BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Rundschreiben 03/2022 (BA)

zur Meldung schwerwiegender Zahlungssicherheitsvorfälle gemäß § 54 Abs. 1 ZAG

An alle Zahlungsinstitute, E-Geld-Institute und CRR-Kreditinstitute

Geschäftszeichen: GIT 1-FR 1529-2021/0009

Datum: 09.03.2022

Inhaltsverzeichnis

I. Vorbemerkung 3

II. Anwendungsbereich 3

III. Begriffsbestimmungen 3

IV. Meldungen gemäß § 54 Abs. 1 ZAG 4

1. Klassifizierung der Betriebs- und Sicherheitsvorfälle 4

2. Meldeverfahren 10

3. Delegierte und konsolidierte Meldung 13

4. Betriebs- und Sicherheitsstrategie 15

I. Vorbemerkung

Gemäß § 54 Absatz 1 Satz 1 Zahlungsdiensteaufsichtsgesetz (ZAG) hat ein Zahlungsdienstleister die BaFin unverzüglich über einen schwerwiegenden Betriebs- oder Sicherheitsvorfall zu unterrichten. Mit dem „Rundschreiben 08/2018 (BA) zur Meldung schwerwiegender Sicherheitsvorfälle" vom 07.06.2018 habe ich Sie darüber informiert, wann ein Betriebs- oder Sicherheitsvorfall als schwerwiegend und damit meldepflichtig einzustufen und wie die Meldung zu erstatten ist. Dieses Rundschreiben basiert auf den von der European Banking Authority (EBA) am 19.12.2017 gemäß Artikel 96 Abs. 3 der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (PSD2) herausgegebenen Leitlinien. Diese Leitlinien wurden von der EBA im vergangenen Jahr überprüft und aktualisiert.

Mit diesem Rundschreiben möchte ich Sie über die neuen Regelungen, die ab dem 01.10.2022 für die Meldung schwerwiegender Sicherheitsvorfälle gemäß § 54 Absatz 1 Satz 1 ZAG gelten, informieren. Das „Rundschreiben 08/2018 (BA) zur Meldung schwerwiegender Sicherheitsvorfälle" vom 07.06.2018 wird gleichzeitig aufgehoben.

II. Anwendungsbereich

Das Rundschreiben gilt für alle Zahlungsinstitute und E-Geld-Institute sowie für alle CRR-Kreditinstitute und die Kreditanstalt für Wiederaufbau, soweit diese Zahlungsdienste im Sinne des § 1 Absatz 1 Satz 2 ZAG erbringen. Räumlich gilt es nur für Unternehmen mit Sitz im Inland sowie für Institute im Sinne des § 53 Kreditwesengesetz (KWG) sowie im Sinne des § 42 ZAG.

III. Begriffsbestimmungen

Sofern nicht anders angegeben, gelten die Begriffsbestimmungen des ZAG auch für dieses Rundschreiben. Für die Zwecke dieses Rundschreibens gelten darüber hinaus die folgenden Begriffsbestimmungen:

Authentizität

Die Eigenschaft einer Quelle, dass diese tatsächlich das ist, was sie zu sein vorgibt

Betriebs- oder Sicherheitsvorfall

Ein aus einem Einzelereignis oder einer Verkettung von Ereignissen bestehender Vorfall, der vom Zahlungsdienstleister nicht beabsichtigt wurde und sich nachteilig auf die Integrität, die

Verfügbarkeit, die Vertraulichkeit und/oder die Authentizität von zahlungsbezogenen Diensten auswirkt oder wahrscheinlich auswirken wird

Integrität

Die Eigenschaft, die Korrektheit und Vollständigkeit von Vermögenswerten (einschließlich Daten) zu schützen

Verfügbarkeit

Die Eigenschaft, dass zahlungsbezogene Dienste in dem von dem Zahlungsdienstleister vorab festgelegten Umfang uneingeschränkt für die Zahlungsdienstnutzer zugänglich sind und von diesen verwendet werden können

Vertraulichkeit

Die Eigenschaft, dass Informationen unbefugten Personen, Stellen oder Prozessen nicht zugänglich gemacht oder diesen nicht offengelegt werden

Zahlungsbezogene Dienste

Eine gewerbliche Tätigkeit im Sinne von § 1 Abs. 1 Satz 2 ZAG sowie alle technischen unterstützenden Aufgaben, die für die korrekte Erbringung von Zahlungsdiensten notwendig sind

IV. Meldungen gemäß § 54 Abs. 1 ZAG

1. Klassifizierung der Betriebs- und Sicherheitsvorfälle

Alle Betriebs- und Sicherheitsvorfälle sind anhand der nachfolgend dargestellten Kriterien und Indikatoren zu bewerten und entweder als schwerwiegender oder als nicht schwerwiegender Vorfall zu klassifizieren. Die als schwerwiegend eingestuften Vorfälle müssen der BaFin gemeldet werden.

1.1 Ein Betriebs- oder Sicherheitsvorfall ist schwerwiegend und damit meldepflichtig, wenn er auf Grundlage der in diesem Rundschreiben beschriebenen Kriterien (siehe Nr. 1.2) und Schwellenwerte (siehe Nr. 1.3)

- mindestens ein Kriterium der „hohen Auswirkungsstufe“ oder
- mindestens drei Kriterien der „niedrigen Auswirkungsstufe“ erfüllt.

1.2 Ein Betriebs- oder Sicherheitsvorfall ist anhand der folgenden grundsätzlichen Kriterien und den zugrundeliegenden Indikatoren zu bewerten:

i. Betroffene Zahlungsvorgänge

Zu bestimmen ist der Gesamtwert der betroffenen Zahlungsvorgänge sowie die Anzahl der beeinträchtigten Zahlungen als Prozentsatz des üblichen Volumens der mit dem betroffenen Zahlungsdienst ausgeführten Zahlungsvorgänge.

Als generelle Regel sind als „betroffene Zahlungsvorgänge" alle inländischen und grenzüberschreitenden Zahlungsvorgänge zu berücksichtigen, die direkt oder indirekt von dem Vorfall betroffen waren oder wahrscheinlich betroffen sein werden. Insbesondere fallen darunter solche Vorgänge, die nicht ausgelöst oder verarbeitet werden konnten, solche, für die der Inhalt der Zahlungsnachricht geändert wurde, und solche, die in betrügerischer Absicht in Auftrag gegeben wurden oder deren ordnungsgemäße Ausführung in anderer Weise durch den Vorfall verhindert oder beeinträchtigt wurde (unabhängig davon, ob der Betrag wiedererlangt wurde).

Betriebsvorfälle, in deren Folge die Fähigkeit beeinträchtigt wird, Transaktionen auszulösen und/oder zu verarbeiten, sind nur dann zu melden, wenn sie länger als eine Stunde andauerten. Dies gilt nicht für Betriebsvorfälle, bei den die Schwellenwerte der hohen Auswirkungsstufe überschritten werden. Diese sind unabhängig von ihrer Dauer immer zu melden. Die Dauer des Vorfalls ist ab dem Zeitpunkt seines Eintretens bis zu dem Zeitpunkt, zu dem die regulären Tätigkeiten wieder in dem Umfang ausgeführt werden können, wie es vor dem Vorfall der Fall war, zu messen.

Beim üblichen Volumen der Zahlungsvorgänge ist vom jährlichen Tagesdurchschnitt der mit denselben Zahlungsdiensten ausgeführten inländischen und grenzüberschreitenden und von dem Vorfall betroffenen Zahlungsvorgänge auszugehen. Für die Berechnungen ist das Vorjahr als Bezugszeitraum heranzuziehen. Wenn dieser Wert als nicht repräsentativ erachten wird (z. B. aufgrund saisonaler Schwankungen), kann stattdessen eine andere repräsentativere Messzahl verwenden werden. In diesem Fall sind die Gründe für die Wahl der anderen Messzahl der BaFin in dem Feld „Anmerkungen" mitzuteilen.

ii. Betroffene Zahlungsdienstnutzer

Zu bestimmen ist die Anzahl der betroffenen Zahlungsdienstnutzer sowohl als absolute Zahl als auch als Prozentsatz der Gesamtzahl der Zahlungsdienstnutzer.

Als „betroffene Zahlungsdienstnutzer" sind alle Kunden (inländische oder ausländische, Verbraucher oder Unternehmen) zu berücksichtigen, die einen Vertrag mit dem betroffenen Zahlungsdienstleister, der ihnen Zugang zu dem betroffenen Zahlungsdienst gewährt, geschlossen haben und die von den Folgen des Vorfalls beeinträchtigt waren oder wahrscheinlich beeinträchtigt sein werden. Zur Bestimmung der Anzahl der Zahlungsdienstnutzer, die den Zahlungsdienst während der Dauer des Vorfalls eventuell genutzt haben, sind Schätzungen heranziehen, die auf früheren Aktivitäten beruhen.

Im Falle einer Gruppenzugehörigkeit sind nur die eigenen Zahlungsdienstnutzer zu berücksichtigen. Falls ein Zahlungsdienstleister anderen operationelle Dienste bereitstellt, sind von diesem Zahlungsdienstleister nur die eigenen Zahlungsdienstnutzer (sofern vorhanden) zu berücksichtigen. Die Zahlungsdienstleister, welche diese operationellen

Dienste in Anspruch nehmen, haben den Vorfall in Bezug auf ihre eigenen Zahlungsdienstnutzer zu bewerten.

Betriebsvorfälle, in deren Folge die Fähigkeit beeinträchtigt wird, Transaktionen auszulösen und/oder zu verarbeiten, sind nur dann zu melden, wenn die Zahlungsdienstnutzer länger als eine Stunde davon betroffen waren. Dies gilt nicht für Betriebsvorfälle, bei den die Schwellenwerte der hohen Auswirkungsstufe überschritten werden. Diese sind unabhängig von ihrer Dauer immer zu melden. Die Dauer des Vorfalls ist ab dem Zeitpunkt seines Eintretens bis zu dem Zeitpunkt, zu dem die regulären Tätigkeiten wieder in dem Umfang ausgeführt werden können, wie es vor dem Vorfall der Fall war, zu messen.

Des Weiteren ist als Gesamtzahl der Zahlungsdienstnutzer die aggregierte Anzahl der inländischen und grenzüberschreitenden Zahlungsdienstnutzer zu verwenden, die zum Zeitpunkt des Vorfalls vertraglich an den Zahlungsdienstleister gebunden sind (oder alternativ die neueste verfügbare Anzahl) und die Zugang zu dem betroffenen Zahlungsdienst haben, unabhängig von deren Größe und davon, ob es sich um aktive oder passive Zahlungsdienstnutzer handelt.

iii. Verletzung der Sicherheit von Netz- und Informationssystemen

Festzustellen ist, ob die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der Netz- oder Informationssysteme (einschließlich der Daten), die mit der Erbringung von Zahlungsdiensten verbunden sind, durch eine böswillige Handlung verletzt wurde.

iv. Dienstausfallzeit

Zu bestimmen ist die Zeitspanne, innerhalb der der Dienst dem Zahlungsdienstnutzer wahrscheinlich nicht zur Verfügung steht oder innerhalb der der Zahlungsauftrag im Sinne von § 675f Abs. 4 Satz 2 BGB vom Zahlungsdienstleister nicht ausgeführt werden kann.

Es ist der Zeitraum zu berücksichtigen, in dem eine Aufgabe, ein Prozess oder ein Kanal in Verbindung mit der Bereitstellung von Zahlungsdiensten nicht oder wahrscheinlich nicht zur Verfügung steht und dadurch

- die Auslösung und/oder Ausführung eines Zahlungsdienstes und/oder
- der Zugang zu einem Zahlungskonto verhindert werden.

Die Dienstausfallzeit ist ab dem Zeitpunkt des Ausfallbeginns zu messen. Dabei ist sowohl die Zeitspanne zu berücksichtigen, innerhalb der der für die Ausführung von Zahlungsvorgängen erforderlichen Geschäftsbetrieb unterhalten wird, als auch die Schließungs- und Wartungszeiten, sofern relevant und anwendbar. Wenn der Beginn der Dienstausfallzeit vom Zahlungsdienstleister nicht bestimmt werden kann, ist die Ausfallzeit ausnahmsweise ab dem Zeitpunkt, zu dem der Ausfall erkannt wurde, zu messen.

v. Wirtschaftliche Auswirkungen

Zu bestimmen sind die mit dem Vorfall insgesamt verbundenen monetären Kosten. Dabei sind sowohl die absolute Höhe als auch ggf. die relative Bedeutung dieser Kosten im Verhältnis zur Größe des Zahlungsdienstleisters (d.h. zu seinem Kernkapital) zu berücksichtigen.

Es sind sowohl die Kosten zu berücksichtigen, die unmittelbar mit dem Vorfall in Verbindung gebracht werden können, als auch diejenigen, die mittelbar mit dem Vorfall in Zusammenhang stehen. Unter anderem sind veruntreute Gelder oder Vermögenswerte, Kosten für den Ersatz von Hard- oder Software, sonstige forensische oder Sanierungskosten, Gebühren aufgrund der Nichteinhaltung vertraglicher Verpflichtungen, Sanktionen, Auslandsverbindlichkeiten und entgangene Einnahmen zu berücksichtigen. Im Hinblick auf indirekte Kosten sind nur die bereits bekannten oder die aller Wahrscheinlichkeit nach entstehenden Kosten einzubeziehen.

vi. Hohe interne Eskalationsstufe

Es ist festzustellen, ob der betreffende Vorfall den Führungskräften gemeldet wurde oder diesen wahrscheinlich gemeldet werden wird.

Von einer hohen internen Eskalationsstufe ist auszugehen, wenn aufgrund der Beeinträchtigung zahlungsbezogener Dienste die Geschäftsleitung außerhalb des regelmäßigen Meldeverfahrens sowie fortlaufend während der Dauer des Vorfalls über den Vorfall informiert wurde oder wahrscheinlich informiert werden wird. Des Weiteren ist bei der Auslösung oder voraussichtlichen Auslösung eines Krisenmodus von einer hohen internen Eskalationsstufe auszugehen.

vii. Anderer Zahlungsdienstleister oder maßgebliche Infrastrukturen, die möglicherweise betroffen sind

Zu bestimmen sind die systemischen Auswirkungen, die der Vorfall wahrscheinlich hat, d. h., inwieweit der Vorfall sich über den ursprünglich betroffenen Zahlungsdienstleister hinaus auf andere Zahlungsdienstleister, Finanzmarktinfrastrukturen und/oder Zahlungssysteme auswirken kann.

Es sind die Auswirkungen des Vorfalls auf den Finanzmarkt zu bewerten, wobei darunter die Finanzmarktinfrastrukturen und/oder die Zahlungssysteme zu verstehen sind, auf die sich der betroffene Zahlungsdienstleister sowie andere Zahlungsdienstleister stützen. Insbesondere ist zu bestimmen, ob der Vorfall auch bei anderen Zahlungsdienstleistern aufgetreten ist oder wahrscheinlich auftreten wird, ob er sich auf das reibungslose Funktionieren der Finanzmarktinfrastrukturen ausgewirkt hat oder wahrscheinlich auswirken wird und ob er die stabile Funktion des Finanzsystems insgesamt beeinträchtigt hat oder wahrscheinlich beeinträchtigen wird. Dabei sind verschiedene Aspekte zu berücksichtigen, z. B. ob die betroffene Komponente oder Software eine Eigenentwicklung oder allgemein verfügbar ist, ob es sich bei dem beeinträchtigten Netzwerk um ein internes oder externes Netzwerk handelt und ob der Zahlungsdienstleister die Erfüllung seiner

Verpflichtungen innerhalb der Finanzmarktinfrastrukturen, denen er angehört, eingestellt hat oder wahrscheinlich einstellen wird.

viii. Reputationsschäden

Zu bestimmen ist, inwiefern der Vorfall das Vertrauen der Nutzer in den Zahlungsdienstleister oder allgemeiner in den zugrundeliegenden Dienst oder den Markt insgesamt erschüttern kann.

Zu berücksichtigen ist der Grad der Sichtbarkeit, den der Vorfall nach Ihrem besten Wissen auf dem Markt erlangt hat oder wahrscheinlich erlangen wird. Insbesondere die Wahrscheinlichkeit, dass der Vorfall die Gesellschaft schädigt, sollte als geeigneter Indikator herangezogen werden, um das ihm innewohnende Potenzial zur Schädigung der Reputation zu bestimmen. Des Weiteren ist zu berücksichtigen, ob

- die Zahlungsdienstnutzer und/oder andere Zahlungsdienstleister sich über nachteilige Auswirkungen des Vorfalls beschwert haben,

- der Vorfall einen sichtbaren Prozess im Zusammenhang mit Zahlungsdiensten betraf und daher in den Medien wahrscheinlich Beachtung findet oder bereits gefunden hat (wobei nicht nur herkömmliche Medien wie Zeitungen, sondern auch Blogs, soziale Netzwerke usw. einzubeziehen sind),

- vertragliche Verpflichtungen nicht erfüllt wurden oder wahrscheinlich nicht erfüllt werden, sodass rechtliche Schritte gegen den Zahlungsdienstleister und deren Veröffentlichung zu erwarten sind,

- aufsichtsrechtliche Pflichten nicht eingehalten wurden, sodass aufsichtsbehördliche Maßnahmen oder Sanktionen verhängt werden, die öffentlich bekannt wurden oder wahrscheinlich werden, und ob

- ein Vorfall ähnlicher Art bereits zuvor aufgetreten ist.

1.3 Ein Vorfall ist zu bewerten, indem für jedes oben genannte Kriterium ermittelt wird, ob die in der folgenden Tabelle aufgeführten jeweiligen Schwellenwerte vor Lösung des Vorfalls erreicht oder wahrscheinlich erreicht werden.

Kriterien	Niedrige Auswirkungsstufe	Hohe Auswirkungsstufe
Betroffene Zahlungsvorgänge	> 10 % des üblichen Transaktionsvolumens des Zahlungsdienstleisters (in Bezug auf die Anzahl der Transaktionen) **und** Dauer des Vorfalls > 1 Stunde[1]	> 25 % des üblichen Transaktionsvolumens des Zahlungsdienstleisters (in Bezug auf die Anzahl der Transaktionen)
	oder > 500.000 EUR **und** Dauer des Vorfalls > 1 Stunde[1]	**oder** > 15.000.000 EUR
Betroffene Zahlungsdienstnutzer	> 5.000 **und** Dauer des Vorfalls > 1 Stunde[1]	> 50.000
	oder > 10 % der Zahlungsdienstnutzer des Zahlungsdienstleisters **und** Dauer des Vorfalls > 1 Stunde[1]	**oder** > 25 % der Zahlungsdienstnutzer des Zahlungsdienstleisters
Dienstausfallzeit	> 2 Stunden	Nicht anwendbar
Verletzung der Sicherheit von Netzwerk- oder Informationssystemen	Ja	Nicht anwendbar
Wirtschaftliche Auswirkungen	Nicht anwendbar	> Max (0,1 % Kernkapital[2]; 200.000 EUR)
		oder > 5.000.000 EUR

Hohe interne Eskalationsstufe	Ja	Ja und voraussichtliche Auslösung eines Krisenmodus (oder eines ähnlichen Verfahrens)
Andere Zahlungsdienstleister oder maßgebliche Infrastrukturen, die möglicherweise betroffen sind	Ja	Nicht anwendbar
Reputationsschäden	Ja	Nicht anwendbar

[1] Der Schwellenwert für die Dauer des Vorfalls für einen Zeitraum von mehr als einer Stunde gilt nur für betriebliche Vorfälle, die die Fähigkeit des Zahlungsdienstleisters zur Einleitung und/oder Bearbeitung von Transaktionen beeinträchtigen.

[2] Kernkapital im Sinne von Artikel 25 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 648/2012.

1.4 Falls keine konkreten Daten vorliegen, um genauer beurteilen zu können, ob ein bestimmter Schwellenwert vor Lösung des Vorfalls erreicht oder wahrscheinlich erreicht wird (dies kann beispielsweise während der anfänglichen Untersuchungsphase der Fall sein), ist auf Schätzungen zurückzugreifen.

1.5 Eine solche Bewertung ist während der Dauer des Vorfalls kontinuierlich durchzuführen, um eine mögliche Zustandsänderung – (von nicht schwerwiegend in schwerwiegend oder umgekehrt) – zu ermitteln. Jede Reklassifizierung eines Vorfalls von schwerwiegend zu nicht schwerwiegend muss der BaFin unverzüglich gemeldet werden.

2. Meldeverfahren

2.1 Alle relevanten Informationen sind zu sammeln und der BaFin in einer Vorfallsmeldung unter Verwendung der von ihr bereitgestellten Meldewege (Melde- und Veröffentlichungsplattform - MVP-Portal) und elektronischen Formulare zu übermitteln.

Falls das MVP-Portal zu dem betreffenden Zeitpunkt nicht verfügbar oder funktionsbereit ist, sollte über die von der BaFin bekannt gemachten alternativen Kommunikationskanäle eine formlose Information über das Auftreten eines Betriebs- oder Sicherheitsvorfalls erfolgen. Die vollständige Vorfallsmeldung (Erst-, Zwischen- oder Abschlussmeldung) ist nachzureichen, sobald der reguläre Meldekanal wieder verfügbar oder funktionsbereit ist.

2.2 Während der Dauer des Vorfalls ist die BaFin unter Angabe der bei der Erstmeldung erhaltenen Vorfallsidentifikationsnummer über den Verlauf zu unterrichten (das heißt bei Erst-, Zwischen- und Abschlussmeldungen, wie in Nr. 2.7 bis 2.21 beschrieben). Alle abgefragten Informationen sind nach bestem Bemühen bereitzustellen. Sobald mehr Informationen im Laufe der internen Untersuchung zutage treten, können Zwischenmeldungen abgegeben werden, um die bis dahin eingereichten Informationen zu ergänzen (siehe Nr. 2.12).

2.3 Der BaFin ist ggf. eine Kopie der Informationen vorzulegen, die den Zahlungsdienstnutzern gemäß § 54 Absatz 4 ZAG bereitgestellt wurden oder bereitgestellt werden (sobald diese Informationen verfügbar sind).

2.4 Der BaFin sind auf Anforderung über die zur Verfügung gestellten Meldewege alle zusätzlichen Unterlagen zukommen zu lassen, die geeignet sind, die auf dem Meldeformular übermittelten Informationen zu ergänzen.

2.5 Zusätzliche Informationen, die der BaFin entweder auf eigene Initiative oder auf Ersuchen übermittelt werden, sind auf dem Meldeformular zu vermerken.

2.6 Die Vertraulichkeit und Integrität der mit der BaFin ausgetauschten Informationen ist jederzeit zu wahren; auf eine ordnungsgemäße Authentifizierung ist zu achten.

Erstmeldung

2.7 Der BaFin ist eine Erstmeldung zu übermitteln, sobald ein Betriebs- oder Sicherheitsvorfall als schwerwiegend klassifiziert wurde. Die im Rahmen der Übermittlung der Erstmeldung von der BaFin vergebene Vorfallsidentifikationsnummer ist bei allen folgenden Meldungen, die diesen Vorfall betreffen, anzugeben.

2.8 Die Erstmeldung ist innerhalb von vier Stunden ab der erstmaligen Klassifizierung des Betriebs- oder Sicherheitsvorfalls als schwerwiegend über die von der BaFin zur Verfügung gestellten Meldewege zu übermitteln. Die Arbeitsabläufe des Zahlungsdienstleisters sind so zu gestalten, dass eine Erkennung und Klassifizierung von Betriebs- oder Sicherheitsvorfällen mindestens während der üblichen Geschäftszeiten erfolgen kann.

2.9 Ein Betriebs- oder Sicherheitsvorfall ist gemäß Nr. 1.1 bis 1.5 dieses Rundschreibens zügig zu klassifizieren, jedenfalls nicht später als 24 Stunden nach seiner Erkennung und unverzüglich, nachdem die für Klassifizierung des Vorfalls erforderlichen Informationen vorliegen. Wenn für die Klassifizierung des Vorfalls mehr Zeit benötigt wird, sind die Gründe dafür in der Erstmeldung darzulegen.

2.10 Der BaFin ist ebenfalls eine Erstmeldung zu übermitteln, wenn ein zuvor nicht schwerwiegender Vorfall als schwerwiegender Vorfall reklassifiziert wird. In diesem Fall ist die Erstmeldung unmittelbar nach Erkennung der Statusänderung zu übermitteln.

2.11 In die Erstmeldung (Abschnitt A des Formulars) sind Übersichtsinformationen aufzunehmen, um so einige grundlegende Merkmale des Vorfalls sowie seine voraussichtlichen Folgen anhand der Informationen anzugeben, die unmittelbar nach der Klassifizierung

des Vorfalls als schwerwiegend verfügbar waren. Liegen keine konkreten Daten vor, ist auf Schätzungen zurückzugreifen.

Zwischenmeldung

2.12 Eine Zwischenmeldung ist zu übermitteln, wenn die regulären Tätigkeiten wiederaufgenommen wurden und der Regelbetrieb wiederhergestellt wurde. Von einer Wiederherstellung des Regelbetriebes ist auszugehen, wenn die Aktivitäten/die Vorgänge wieder dasselbe Leistungsniveau/dieselben Bedingungen in Bezug auf Verarbeitungszeiten, Kapazität, Sicherheitsanforderungen usw. erreichen, die vom Zahlungsdienstleister festgelegt oder extern durch eine Dienstgütevereinbarung festgeschrieben wurden, und keine Notfallmaßnahmen mehr aktiv sind. In der Zwischenmeldung (Abschnitt B des Formulars) sind der Vorfall und seine Folgen genauer zu beschreiben.

2.13 Wenn die regulären Tätigkeiten noch nicht wiederaufgenommen wurden, ist der BaFin innerhalb von drei Geschäftstagen nach Übermittlung der Erstmeldung eine Zwischenmeldung zu übermitteln.

2.14 Die in den Abschnitten A und B des Formulars angegebenen Informationen müssen, wenn seit der vorherigen Meldung wesentliche Änderungen eingetreten sind (z. B. wenn sich der Vorfall verschlimmert oder abgeschwächt hat, neue Ursachen ermittelt oder Maßnahmen zur Behebung des Problems ergriffen wurden), aktualisiert werden. Dies gilt auch für den Fall, dass der Vorfall nicht innerhalb von drei Geschäftstagen behoben wurde. In diesem Fall ist eine weitere Zwischenmeldung zu übermitteln. Auf Ersuchen der BaFin muss in jedem Fall eine zusätzliche Zwischenmeldung übermittelt werden.

2.15 Wie im Fall von Erstmeldungen ist auf Schätzungen zurückzugreifen, wenn keine konkreten Daten verfügbar sind.

2.16 Sollte sich der Regelbetrieb vor Ablauf von vier Stunden seit der Klassifizierung des Vorfalls als schwerwiegend wieder normalisiert haben, sind die Erstmeldung und die Zwischenmeldung möglichst zeitgleich innerhalb der Frist von vier Stunden zu übermitteln (indem die Abschnitte A und B des Formulars ausgefüllt werden).

Abschlussmeldung

2.17 Nachdem die Ursachenanalyse durchgeführt wurde (unabhängig davon, ob Maßnahmen zur Begrenzung der Auswirkungen bereits umgesetzt wurden oder die Hauptursache endgültig ermittelt wurde) und ggf. konkrete Zahlen zur Ersetzung der Schätzungen vorliegen, ist eine Abschlussmeldung zu übermitteln.

2.18 Diese Abschlussmeldung ist der BaFin spätestens 20 Geschäftstage nach der Wiederherstellung des Regelbetriebs zu übermitteln. Wird eine Verlängerung dieser Frist benötigt (wenn z. B. noch keine konkreten Zahlen zu den Auswirkungen des Vorfalls vorliegen oder die Hauptursachen noch nicht ermittelt wurden), hat der Zahlungsdienstleister sich vor Ablauf der Frist mit der BaFin in Verbindung zu setzen und eine angemessene Begründung für die Verzögerung vorzulegen sowie ein neues Datum für die Abschlussmeldung vorzuschlagen.

2.19 Falls der Zahlungsdienstleister alle für die Abschlussmeldung erforderlichen Informationen innerhalb der Frist von vier Stunden seit der Klassifizierung des Vorfalls als schwerwiegend vorlegen kann, kann eine kombinierte Erst-, Zwischen- und Abschlussmeldung als „Gesamtmeldung" über das MVP-Portal übermittelt werden.

2.20 In der Abschlussmeldung sind möglichst vollständige Angaben zu machen, das heißt

- konkrete Zahlen zu den Auswirkungen des Vorfalls statt Schätzungen (sowie jede weitere ggf. erforderliche Aktualisierung der Angaben in den Abschnitten A und B des Formulars) und

- Angaben in Abschnitt C des Formulars, wozu die Hauptursache, sofern bereits bekannt, und eine Übersicht über die Maßnahmen zählen, die zur Behebung des Problems oder zur Verhinderung seines erneuten Auftretens in der Zukunft ergriffen wurden oder geplant sind.

2.21 Falls ein Zahlungsdienstleister infolge der kontinuierlichen Bewertung des Vorfalls feststellt, dass ein bereits gemeldeter Vorfall die Kriterien für eine Klassifizierung als schwerwiegend nicht länger erfüllt und nicht davon auszugehen ist, dass er sie vor seiner Lösung erfüllen wird, so ist die Abschlussmeldung so schnell wie möglich nach Erkennung dieses Sachverhalts, jedoch in jedem Fall innerhalb der für die Übermittlung der nächsten Meldung geltenden Frist zu übermitteln. In dieser speziellen Situation ist der Abschnitt C des Formulars nicht auszufüllen, sondern das Feld „Vorfall als nicht schwerwiegend reklassifiziert" auszuwählen und die Gründe für diese Reklassifizierung zu erläutern.

3. Delegierte und konsolidierte Meldung

3.1 Sollten Zahlungsdienstleister die in diesem Rundschreiben aufgeführten Meldepflichten an einen Dritten delegieren (auslagern), sind folgende Bedingungen zu erfüllen:

a. Im förmlichen Vertrag oder in den ggf. innerhalb einer Gruppe bestehenden internen Regelungen, der bzw. die der delegierten Meldung zwischen dem Zahlungsdienstleister und dem Dritten zugrunde liegt bzw. liegen, ist die Zuweisung der Verantwortlichkeiten aller Parteien eindeutig festgelegt. Insbesondere wird in einem solchen Vertrag oder in solchen Regelungen klar dargelegt, dass der betreffende Zahlungsdienstleister, unabhängig von der möglichen Delegierung der Meldepflichten, für die Erfüllung der Pflichten gemäß § 54 Abs. 1 ZAG sowie für den Inhalt der an die zuständige Behörde im Herkunftsmitgliedstaat übermittelten Informationen weiterhin in vollem Umfang verantwortlich und rechenschaftspflichtig ist.

b. Die Delegierung steht im Einklang mit den Anforderungen für die Auslagerung wichtiger betrieblicher Aufgaben gemäß

   i. § 26 ZAG bei Zahlungs- und E-Geld-Instituten in Verbindung mit Ziffer 9 des Rundschreibens 11/2021 (BA) vom 16.08.2021 (ZAIT) bei Zahlungs- und E-Geld-Instituten (einschließlich der Institute im Sinne des § 42 Abs. 1 ZAG)

ii. § 25b KWG in Verbindung mit AT 9 des Rundschreibens 10/2021 (BA) vom 16.08.2021 „Mindestanforderungen an das Risikomanagement" bei CRR-Kreditinstituten (einschließlich der Institute im Sinne des § 53 Abs. 1 KWG)

c. Die Informationen über die Delegierung der Meldepflicht wird der BaFin - sofern nicht bereits geschehen - vorab übermittelt.

d. Die Vertraulichkeit sensibler Daten sowie die Qualität, die Konsistenz, die Integrität und die Zuverlässigkeit der an die BaFin zu übermittelnden Informationen werden ordnungsgemäß gewährleistet.

3.2 Zahlungsdienstleister, die dem benannten Dritten die Erfüllung der Meldepflichten auf konsolidierte Weise gestatten möchten (d. h. durch Vorlage einer einzigen Meldung, die sich auf mehrere Zahlungsdienstleister bezieht, welche von demselben schwerwiegenden Betriebs- oder Sicherheitsvorfall betroffen sind), haben sicherzustellen, dass die folgenden Bedingungen erfüllt sind:

a. Die Zulässigkeit dieses Vorgehens wird in den der delegierten Meldung zugrundeliegenden Vertrag aufgenommen.

b. Die konsolidierte Meldung setzt voraus, dass der Vorfall durch eine Unterbrechung der von dem Dritten erbrachten Dienste verursacht wurde.

c. Die konsolidierte Meldung beschränkt sich auf Zahlungsdienstleister, die im selben Mitgliedstaat ansässig sind.

d. Es wird eine Liste aller von dem Vorfall betroffenen Zahlungsdienstleister übermittelt.

e. Es wird sichergestellt, dass der Dritte die Wesentlichkeit des Vorfalls für jeden betroffenen Zahlungsdienstleister bewertet und in die konsolidierte Meldung nur diejenigen Zahlungsdienstleister aufnimmt, für die der Vorfall als schwerwiegend klassifiziert wird. In Zweifelsfällen ist ein Zahlungsdienstleister in die konsolidierte Meldung einzubeziehen.

f. Bei der Übermittlung der Meldung ist darauf zu achten, dass bei den Feldern des Formulars, in denen keine gemeinsame Antwort möglich ist (z. B. in den Abschnitten B 2, B 4 oder C 3), der Dritte die kumulierten Werte angibt, die für die Zahlungsdienstleister beobachtet oder geschätzt wurden.

g. Der Dritte hält die Zahlungsdienstleister jederzeit über alle relevanten Informationen bezüglich des Vorfalls und über jegliche etwaigen Interaktionen des Dritten mit der zuständigen Behörde sowie deren Inhalt auf dem Laufenden; dies gilt jedoch nur in dem Maße, in dem die Vertraulichkeit von Informationen, die sich auf andere Zahlungsdienstleister beziehen, nicht verletzt wird.

h. Die BaFin wird über dieses Verfahren - sofern nicht bereits geschehen - über die bekannt gemachten Kommunikationskanäle informiert. Die Anzeige kann zusammen mit der Anzeige der Delegierung der Meldepflicht unter Nr. 3.1 (c) erfolgen.

3.3 Meldepflichten dürfen nicht delegiert werden, bevor die BaFin darüber informiert wurde. Des Weiteren dürfen Meldepflichten nicht delegiert werden, nachdem ein Zahlungsdienstleister davon in Kenntnis gesetzt wurde, dass die Auslagerungsvereinbarung die in Nr. 3.1 Buchstabe b genannten Anforderungen nicht erfüllt.

3.4. Wenn Zahlungsdienstleister die Delegierung ihrer Meldepflichten widerrufen möchten, ist diese Entscheidung der BaFin über die bekannt gemachten Kommunikationskanäle mitzuteilen. Außerdem ist die BaFin über jede wesentliche Entwicklung in Bezug auf den benannten Dritten und dessen Fähigkeit, den Meldepflichten nachzukommen, in Kenntnis zu setzen.

3.5. Falls es der benannte Dritte unterlässt, die BaFin entgegen der getroffenen Vereinbarungen von einem schwerwiegenden Betriebs- oder Sicherheitsvorfall gemäß § 54 Abs. 1 ZAG und diesem Rundschreiben zu unterrichten, so haben die Zahlungsdienstleister sicherzustellen, dass sie ihren Meldepflichten auch ohne externe Unterstützung nachkommen können. Zahlungsdienstleister haben zudem sicherzustellen, dass ein Vorfall nicht zweimal gemeldet wird, d. h. zum einen vom betreffenden Zahlungsdienstleister und ein weiteres Mal von dem Dritten.

3.6. Wenn ein Vorfall auf eine durch einen technischen Dienstleister (oder eine Infrastruktur) verursachte Störung zurückzuführen ist, von der mehrere Zahlungsdienstleister betroffen sind, haben die Zahlungsdienstleister zu gewährleisten, dass sich die delegierte Meldung auf die individuellen Daten des jeweiligen Zahlungsdienstleisters bezieht (es sei denn, es handelt sich um eine konsolidierte Meldung).

4. Betriebs- und Sicherheitsstrategie

4.1 Die Zahlungsdienstleister haben sicherzustellen, dass in ihrer Betriebs- und Sicherheitsstrategie alle Zuständigkeiten für die Meldung von Vorfällen gemäß der PSD2 sowie die zu diesem Zweck eingeführten Prozesse klar definiert sind, damit die in den vorliegenden Leitlinien beschriebenen Anforderungen eingehalten werden können.