer AG abgeschlossenen Verträge den Anforderungen des FINMA-Rundschreibens 2018/3 entsprechen, wurde im Rahmen der vorliegenden Abklärungen nicht überprüft. Es wird aber davon ausgegangen, dass sowohl die unternehmensinternen Voraussetzungen für ein Outsourcing gegeben sind und die vertraglichen Vereinbarungen den Anforderungen entsprechen.

B. Auftrag

Der Auftrag umfasst das Aktualisieren einer Beurteilung der Belser Datenschutz GmbH vom 07.03.2012 auf das aktuelle FINMA-Rundschreiben 2018/3 "Outsourcing".

In der Beurteilung wird darauf eingegangen, inwieweit die Baumer AG die Anforderungen des aktuellen FINMA-Rundschreibens 2018/3 "Outsourcing" erfüllt, und insbesondere die Klärung der Frage, welche Bedeutung die bestehende GoodPriv@cy®-Zertifizierungen für die Erfüllung der Prüfungsanforderungen hat.¹

C. Ergebnis

1. Ausgangslage

Das FINMA-Rundschreiben 2018/3 legt dieaufsichtsrechtlichen Anforderungen an Outsourcing-Lösungen von Banken, Versicherungsunternehmen und bestimmten Finanzinstituten nach FINIG fest. Dabei werden die verschiedenen Voraussetzungen beschrieben, welche durch die auslagernden Unternehmen erfüllt sein müssen, damit ein Outsourcing zulässig ist. Dies betrifft insbesondere die Sorgfaltspflicht bei der Auswahl des Dienstleisters, die Ausgestaltung des Outsourcing-Vertrages, die kontinuierliche Kontrolle sowie die Gewährleistung einer angemessenen Aufsicht. Es wird davon ausgegangen, dass seitens der auslagernden Unternehmen sämtliche Anforderungen an das Outsourcing an die Baumer AG erfüllt werden. Die nachfolgenden Ausführungen konzentrieren sich auf die Erfüllung der Anforderungen an den Dienstleister.

¹ Zertifizierung der Baumer AG siehe unter <https://www.sqs.ch/de/zertifizierte-organisationen?title=Baumer%20AG> (aufgerufen 31.03.2025).

2. Anwendbarkeit des FINMA-Rundschreibens 2018/3

Die Baumer AG kann als Dienstleister unter den Anwendungsbereich des Rundschreibens fallen, sofern sie wesentliche Funktionen für Institute erbringt, die dem FINMA-Rundschreiben unterliegen. Die von der Baumer AG angebotenen Back- und Mid-Office-Funktionen sind grundsätzlich als wesentliche Funktionen im Sinne des Rundschreibens einzustufen.

3. Zulässigkeit des Outsourcings

Die Auslagerung der betreffenden Funktionen an die Baumer AG ist grundsätzlich zulässig, da keine der nicht auslagerbaren Funktionen gemäss Rz 8 des Rundschreibens betroffen sind. Eine spezielle Bewilligung der FINMA ist nicht erforderlich, sofern die auslagernden Unternehmen die Vorgaben des Rundschreibens einhalten.

4. Anforderungen und GoodPriv@cy®

Die Baumer AG deckt durch ihre ISO 9001, ISO 27001 und GoodPriv@cy®-Zertifizierungen wesentliche Teilbereiche der FINMA-Rundschreiben 2018/3 "Outsourcing"-Anforderungen ab. Die zertifizierten Managementsysteme (Qualitätsmanagementsystem, Informationssicherheitsmanagementsystem und Datenschutz-Managementsystem), welche auf anerkannten Standards basieren, adressieren die Anforderungen bezüglich systematischer Kontrolle (Rz 20), Informationssicherheit (Rz 24-25) und Notfallkonzepte zur Geschäftskontinuität. Die auslagernden Unternehmen prüfen im Rahmen ihrer üblichen Sorgfaltspflichten, inwieweit diese standardisierten Zertifizierungen für ihre spezifischen Geschäftsmodelle und Risikoprofile ausreichend sind und können vertraglich weitere Massnahmen vorsehen.

5. Prüfung und Aufsicht

Gemäss Rz 26-27 des Rundschreibens 2018/3 muss das auslagernde Unternehmen, dessen Prüfgesellschaft sowie die FINMA in der Lage sein, die Einhaltung der aufsichtsrechtlichen Bestimmungen beim Dienstleister zu prüfen. Die Baumer AG gewährleistet dies durch transparente Prozesse und umfassende Dokumentation, sowie durch die GoodPriv@cy®-Zertifizierungen.

6. Rolle der SQS-Zertifizierungen bei der Prüfung

Die SQS ist eine, durch die Schweizer Akkreditierungsstelle (SAS),² akkreditierte Zertifizierungsstelle mit anerkannter Fachexpertise in den Bereichen Qualitätsmanagement, Informationssicherheit und Datenschutz. Die durch die SQS durchgeführten ISO 9001, ISO 27001 und GoodPriv@cy®-Zertifizierungsprüfungen stellen gemäss den Grundsätzen der risikoorientierten Aufsicht und wirtschaftlicher Prüfungsplanung bedeutsame

² Siehe <https://www.sas.admin.ch/sas/de/home.html> (aufgerufen 31.03.2025); Siehe https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellensuchesas.exturl.html/aHR0cHM6Ly9zYXNkYi5jbGllbnRz-LmxpaXAuY2gvc2VhcmNoLm/h0bWw=.html?csrfmiddlewaretoken=usTmvI-OKtMwvRI0C6I3v484DzA5a7ri7IVZibiuRY0ZH4SkcJsiu0ckSdVSpF7&lang=de&search_term=SQS&accreditation_type=&submit=Suche+starten (aufgerufen 31.03.2025).

Prüfungsnachweise dar, die von der Prüfgesellschaft des FINMA-regulierten Unternehmens in ihrer Prüfungsstrategie angemessen berücksichtigt werden sollten. Die fachspezifische Tiefe dieser Zertifizierungsprüfungen ermöglicht es der Prüfgesellschaft, ihre eigenen Prüfungshandlungen auf ergänzende Aspekte der aufsichtsrechtlichen Anforderungen zu fokussieren und so eine fachlich fundierte, aber ressourceneffiziente Gesamtprüfung sicherzustellen.

Die SQS verfügt durch ihre Spezialisierung über eine fundierte Fachexpertise in den Bereichen Qualitätsmanagement, Informationssicherheit und Datenschutz. Nach den Grundsätzen der risikoorientierten Aufsicht und wirtschaftlichen Prüfungsplanung ist die Prüfgesellschaft des FINMA-regulierten Unternehmens gehalten, diese Prüfungsergebnisse in ihre aufsichtsrechtliche Gesamtbeurteilung einzubeziehen. Dies kann sowohl die fachliche Qualität der Beurteilung unterstützen als auch dazu beitragen, Doppelprüfungen zu vermeiden, die weder im Interesse des beaufsichtigten Unternehmens noch der Aufsichtsbehörde liegen.

D. Fazit

Die Baumer AG erfüllt durch ihre bestehenden Zertifizierungen und die damit verbundenen Managementsysteme wesentliche Anforderungen des FINMA-Rundschreibens 2018/3. Diese Beurteilung erfolgt in Anlehnung an die im Rahmen der früheren Praxis definierten Kriterien für die Beurteilung von Dienstleistern.

In Fortführung der Beurteilung der Belser Datenschutz GmbH vom 07.03.2012, die feststellte: «Mit der Zertifizierung auf der Grundlage von GoodPriv@cy® erfüllt die Baumer AG die Anforderungen an einen Dienstleister gemäss RS 08/07», kann auch unter dem aktuellen prinzipienbasierten regulatorischen Rahmen eine positive Beurteilung bestätigt werden.

Die SQS-Zertifizierungen stellen relevante Prüfungsnachweise dar, die von den Prüfgesellschaften im Rahmen ihrer aufsichtsrechtlichen Verantwortung zu berücksichtigen sind. Die ISO 9001, ISO 27001 und GoodPriv@cy®-Zertifizierungen bieten dabei spezialisierte Fachprüfungen in den Bereichen Qualitätsmanagement, Informationssicherheit und Datenschutz, die das übliche Kompetenz- und Ressourcenprofil einer Prüfgesellschaft sinnvoll ergänzt. Eine verantwortungsvolle und effiziente Prüfungsplanung kann durch die Integration dieser Zertifizierungsergebnisse in die aufsichtsrechtliche Beurteilung gefördert werden. Dies optimiert nicht nur den Einsatz von Prüfressourcen, sondern kann auch die fachliche Qualität der Gesamtbeurteilung erhöhen.

Die vertragliche Ausgestaltung der Outsourcing-Beziehung gemäss den Anforderungen des FINMA-Rundschreibens liegt in der Verantwortung der auslagernden Unternehmen. Es wird davon ausgegangen, dass die auslagernden Unternehmen ihre vertraglichen Vereinbarungen mit der Baumer AG entsprechend den regulatorischen Anforderungen ausgestalten und die Prüfungsmodalitäten sachgerecht regeln.