EBA/GL/2021/03

10. Juni 2021

Überarbeitete Leitlinien

für die Meldung schwerwiegender Vorfälle gemäß der Richtlinie (EU) 2015/2366 (PSD2)

1. Einhaltung der Vorschriften und Meldepflichten

Status dieser Leitlinien

1. Dieses Dokument Dokument enthält Leitlinien, die nach Artikel 16 der EBA-Verordnung [1] herausgegeben werden. Gemäß Artikel 16 Absatz 3 der EBA-Verordnung müssen die zuständigen Behörden und die Finanzinstitute alle erforderlichen Anstrengungen unternehmen, um diesen Leitlinien nachzukommen.

2. Die Leitlinien legen fest, was nach Ansicht der EBA angemessene Aufsichtspraktiken innerhalb des Europäischen Finanzaufsichtssystems sind oder wie das Unionsrecht in einem bestimmten Bereich anzuwenden ist. Zuständige Behörden im Sinne von Artikel 4 Absatz 2 der EBA-Verordnung sollten die an sie gerichteten Leitlinien in geeigneter Weise (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren) in ihre Aufsichtspraktiken integrieren, einschließlich der Leitlinien, die in erster Linie an Institute gerichtet sind.

Meldepflichten

3. Nach Artikel 16 Absatz 3 der EBA-Verordnung müssen die zuständigen Behörden der EBA bis zum (07.11.2021) mitteilen, ob sie diesen Leitlinien nachkommen oder nachzukommen beabsichtigen, oder die Gründe nennen, warum sie dies nicht tun. Geht innerhalb der genannten Frist keine Mitteilung ein, geht die EBA davon aus, dass die zuständigen Behörden den Anforderungen nicht nachkommen. Die Mitteilungen sind unter Verwendung des auf der Website der EBA abrufbaren Formulars mit dem Betreff „EBA/GL/2021/03“ zu übermitteln. Die Mitteilungen sollten durch Personen erfolgen, die befugt sind, im Namen ihrer Behörde die Einhaltung zu melden. Jegliche Änderungen des Status der Einhaltung müssen der EBA ebenfalls gemeldet werden.

4. Die Meldungen werden gemäß Artikel 16 Absatz 3 der EBA-Verordnung auf der Website der EBA veröffentlicht.

[1] Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 12).

2. Gegenstand, Anwendungsbereich und Begriffsbestimmungen

Gegenstand

5. Diese Leitlinien dienen der Erfüllung des Auftrags, der der EBA gemäß Artikel 96 Absatz 3 der Richtlinie (EU) 2015/2366 (zweite Zahlungsdiensterichtlinie, PSD2) 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 erteilt wurde.

6. Insbesondere werden in diesen Leitlinien die Kriterien für die von den Zahlungsdienstleistern vorzunehmende Klassifizierung schwerwiegender Betriebs- oder Sicherheitsvorfälle sowie das Format und die Verfahren beschrieben, die Zahlungsdienstleister gemäß Artikel 96 Absatz 1 der PSD2 bei der Meldung solcher Vorfälle an die zuständige Behörde im Herkunftsmitgliedstaat einhalten sollten.

7. Des Weiteren wird in diesen Leitlinien darauf eingegangen, wie die betreffenden zuständigen Behörden die Relevanz eines Vorfalls bewerten und welche Einzelheiten sie bei der Meldung von Vorfällen an andere nationale Behörden gemäß Artikel 96 Absatz 2 der PSD2 übermitteln sollten.

8. Darüber hinaus enthalten diese Leitlinien Informationen hinsichtlich der Unterrichtung der EBA und der EZB über die maßgeblichen Einzelheiten der gemeldeten Vorfälle, um eine gemeinsame und einheitliche Vorgehensweise zu fördern.

Anwendungsbereich

9. Diese Leitlinien gelten in Bezug auf die Klassifizierung und die Meldung schwerwiegender Betriebs- oder Sicherheitsvorfälle gemäß Artikel 96 der PSD2.

10. Sie beziehen sich auf alle Vorfälle, die unter die Definition von „schwerwiegenden Betriebs- oder Sicherheitsvorfällen“ fallen, in die sowohl externe als auch interne Ereignisse, seien sie in böswilliger Absicht oder aus Versehen verursacht, eingeschlossen sind.

11. Außerdem gelten diese Leitlinien in Fällen, in denen ein schwerwiegender Betriebs- oder Sicherheitsvorfall seinen Ursprung außerhalb der Union hat (z. B. wenn sich ein Vorfall in der Muttergesellschaft oder in einer Tochtergesellschaft ereignet, die außerhalb der Union ansässig ist) und die von einem in der Union ansässigen Zahlungsdienstleister erbrachten Zahlungsdienste direkt (ein zahlungsbezogener Dienst wird von dem nicht in der Union ansässigen betroffenen Unternehmen erbracht) oder indirekt (die Fähigkeit des

Zahlungsdienstleisters, seine Zahlungstätigkeit weiterhin wahrzunehmen, wird infolge des Vorfalls auf sonstige Weise gefährdet) beeinträchtigt.

12. Diese Leitlinien gelten zudem für schwerwiegende Vorfälle, die Funktionen betreffen, mit denen Zahlungsdienstleister Dritte beauftragt haben.

Adressaten

13. Die erste Gruppe der Leitlinien (Abschnitt 4) richtet sich an Zahlungsdienstleister im Sinne von Artikel 4 Absatz 11 der PSD2 sowie an solche, die in Artikel 4 Absatz 1 der Verordnung (EU) Nr. 1093/2010 genannt sind.

14. Die zweite und dritte Gruppe der Leitlinien (Abschnitte 5 und 6) richten sich an die zuständigen Behörden im Sinne von Artikel 4 Absatz 2 Ziffer i der Verordnung (EU) Nr. 1093/2010.

Begriffsbestimmungen

15. Sofern nicht anders angegeben, haben die in der PSD2 verwendeten und definierten Begriffe in den vorliegenden Leitlinien dieselbe Bedeutung. Für die Zwecke der vorliegenden Leitlinien gelten darüber hinaus die folgenden Begriffsbestimmungen:

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 eine solche nachteilige Auswirkung haben wird
Integrität	Die Eigenschaft, die Korrektheit und Vollständigkeit von Vermögenswerten (einschließlich Daten) zu schützen
Verfügbarkeit	Die Eigenschaft, dass zahlungsbezogene Dienste in dem vom Zahlungsdienstleister vorab festgelegten akzeptablen 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
Authentizität	Die Eigenschaft einer Quelle, dass diese tatsächlich das ist, was sie zu sein vorgibt

Zahlungsbezogene Dienste	Eine gewerbliche Tätigkeit im Sinne von Artikel 4 Absatz 3 der PSD2 sowie alle technischen unterstützenden Aufgaben, die für die korrekte Erbringung von Zahlungsdiensten notwendig sind

3. Umsetzung

Geltungsbeginn

16. Diese Leitlinien gelten ab dem 1. Januar 2022.

Aufhebung

17. Folgende Leitlinien werden mit Wirkung zum 1. Januar 2022 aufgehoben:

Leitlinien für die Meldung schwerwiegender Vorfälle gemäß der Richtlinie 2015/2366/EU (EBA/GL/2017/10)

4. Leitlinien für Zahlungsdienstleister in Bezug auf die Meldung schwerwiegender Betriebs- oder Sicherheitsvorfälle an die zuständige Behörde in ihrem Herkunftsmitgliedstaat

Leitlinie 1: Klassifizierung als schwerwiegender Vorfall

1.1. Folgende Vorfälle sollten die Zahlungsdienstleister als schwerwiegende Betriebs- oder Sicherheitsvorfälle einstufen:

a. Vorfälle, die ein Kriterium oder mehrere Kriterien des „Higher Impact Level“ erfüllen, oder

b. Vorfälle, die drei oder mehr Kriterien des „Lower Impact Level“ erfüllen,

wie in Leitlinie 1.4 dargelegt sowie entsprechend der in den vorliegenden Leitlinien beschriebenen Bewertung.

1.2. Zur Bewertung eines Betriebs- oder Sicherheitsvorfalls sollten die Zahlungsdienstleister die folgenden Kriterien und zugrunde liegenden Indikatoren verwenden:

i. Betroffene Zahlungsvorgänge

Die Zahlungsdienstleister sollten den Gesamtwert der betroffenen Zahlungsvorgänge bestimmen sowie die Anzahl der beeinträchtigten Zahlungen als Prozentsatz des üblichen Volumens der mit dem betroffenen Zahlungsdienst ausgeführten Zahlungsvorgänge.

ii. Betroffene Zahlungsdienstnutzer

Die Zahlungsdienstleister sollten ermitteln, wie viele Zahlungsdienstnutzer betroffen sind, und diesen Wert sowohl als absolute Zahl als auch als Prozentsatz der Gesamtzahl der Zahlungsdienstnutzer angeben.

iii. Verletzung der Sicherheit von Netz- oder Informationssystemen

Die Zahlungsdienstleister sollten feststellen, ob die Sicherheit vom Netz- oder Informationssystemen, die mit der Erbringung von Zahlungsdiensten verbunden sind, durch eine böswillige Handlung verletzt wurde.

iv. Dienstausfallzeit

Die Zahlungsdienstleister sollten die Zeitspanne bestimmen, in deren Verlauf der Dienst dem Zahlungsdienstnutzer wahrscheinlich nicht zur Verfügung steht oder in deren Verlauf der Zahlungsauftrag im Sinne von Artikel 4 Absatz 13 der PSD2 vom Zahlungsdienstleister nicht ausgeführt werden kann.

v. Wirtschaftliche Auswirkungen

Die Zahlungsdienstleister sollten die mit dem Vorfall insgesamt verbundenen monetären Kosten bestimmen und sowohl die absolute Höhe als auch ggf. die relative Bedeutung dieser Kosten im Verhältnis zur Größe des Zahlungsdienstleisters (d. h. zu seinem Kernkapital („Tier 1 Capital“)) berücksichtigen.

vi. Hohe interne Eskalationsstufe

Die Zahlungsdienstleister sollten feststellen, ob der betreffende Vorfall ihren Führungskräften gemeldet wurde oder diesen wahrscheinlich gemeldet werden wird.

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

Die Zahlungsdienstleister sollten die systemischen Auswirkungen bestimmen, 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.

viii. Reputationsschäden

Die Zahlungsdienstleister sollten bestimmen, inwiefern der Vorfall das Vertrauen der Nutzer in den Zahlungsdienstleister oder allgemeiner in den zugrunde liegenden Dienst oder den Markt insgesamt erschüttern kann.

1.3. Von den Zahlungsdienstleistern sollten die Indikatorwerte gemäß der folgenden Methode berechnet werden:

i. Betroffene Zahlungsvorgänge:

Als generelle Regel sollten die Zahlungsdienstleister als „betroffene Zahlungsvorgänge“ alle inländischen und grenzüberschreitenden Zahlungsvorgänge erachten, die direkt oder indirekt von dem Vorfall betroffen waren oder wahrscheinlich betroffen sein werden. Insbesondere sollten darunter solche Vorgänge fallen, 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 (unabhängig davon, ob der Betrag wiedererlangt wurde) oder deren ordnungsgemäße Ausführung in anderer Weise durch den Vorfall verhindert oder beeinträchtigt wurde.

Betriebsvorfälle, in deren Folge die Fähigkeit beeinträchtigt wird, Transaktionen auszulösen und/oder zu verarbeiten, sollten von den Zahlungsdienstleistern nur gemeldet werden, wenn sie länger als eine Stunde andauerten. Die Dauer des Vorfalls sollte ab dem Zeitpunkt seines Eintretens bis zu dem Zeitpunkt gemessen werden, zu dem die regulären Tätigkeiten wieder in dem Umfang ausgeführt werden können, wie es vor dem Vorfall der Fall war.

Als übliches Volumen der Zahlungsvorgänge sollten die Zahlungsdienstleister des Weiteren den jährlichen Tagesdurchschnitt der mit denselben Zahlungsdiensten ausgeführten inländischen und grenzüberschreitenden Zahlungsvorgänge erachten, die von dem Vorfall betroffen waren, wobei für die Berechnungen das Vorjahr als Bezugszeitraum heranzuziehen ist. Falls die Zahlungsdienstleister diesen Wert als nicht repräsentativ erachten (z. B. aufgrund saisonaler Schwankungen), sollten sie stattdessen eine andere repräsentativere Messzahl verwenden und der zuständigen Behörde im betreffenden Feld der Vorlage (siehe Anhang) das diesem Ansatz zugrunde liegende Prinzip mitteilen.

ii. Betroffene Zahlungsdienstnutzer

Als „betroffene Zahlungsdienstnutzer" sollten die Zahlungsdienstleister alle Kunden (inländische oder ausländische, Verbraucher oder Unternehmen) erachten, 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, sollten die Zahlungsdienstleister Schätzungen heranziehen, die auf früheren Aktivitäten beruhen.

Im Falle von Gruppen sollte jeder Zahlungsdienstleister nur die eigenen Zahlungsdienstnutzer berücksichtigen. Falls ein Zahlungsdienstleister anderen operationelle Dienste bereitstellt, sollte dieser Zahlungsdienstleister nur die eigenen Zahlungsdienstnutzer (sofern vorhanden) berücksichtigen. Die Zahlungsdienstleister, welche diese operationellen Dienste in Anspruch nehmen, sollten den Vorfall in Bezug auf ihre eigenen Zahlungsdienstnutzer bewerten.

Betriebsvorfälle, in deren Folge die Fähigkeit beeinträchtigt wird, Transaktionen auszulösen und/oder zu verarbeiten, sollten von den Zahlungsdienstleistern nur gemeldet werden, wenn die Zahlungsdienstnutzer länger als eine Stunde davon betroffen waren. Die Dauer des Vorfalls sollte ab dem Zeitpunkt seines Eintretens bis zu dem Zeitpunkt gemessen werden, zu dem die regulären Tätigkeiten wieder in dem Umfang ausgeführt werden können, wie es vor dem Vorfall der Fall war.

Des Weiteren sollten Zahlungsdienstleister als Gesamtzahl der Zahlungsdienstnutzer die aggregierte Anzahl der inländischen und grenzüberschreitenden Zahlungsdienstnutzer verwenden, die zum Zeitpunkt des Vorfalls vertraglich an sie 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- oder Informationssystemen

Die Zahlungsdienstleister sollten feststellen, 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

Die Zahlungsdienstleister sollten den Zeitraum 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 i) die Auslösung und/oder Ausführung eines Zahlungsdienstes und/oder ii) der Zugang zu einem Zahlungskonto verhindert werden. Die Dienstausfallzeit sollte ab dem Zeitpunkt des Ausfallbeginns gemessen werden, und die Zahlungsdienstleister sollten sowohl die Zeitspanne berücksichtigen, in deren Verlauf sie den für die Ausführung von Zahlungsvorgängen erforderlichen Geschäftsbetrieb unterhalten, als auch die Schließungs- und Wartungszeiten, sofern relevant und anwendbar. Wenn der Zahlungsdienstleister den Beginn der Dienstausfallzeit nicht bestimmen kann, sollte er die Ausfallzeit ausnahmsweise ab dem Zeitpunkt messen, zu dem der Ausfall erkannt wurde.

v. Wirtschaftliche Auswirkungen

Die Zahlungsdienstleister sollten sowohl die Kosten in Betracht ziehen, die unmittelbar mit dem Vorfall in Verbindung gebracht werden können, als auch diejenigen, die mittelbar mit dem Vorfall in Zusammenhang stehen. Unter anderem sollten 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 berücksichtigt werden. Im Hinblick auf indirekte Kosten sollten nur die bereits bekannten oder die aller Wahrscheinlichkeit nach entstehenden Kosten in Betracht gezogen werden.

vi. *Hohe interne Eskalationsstufe*

Die Zahlungsdienstleister sollten prüfen, ob aufgrund der Beeinträchtigung zahlungsbezogener Dienste das Leitungsorgan im Sinne der EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken nach Maßgabe der Leitlinie 60 Buchstabe d besagter Leitlinien außerhalb des regelmäßigen Meldeverfahrens sowie fortlaufend während der Dauer des Vorfalls über den Vorfall informiert wurde oder wahrscheinlich informiert werden wird. Des Weiteren sollten die Zahlungsdienstleister in Erwägung ziehen, ob infolge der Auswirkungen des Vorfalls auf zahlungsbezogene Dienste ein Krisenmodus ausgelöst wurde oder wahrscheinlich ausgelöst werden wird.

vii. *Andere Zahlungsdienstleister oder maßgebliche Infrastrukturen, die möglicherweise betroffen sind*

Die Zahlungsdienstleister sollten die Auswirkungen des Vorfalls auf den Finanzmarkt bewerten, wobei darunter die Finanzmarktinfrastrukturen und/oder die Zahlungssysteme zu verstehen sind, auf die sich der betroffene Zahlungsdienstleister sowie andere Zahlungsdienstleister stützen. Insbesondere sollte bewertet werden, 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 sollten die Zahlungsdienstleister verschiedene Aspekte in ihren Überlegungen berücksichtigen, z. B. ob

es sich bei der betroffenen Komponente oder Software um eine Eigenentwicklung handelt oder ob sie 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*

Die Zahlungsdienstleister sollten den Grad der Sichtbarkeit erwägen, 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, sollten die Zahlungsdienstleister als geeigneten Indikator heranziehen, um das ihm innewohnende Potenzial zur Schädigung ihrer Reputation zu bestimmen. Die Zahlungsdienstleister sollten berücksichtigen, ob i) die Zahlungsdienstnutzer und/oder andere Zahlungsdienstleister sich über nachteilige Auswirkungen des Vorfalls beschwert haben, ii) 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), iii) vertragliche Verpflichtungen nicht erfüllt wurden oder wahrscheinlich nicht erfüllt werden, sodass rechtliche Schritte gegen den Zahlungsdienstleister und deren Veröffentlichung zu erwarten sind, iv) aufsichtsrechtliche Pflichten missachtet wurden, sodass aufsichtsbehördliche Maßnahmen oder Sanktionen verhängt werden, die öffentlich bekannt wurden oder wahrscheinlich werden, und ob v) ein Vorfall ähnlicher Art bereits zuvor aufgetreten ist.

1.4. Die Zahlungsdienstleister sollten einen Vorfall bewerten, indem für jedes Kriterium festgestellt wird, ob die in Tabelle 1 aufgeführten jeweiligen Schwellenwerte vor Lösung des Vorfalls erreicht oder wahrscheinlich erreicht werden.

Tabelle 1: Schwellenwerte

Kriterien	Lower Impact Level	Higher Impact Level
Betroffene Zahlungsvorgänge	> 10 % des üblichen Transaktionsvolumens des Zahlungsdienstleisters (in Bezug auf die Anzahl der Transaktionen) **und** Dauer des Vorfalls > 1 Stunde* **oder** > 500 000 EUR **und** Dauer des Vorfalls > 1 Stunde*	> 25 % des üblichen Transaktionsvolumens des Zahlungsdienstleisters (in Bezug auf die Anzahl der Transaktionen) **oder** > 15 Mio. EUR
Betroffene Zahlungsdienstnutzer	> 5 000 **und** Dauer des Vorfalls > 1 Stunde*	> 50 000 **oder**

	oder > 10 % der Zahlungsdienstnutzer des Zahlungsdienstleisters **und** Dauer des Vorfalls > 1 Stunde*	> 25 % der Zahlungsdienstnutzer des Zahlungsdienstleisters
Dienstausfallzeit	> 2 Stunden	Nicht anwendbar
Verletzung der Sicherheit von Netz- oder Informationssystemen	Ja	Nicht anwendbar
Wirtschaftliche Auswirkungen	Nicht anwendbar	> Max. (0,1 % Kernkapital**, 200 000 EUR) **oder** > 5 Mio. 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

* Der Schwellenwert für die Dauer des Vorfalls von mehr als einer Stunde gilt nur für Betriebsvorfälle, die die Fähigkeit des Zahlungsdienstleisters beeinträchtigen, Transaktionen auszulösen und/oder zu verarbeiten.

**Kernkapital gemäß 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.

1.5. Falls Zahlungsdienstleister über keine konkreten Daten verfügen, um ihre Beurteilung, ob ein bestimmter Schwellenwert vor Lösung des Vorfalls erreicht oder wahrscheinlich erreicht wird, zu stützen (dies kann beispielsweise während der anfänglichen Untersuchungsphase der Fall sein), sollten sie auf Schätzungen zurückgreifen.

1.6. Eine solche Bewertung sollte während der Dauer des Vorfalls kontinuierlich durchgeführt werden, um eine mögliche Zustandsänderung – nach oben oder nach unten – (von nicht schwerwiegend in schwerwiegend oder umgekehrt) – zu ermitteln. Jede Reklassifizierung des Vorfalls von schwerwiegend in nicht schwerwiegend sollte der zuständigen Behörde im Einklang mit der Leitlinie 2.21 unverzüglich gemeldet werden.

Leitlinie 2: Meldeverfahren

2.1. Die Zahlungsdienstleister sollten alle relevanten Informationen sammeln, eine Vorfallsmeldung unter Verwendung der im Anhang bereitgestellten Vorlage erstellen und diese Meldung der zuständigen Behörde im Herkunftsmitgliedstaat übermitteln. Die Zahlungsdienstleister sollten alle Felder der Vorlage gemäß den Anweisungen im Anhang ausfüllen.

2.2. Zur Übermittlung der Erst-, Zwischen- und Abschlussmeldung zu dem betreffenden Vorfall sollten die Zahlungsdienstleister dieselbe Vorlage verwenden. Daher sollten die Zahlungsdienstleister ein und dieselbe Vorlage sukzessive ergänzen und darin die in früheren Berichten übermittelten Informationen bei Bedarf aktualisieren.

2.3. Außerdem sollten die Zahlungsdienstleister der zuständigen Behörde in ihrem Herkunftsmitgliedstaat ggf. eine Kopie der Informationen vorlegen (sobald diese Informationen verfügbar sind), die sie ihren Nutzern gemäß Artikel 96 Absatz 1 zweiter Unterabsatz der PSD2 bereitgestellt haben oder bereitstellen werden.

2.4. Die Zahlungsdienstleister sollten der zuständigen Behörde in ihrem Herkunftsmitgliedstaat auf Anforderung alle zusätzlichen Unterlagen zukommen lassen, die geeignet sind, die auf der Standardvorlage übermittelten Informationen zu ergänzen. Die Zahlungsdienstleister sollten allen Ersuchen seitens der zuständigen Behörde im Herkunftsmitgliedstaat Folge leisten und zusätzliche Informationen oder Klarstellungen in Bezug auf die bereits übermittelten Unterlagen liefern.

2.5. Zusätzliche Informationen, die Zahlungsdienstleister der zuständigen Behörde entweder auf eigene Initiative oder auf Ersuchen der zuständigen Behörde gemäß Leitlinie 2.4 zukommen lassen, sollten von dem betreffenden Zahlungsdienstleister auf der Vorlage gemäß Leitlinie 2.1 vermerkt werden.

2.6. Die Zahlungsdienstleister sollten jederzeit die Vertraulichkeit und Integrität der ausgetauschten Informationen wahren und sich gegenüber der zuständigen Behörde in ihrem Herkunftsmitgliedstaat ordnungsgemäß authentifizieren.

Erstmeldung

2.7. Die Zahlungsdienstleister sollten der zuständigen Behörde im Herkunftsmitgliedstaat eine Erstmeldung übermitteln, sobald ein Betriebs- oder Sicherheitsvorfall als schwerwiegend klassifiziert wurde. Die zuständigen Behörden sollten den Erhalt der Erstmeldung unverzüglich bestätigen und eine eindeutige Vorfallidentifikationsnummer vergeben. Diese Identifikationsnummer sollten die Zahlungsdienstleister angeben, wenn sie eine Aktualisierung der Erstmeldung bzw. die Zwischen- und Abschlussmeldung zu dem betreffenden Vorfall übermitteln, es sei denn, die letzteren beiden Meldungen werden zusammen mit der Erstmeldung eingereicht.

2.8. Die Erstmeldung sollte innerhalb von vier Stunden ab der erstmaligen Klassifizierung des Betriebs- oder Sicherheitsvorfalls als schwerwiegend an die zuständige Behörde übermittelt werden. Falls bekannt ist, dass die Meldekanäle der zuständigen Behörde zu dem betreffenden Zeitpunkt nicht verfügbar oder funktionsbereit sind, sollte die Erstmeldung erfolgen, sobald die Meldekanäle wieder verfügbar oder funktionsbereit sind.

2.9. Die Zahlungsdienstleister sollten den Vorfall gemäß den Leitlinien 1.1 und 1.4 rechtzeitig klassifizieren, jedenfalls nicht später als 24 Stunden nach seiner Erkennung und unverzüglich,

nachdem ihnen die für die Klassifizierung des Vorfalls erforderlichen Informationen vorliegen. Wenn zur Klassifizierung des Vorfalls mehr Zeit benötigt wird, sollten die Zahlungsdienstleister in der Erstmeldung an die zuständige Behörde die Gründe darlegen.

2.10. Die Zahlungsdienstleister sollten der zuständigen Behörde im Herkunftsmitgliedstaat ebenfalls eine Erstmeldung übermitteln, wenn ein zuvor nicht schwerwiegender Vorfall als schwerwiegender Vorfall reklassifiziert wird. In diesem speziellen Fall sollte der zuständigen Behörde die Erstmeldung unmittelbar nach Erkennung der Statusänderung übermittelt werden. Falls bekannt ist, dass die Meldekanäle der zuständigen Behörde zu dem betreffenden Zeitpunkt nicht verfügbar oder funktionsbereit sind, sollte die Erstmeldung erfolgen, sobald die Meldekanäle wieder verfügbar oder funktionsbereit sind.

2.11. Die Zahlungsdienstleister sollten in ihrer Erstmeldung (Abschnitt A der Vorlage) Übersichtsinformationen bereitstellen, 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, sollten Zahlungsdienstleister auf Schätzungen zurückgreifen.

Zwischenmeldung

2.12. Wenn die regulären Tätigkeiten wieder aufgenommen wurden und der Regelbetrieb wiederhergestellt wurde, sollten die Zahlungsdienstleister eine Zwischenmeldung übermitteln, in der sie die zuständige Behörde über diesen Sachverhalt unterrichten. Die Zahlungsdienstleister sollten davon ausgehen, dass der Regelbetrieb wiederhergestellt ist, 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 der Vorlage) sollten der Vorfall und seine Folgen genauer beschrieben werden.

2.13. Wenn die regulären Tätigkeiten noch nicht wieder aufgenommen wurden, sollten die Zahlungsdienstleister der zuständigen Behörde innerhalb von drei Geschäftstagen nach Übermittlung der Erstmeldung eine Zwischenmeldung zukommen lassen.

2.14. Die Zahlungsdienstleister sollten die bereits in den Abschnitten A und B der Vorlage angegebenen Informationen aktualisieren, wenn sie erkennen, dass 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). Dies gilt auch für den Fall, dass der Vorfall nicht innerhalb von drei Geschäftstagen behoben wurde. In diesem Fall sind die Zahlungsdienstleister verpflichtet, eine weitere Zwischenmeldung zu übermitteln. In jedem Fall sollten die Zahlungsdienstleister eine zusätzliche Zwischenmeldung auf Ersuchen der zuständigen Behörde im Herkunftsmitgliedstaat übermitteln.

2.15. Wie im Fall von Erstmeldungen sollten Zahlungsdienstleister auf Schätzungen zurückgreifen, 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, sollten die Zahlungsdienstleister die Erstmeldung und die Zwischenmeldung möglichst zeitgleich innerhalb der Frist von vier Stunden übermitteln (indem sie die Abschnitte A und B der Vorlage ausfüllen).

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, sollten die Zahlungsdienstleister eine Abschlussmeldung übermitteln.

2.18. Diese Abschlussmeldung sollte der zuständigen Behörde spätestens 20 Geschäftstage nach der Wiederherstellung des Regelbetriebs übermittelt werden. Benötigt der Zahlungsdienstleister eine Verlängerung dieser Frist (wenn z. B. noch keine konkreten Zahlen zu den Auswirkungen des Vorfalls vorliegen oder die Hauptursachen noch nicht ermittelt wurden), sollte er sich vor Ablauf der Frist mit der zuständigen Behörde in Verbindung setzen und eine angemessene Begründung für die Verzögerung vorlegen sowie ein neues Datum für die Abschlussmeldung vorschlagen.

2.19. Falls die Zahlungsdienstleister alle für die Abschlussmeldung erforderlichen Informationen (d. h. die Angaben in Abschnitt C der Vorlage) innerhalb der Frist von vier Stunden seit der Klassifizierung des Vorfalls als schwerwiegend vorlegen können, sollten sie nach Möglichkeit die für die Erst-, die Zwischen- und die Abschlussmeldung maßgeblichen Informationen zusammen übermitteln.

2.20. Die Zahlungsdienstleister sollten in ihren Abschlussmeldungen möglichst vollständige Angaben machen, d. h. i) konkrete Zahlen zu den Auswirkungen des Vorfalls statt Schätzungen (sowie jede weitere ggf. erforderliche Aktualisierung der Angaben in den Abschnitten A und B der Vorlage) und ii) Angaben in Abschnitt C der Vorlage, 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. Die Zahlungsdienstleister sollten außerdem eine Abschlussmeldung übermitteln, wenn sie infolge der kontinuierlichen Bewertung des Vorfalls feststellen, 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. In diesem Fall sollte die Abschlussmeldung so schnell wie möglich nach Erkennung dieses Sachverhalts, jedoch in jedem Fall innerhalb der für die Übermittlung der nächsten Meldung geltenden Frist übermittelt werden. In dieser speziellen Situation sollten die Zahlungsdienstleister

Abschnitt C der Vorlage nicht ausfüllen, sondern das Feld „Vorfall als nicht schwerwiegend reklassifiziert“ ankreuzen und die Gründe für diese Reklassifizierung erläutern.

Leitlinie 3: Delegierte und konsolidierte Meldung

3.1. Sofern von der zuständigen Behörde gestattet, sollten Zahlungsdienstleister, die ihre Meldepflichten gemäß der PSD2 an einen Dritten delegieren möchten, die zuständige Behörde im Herkunftsmitgliedstaat davon unterrichten und sicherstellen, dass die folgenden Bedingungen erfüllt sind:

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 Artikel 96 der PSD2 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. Artikel 19 Absatz 6 der PSD2 in Bezug auf Zahlungsinstitute und E-Geld-Institute, anwendbar mutatis mutandis im Einklang mit Artikel 3 der Richtlinie 2009/110/EG (E-Geld-Richtlinie), oder

   ii. den EBA-Leitlinien zu Auslagerungen (EBA/GL/2019/02) in Bezug auf alle Zahlungsdienstleister.

c. Die Informationen werden der zuständigen Behörde im Herkunftsmitgliedstaat vorab und in jedem Fall entsprechend den von der zuständigen Behörde ggf. festgelegten Fristen und Verfahren übermittelt.

d. Die Vertraulichkeit sensibler Daten sowie die Qualität, die Konsistenz, die Integrität und die Zuverlässigkeit der an die zuständige Behörde 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), sollten die zuständige Behörde im Herkunftsmitgliedstaat davon in Kenntnis setzen, die Kontaktdaten unter „Betroffener

Zahlungsdienstleister“ in die Vorlage eintragen und sicherstellen, dass die folgenden Bedingungen erfüllt sind:

a. Diese Bestimmung wird in den der delegierten Meldung zugrunde liegenden 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. Des Weiteren wird sichergestellt, dass in Zweifelsfällen ein Zahlungsdienstleister in die konsolidierte Meldung einbezogen wird, solange es keine Belege dafür gibt, dass dies nicht der Fall sein sollte.

f. Es wird sichergestellt, dass bei Feldern der Vorlage, in denen keine gemeinsame Antwort möglich ist (z. B. in den Abschnitten B 2, B 4 oder C 3), der Dritte entweder i) diese Felder für jeden betroffenen Zahlungsdienstleister getrennt ausfüllt, wobei jeweils die Identität des Zahlungsdienstleisters anzugeben ist, auf den sich die Informationen beziehen, oder ii) 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 etwaige 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.

3.3. Die Zahlungsdienstleister sollten ihre Meldepflichten nicht delegieren, bevor sie die zuständige Behörde im Herkunftsmitgliedstaat darüber informiert haben. Des Weiteren sollten sie ihre Meldepflichten nicht delegieren, nachdem sie davon in Kenntnis gesetzt wurden, dass die Auslagerungsvereinbarung die in Leitlinie 3.1 Buchstabe b genannten Anforderungen nicht erfüllt.

3.4. Wenn Zahlungsdienstleister die Delegierung ihrer Meldepflichten widerrufen möchten, sollten sie diese Entscheidung der zuständigen Behörde im Herkunftsmitgliedstaat gemäß den von dieser festgelegten Fristen und Verfahren mitteilen. Außerdem sollten die Zahlungsdienstleister die zuständige Behörde im Herkunftsmitgliedstaat von jeder

wesentlichen Entwicklung in Bezug auf den benannten Dritten und dessen Fähigkeit, den Meldepflichten nachzukommen, in Kenntnis setzen.

3.5. Falls es der benannte Dritte unterlässt, die zuständige Behörde im Herkunftsmitgliedstaat von einem schwerwiegenden Betriebs- oder Sicherheitsvorfall gemäß Artikel 96 der PSD2 und diesen Leitlinien zu unterrichten, sollten die Zahlungsdienstleister ihren Meldepflichten auch ohne externe Unterstützung nachkommen können. Zahlungsdienstleister sollten zudem sicherstellen, 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, sollten die Zahlungsdienstleister gewährleisten, dass sich die delegierte Meldung auf die individuellen Daten des jeweiligen Zahlungsdienstleisters bezieht (es sei denn, es handelt sich um eine konsolidierte Meldung).

Leitlinie 4: Betriebs- und Sicherheitsstrategie

4.1. Die Zahlungsdienstleister sollten sicherstellen, 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.

5. Leitlinien für die zuständigen Behörden in Bezug auf die Kriterien für die Bewertung der Relevanz eines Vorfalls und Einzelheiten der Meldung von Vorfällen an andere nationale Behörden

Leitlinie 5: Bewertung der Relevanz eines Vorfalls

5.1. Die zuständigen Behörden im Herkunftsmitgliedstaat sollten die Relevanz eines schwerwiegenden Betriebs- oder Sicherheitsvorfalls für andere nationale Behörden auf Grundlage ihrer eigenen Einschätzung bewerten. Dabei sollten die folgenden Kriterien als primäre Indikatoren für die Bedeutung des betreffenden Vorfalls herangezogen werden:

a. Die Ursachen des Vorfalls liegen innerhalb des regulatorischen Aufgabenbereichs der anderen nationalen Behörde (d. h. innerhalb ihres Zuständigkeitsbereichs).
b. Die Folgen des Vorfalls wirken sich auf die Zielsetzungen der anderen nationalen Behörde aus (z. B. Schutz der Stabilität des Finanzsystems).
c. Der Vorfall hat weitreichende Auswirkungen auf Zahlungsdienstnutzer oder könnte solche Auswirkungen haben.
d. Der Vorfall fand oder findet wahrscheinlich in den Medien starke Beachtung.

5.2. Die zuständigen Behörden im Herkunftsmitgliedstaat sollten diese Bewertung während der Dauer des Vorfalls kontinuierlich durchführen, um mögliche Änderungen zu erkennen, durch die ein Vorfall Relevanz erlangt, der zuvor nicht als relevant eingestuft wurde.

Leitlinie 6: Auszutauschende Informationen

6.1. Ungeachtet anderer rechtlicher Vorschriften zum Austausch vorfallsbezogener Informationen mit anderen nationalen Behörden sollten die zuständigen Behörden den durch Anwendung der Leitlinie 5.1 ermittelten maßgeblichen nationalen Behörden Informationen über schwerwiegende Betriebs- oder Sicherheitsvorfälle zur Verfügung stellen. Diese Unterrichtung sollte zumindest zum Zeitpunkt des Eingangs der Erstmeldung erfolgen (oder alternativ bei Eingang der Meldung, die den Informationsaustausch auslöste) sowie bei Eingang der Benachrichtigung, dass der Regelbetrieb wiederhergestellt ist (d. h. bei Eingang der Zwischenmeldung).

6.2. Die zuständigen Behörden sollten den maßgeblichen nationalen Behörden die Informationen übermitteln, die notwendig sind, um sich ein klares Bild über den Vorfall und die möglichen Folgen zu machen. Dazu sollten sie zumindest die vom Zahlungsdienstleister in den folgenden Feldern der Vorlage (in der Erst- oder der Zwischenmeldung) angegebenen Informationen übermitteln:

- Datum und Uhrzeit der Klassifizierung des Vorfalls als schwerwiegend;
- Datum und Uhrzeit der Erkennung des Vorfalls;
- Datum und Uhrzeit des Beginns des Vorfalls;
- Zeitpunkt (Datum und Uhrzeit), zu dem der Vorfall behoben wurde oder voraussichtlich behoben wird;
- kurze Beschreibung des Vorfalls (einschließlich nicht sensibler Teile der ausführlichen Beschreibung);
- kurze Beschreibung der ergriffenen oder geplanten Maßnahmen zur Behebung des Vorfalls;
- Beschreibung, inwiefern andere Zahlungsdienstleister und/oder Infrastrukturen von dem Vorfall betroffen sein könnten;
- ggf. Beschreibung der Medienberichterstattung;
- Ursache des Vorfalls.

6.3. Vor dem Austausch von vorfallsbezogenen Informationen mit maßgeblichen nationalen Behörden sollten die zuständigen Behörden bei Bedarf die erforderlichen Anonymisierungen vornehmen und alle Informationen ausschließen, die aufgrund ihrer Vertraulichkeit oder aufgrund von Rechten des geistigen Eigentums Restriktionen unterliegen. Dessen ungeachtet sollten die zuständigen Behörden jedoch den maßgeblichen nationalen Behörden Name und Anschrift des Zahlungsdienstleisters mitteilen, der den Vorfall meldet, wenn die besagten nationalen Behörden gewährleisten können, dass diese Informationen vertraulich behandelt werden.

6.4. Die zuständigen Behörden sollten die Vertraulichkeit und die Integrität der gespeicherten und ausgetauschten Informationen jederzeit wahren und sich gegenüber den maßgeblichen nationalen Behörden ordnungsgemäß authentifizieren. Insbesondere sollten die zuständigen Behörden, unbeschadet des geltenden Unionsrechts sowie geltender nationaler Bestimmungen, alle gemäß den vorliegenden Leitlinien erhaltenen Informationen im Einklang mit der in der PSD2 verankerten beruflichen Geheimhaltungspflicht behandeln.

6. Leitlinien für die zuständigen Behörden in Bezug auf die Kriterien für die Bewertung der an die EBA und die EZB zu übermittelnden maßgeblichen Einzelheiten der Vorfallsmeldungen sowie in Bezug auf das Format und die Verfahren für die entsprechende Kommunikation

Leitlinie 7: Auszutauschende Informationen

7.1. Die zuständigen Behörden sollten die EBA und die EZB stets über alle Meldungen unterrichten, die sie von den von einem schwerwiegenden Betriebs- oder Sicherheitsvorfall betroffenen Zahlungsdienstleistern (oder in deren Namen) erhalten. Zu diesem Zweck sollten die zuständigen Behörden die Standarddatei verwenden, die auf der Website der EBA zur Verfügung gestellt wird.

Leitlinie 8: Kommunikation

8.1. Die zuständigen Behörden sollten die Vertraulichkeit und die Integrität der gespeicherten und ausgetauschten Informationen jederzeit wahren und sich gegenüber der EBA und der EZB ordnungsgemäß authentifizieren. Insbesondere sollten die zuständigen Behörden, unbeschadet des geltenden Unionsrechts sowie geltender nationaler Bestimmungen, alle gemäß den vorliegenden Leitlinien erhaltenen Informationen im Einklang mit der in der PSD2 verankerten beruflichen Geheimhaltungspflicht behandeln.

8.2. Zur Vermeidung von Verzögerungen bei der Übertragung der vorfallsbezogenen Informationen an die EBA und die EZB und zur Minimierung des Risikos von Betriebsunterbrechungen sollten die zuständigen Behörden geeignete Kommunikationswege und -mittel unterstützen.

Anhang – Vorlage für Meldungen von Zahlungsdienstleistern

Erstmeldung

Erstmeldung	innerhalb von 4 Stunden nach Klassifizierung des Vorfalls als schwerwiegend	Dropdown-Auswahl zurücksetzen
Meldedatum *(TT/MM/JJJJ)*		Uhrzeit *(HH:MM)*
Vorfallidentifikationsnummer		

A – Erstmeldung									
A 1 – ALLGEMEINE ANGABEN									
Art der Meldung									
Art der Meldung									
Betroffener Zahlungsdienstleister									
Name des Zahlungsdienstleisters									
Nationale Identifikationsnummer des Zahlungsdienstleisters									
Ggf. Hauptunternehmen der Gruppe									
Vom Vorfall betroffenes Land/betroffene Länder	☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ	☐ DE ☐ DK ☐ EE ☐ ES ☐ FI	☐ FR ☐ LI ☐ GR ☐ HR ☐ HU	☐ IE ☐ IS ☐ IT ☐ LT ☐ LU	☐ LV ☐ MT ☐ NL ☐ NO ☐ PL	☐ PT ☐ RO ☐ SE ☐ SI ☐ SK			
Hauptansprechpartner				E-Mail		Telefon			
Alternativer Ansprechpartner				E-Mail		Telefon			
Meldende Stelle (Machen Sie hier Angaben, wenn im Falle der delegierten Meldung die meldende Stelle nicht der betroffene Zahlungsdienstleister ist.)									
Name der meldenden Stelle									
Nationale Identifikationsnummer									
Hauptansprechpartner				E-Mail		Telefon			
Alternativer Ansprechpartner				E-Mail		Telefon			
A 2 – ERKENNUNG und KLASSIFIZIERUNG DES VORFALLS									
Datum und Uhrzeit der Erkennung des Vorfalls *(TT/MM/JJJJ HH:MM)*									
Datum und Uhrzeit der Klassifizierung des Vorfalls *(TT/MM/JJJJ HH:MM)*									
Vorfall wurde erkannt von				Falls „Sonstige", bitte angeben:					
Art des Vorfalls									
Kriterien für die Meldung eines schwerwiegenden Vorfalls	☐ Betroffene	☐ Betroffene Zahlungsdienstnutzer	☐ Dienstausfallzeit	☐ Verletzung der Sicherheit von Netz- oder Informationssystemen	☐ Wirtschaftliche	☐ Hohe interne Eskalationsstufe	☐ Andere Zahlungsdienstleister/maßgebliche Infrastrukturen, die möglicherweise betroffen sind	☐ Reputationsschäden	
Kurze allgemeine Beschreibung des Vorfalls									
Auswirkungen in anderen EU-Mitgliedstaaten, sofern gegeben									
Meldungen an sonstige Behörden				Falls „JA", bitte angeben:					
Gründe für die verspätete Übermittlung der Erstmeldung:									

Zwischenmeldung

Meldung eines schwerwiegenden Vorfalls

Zwischenmeldung	spätestens 3 Geschäftstage nach Übermittlung der Erstmeldung	Dropdown-Auswahl

Meldedatum *(TT/MM/JJJJ)* | Uhrzeit *(HH:MM)*

Vorfallidentifikationsnummer

B – Zwischenmeldung

B 1 – ALLGEMEINE ANGABEN

Nähere Beschreibung des Vorfalls:

Worin besteht das konkrete Problem?		
Wann ist der Vorfall eingetreten?		
Welchen Verlauf hat der Vorfall genommen?		
Welche Auswirkungen hatte er (insbesondere für Zahlungsdienstnutzer)?		
Wurden die Zahlungsdienstnutzer über den Vorfall informiert?		Falls „JA", bitte angeben:
Besteht ein Zusammenhang zu früheren Vorfällen?		Falls „JA", bitte angeben:
Waren weitere Dienstleister/Dritte betroffen oder beteiligt?		Falls „JA", bitte angeben:
Wurde das (interne und/oder externe) Krisenmanagement ausgelöst?		Falls „JA", bitte angeben:
Datum und Uhrzeit des Beginns des Vorfalls (sofern bereits ermittelt) *(TT/MM/JJJJ HH:MM)*		
Zeitpunkt (Datum und Uhrzeit), zu dem der Vorfall behoben wurde oder voraussichtlich behoben wird *(TT/MM/JJJJ HH:MM)*		
Betroffene Funktionsbereiche	☐ Authentifizierung/Autorisierung ☐ Direkte Verrechnung ☐ Kommunikation ☐ Indirekte Verrechnung ☐ Clearing ☐ Sonstiges	Falls „Sonstiges", bitte angeben:
Änderungen gegenüber früheren Meldungen		

B 2 – KLASSIFIZIERUNG DES VORFALLS/INFORMATIONEN ZUM VORFALL

Betroffene Zahlungsvorgänge[2]	Auswirkungen Anzahl der betroffenen Zahlungsvorgänge Als % der üblichen Anzahl von Zahlungsvorgängen Wert der betroffenen Zahlungsvorgänge in EUR Dauer des Vorfalls (nur für Betriebsvorfälle) Anmerkungen:	
Betroffene Zahlungsdienstnutzer[3]	Auswirkungen Anzahl der betroffenen Zahlungsdienstnutzer Als % der Gesamtzahl der Zahlungsdienstnutzer	
Verletzung der Sicherheit von Netz- oder Informationssystemen	Beschreiben Sie, in welcher Weise die Netz- oder Informationssysteme betroffen waren.	
Dienstausfallzeit	Dienstausfallzeit insgesamt: Tage: Stunden: Minuten:	
Wirtschaftliche Auswirkungen	Auswirkungen Direkte Kosten in EUR Indirekte Kosten in EUR	
Hohe interne Eskalationsstufe	Beschreiben Sie die interne Eskalationsstufe des Vorfalls unter Angabe, ob dieser einen Krisenmodus (oder Ähnliches) ausgelöst hat/voraussichtlich auslösen wird, und falls ja, beschreiben Sie dies bitte.	
Andere Zahlungsdienstleister/maßgebliche Infrastrukturen, die möglicherwe	Beschreiben Sie, inwiefern andere Zahlungsdienstleister und/oder Infrastrukturen vom Vorfall betroffen sein könnten	
Reputationsschäden	Beschreiben Sie, inwiefern der Vorfall die Reputation des Zahlungsdienstleisters schädigen könnte (z. B. Medienberichterstattung, Veröffentlichung von rechtlichen Schritten oder Gesetzesverstößen usw.)	

B 3 – BESCHREIBUNG DES VORFALLS

Art des Vorfalls		
Ursache des Vorfalls	☐ In Untersuchung ☐ Böswillige Handlung ☐ Prozessfehler ☐ Systemfehler ☐ Menschliches Versagen ☐ Externe Ereignisse ☐ Sonstiges	Falls „Sonstiges", bitte angeben:
Waren Sie direkt oder indirekt durch einen Dienstleister vom Vorfall betroffen?		Bei „Indirekt" geben Sie bitte den Namen des Dienstleisters an:

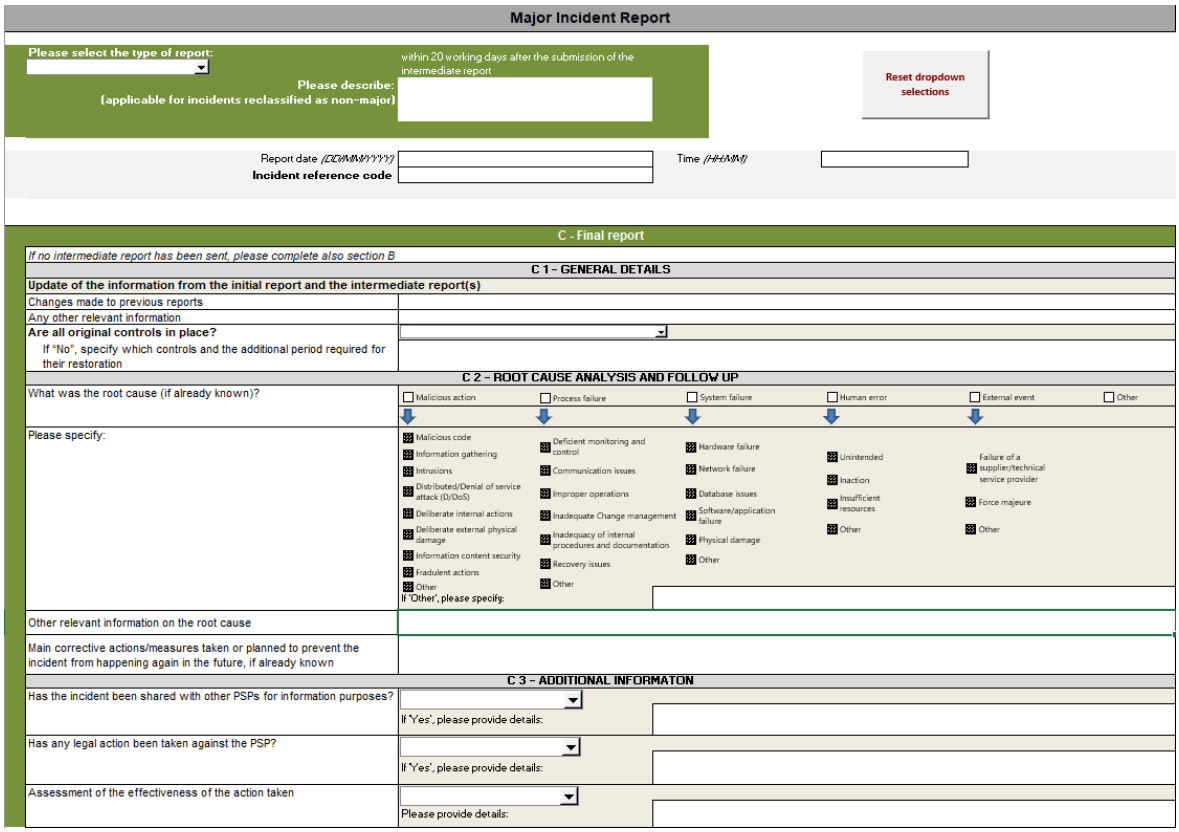
B 4 – AUSWIRKUNGEN DES VORFALLS

Gesamtauswirkung	☐ Integrität ☐ Verfügbarkeit	☐ Vertraulichkeit ☐ Authentizität	
Betroffene Geschäftskanäle	☐ Zweigniederlassungen ☐ E-Banking ☐ Elektronischer Handel	☐ Telefonbanking ☐ Mobile Banking ☐ Geldautomaten	☐ Verkaufsstelle ☐ Sonstiges
	Falls „Sonstiges", bitte angeben:		
Betroffene Zahlungsdienste	☐ Bareinzahlung auf ein Zahlungskonto ☐ Barabhebung von einem Zahlungskonto ☐ Zur Führung eines Zahlungskontos erforderliche Vorgänge ☐ Annahme und Abrechnung von Zahlungsvorgängen (Acquiring)	☐ Überweisungen ☐ Lastschriften ☐ Kartenzahlungen ☐ Ausgabe von Zahlungsinstrumenten	☐ Finanztransfer ☐ Zahlungsauslösedi ☐ Kontoinformationsdienste

B 5 – BEGRENZUNG DER AUSWIRKUNGEN DES VORFALLS

Welche Maßnahmen wurden bisher ergriffen oder sind geplant, um den Vorfall zu beheben?	
Wurde(n) der Plan zur Fortführung des Geschäftsbetriebs und/oder der Plan zur Wiederherstellung des Normalbetriebs aktiviert?	
Falls ja, wann? *(TT/MM/JJJJ, HH:MM)*	
Falls ja, geben Sie bitte Einzelheiten an.	

Abschlussmeldung



Major Incident Report

Please select the type of report:

within 20 working days after the submission of the intermediate report

Please describe: (applicable for incidents reclassified as non-major)

Reset dropdown selections

Report date *(DD/MM/YYYY)*: Time *(HH:MM)*:

Incident reference code

C - Final report

If no intermediate report has been sent, please complete also section B

C 1 – GENERAL DETAILS

Update of the information from the initial report and the intermediate report(s)	
Changes made to previous reports	
Any other relevant information	
Are all original controls in place?	
If "No", specify which controls and the additional period required for their restoration	

C 2 – ROOT CAUSE ANALYSIS AND FOLLOW UP

What was the root cause (if already known)?	☐ Malicious action	☐ Process failure	☐ System failure	☐ Human error	☐ External event	☐ Other
Please specify:	☒ Malicious code ☒ Information gathering ☒ Intrusions ☒ Distributed/Denial of service attack (D/DoS) ☒ Deliberate internal actions ☒ Deliberate external physical damage ☒ Information content security ☒ Fradulent actions ☒ Other If 'Other', please specify:	☒ Deficient monitoring and control ☒ Communication issues ☒ Improper operations ☒ Inadequate Change management ☒ Inadequacy of internal procedures and documentation ☒ Recovery issues ☒ Other	☒ Hardware failure ☒ Network failure ☒ Database issues ☒ Software/application failure ☒ Physical damage ☒ Other	☒ Unintended ☒ Inaction ☒ Insufficient resources ☒ Other	☒ Failure of a supplier/technical service provider ☒ Force majeure ☒ Other	
Other relevant information on the root cause						
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known						

C 3 – ADDITIONAL INFORMATON

Has the incident been shared with other PSPs for information purposes?	If 'Yes', please provide details:
Has any legal action been taken against the PSP?	If 'Yes', please provide details:
Assessment of the effectiveness of the action taken	Please provide details:

Anleitungen für das Ausfüllen der Vorlage

Zahlungsdienstleister sollten je nach Meldephase den entsprechenden Abschnitt der Vorlage ausfüllen: für die Erstmeldung Abschnitt A, für Zwischenmeldungen Abschnitt B und für die Abschlussmeldung Abschnitt C. Zur Übermittlung der Erst-, Zwischen- und Abschlussmeldung zu demselben Vorfall sollten die Zahlungsdienstleister dieselbe Vorlage verwenden. Sofern nichts anderes angegeben ist, sind alle Felder Pflichtfelder.

Überschrift

Erstmeldung: Dies ist die erste Meldung, die der Zahlungsdienstleister der zuständigen Behörde im Herkunftsmitgliedstaat übermittelt.

Zwischenmeldung: In der Zwischenmeldung werden der Vorfall und seine Folgen genauer beschrieben. Es handelt sich um eine Aktualisierung der Erstmeldung (bzw. einer vorangegangenen Zwischenmeldung) zum selben Vorfall.

Abschlussmeldung: Dies ist die letzte Meldung, die der Zahlungsdienstleister zu dem Vorfall übermittelt, da i) bereits eine Ursachenanalyse durchgeführt wurde und die Schätzungen durch konkrete Zahlen ersetzt werden können oder ii) der Vorfall nicht mehr als schwerwiegend eingestuft wird und reklassifiziert werden muss.

Vorfall als nicht schwerwiegend reklassifiziert: Der Vorfall erfüllt die Kriterien für eine Klassifizierung als schwerwiegend nicht mehr und wird sie voraussichtlich auch vor seiner Lösung nicht wieder erfüllen. Die Zahlungsdienstleister sollten die Gründe für diese Herabstufung angeben.

Datum und Uhrzeit der Meldung: das genaue Datum und die genaue Uhrzeit, zu denen der zuständigen Behörde die Meldung übermittelt wurde.

Vorfallidentifikationsnummer (für Zwischen- und Abschlussmeldungen sowie für Aktualisierungen der Erstmeldung): die von der zuständigen Behörde bei Eingang der Erstmeldung zur eindeutigen Identifizierung des Vorfalls vergebene Nummer. Jede zuständige Behörde sollte dieser Nummer den aus zwei Buchstaben bestehenden ISO-Code[2] ihres jeweiligen Mitgliedstaats voranstellen.

A - Erstmeldung

A 1 - Allgemeine Angaben

Art der Meldung

Einzeln: Die Meldung bezieht sich auf einen einzelnen Zahlungsdienstleister.

Konsolidiert: Die Meldung bezieht sich auf mehrere Zahlungsdienstleister im selben Mitgliedstaat, die vom selben schwerwiegenden Betriebs- oder Sicherheitsvorfall betroffen sind und die Möglichkeit einer konsolidierten Meldung nutzen. Die Felder unter „Betroffener Zahlungsdienstleister“ sollten leer bleiben (mit Ausnahme des Felds „Vom Vorfall betroffenes Land/betroffene Länder“), und es sollte eine Liste der in die Meldung eingeschlossenen Zahlungsdienstleister erstellt werden, indem die Tabelle „Konsolidierte Meldung – Liste der Zahlungsdienstleister“ ausgefüllt wird.

Betroffener Zahlungsdienstleister: der Zahlungsdienstleister, bei dem der Vorfall aufgetreten ist.

Name des Zahlungsdienstleisters: vollständiger Name des Zahlungsdienstleisters, der dem Meldeverfahren unterliegt, entsprechend dem Eintrag im jeweiligen offiziellen nationalen Register der Zahlungsdienstleister.

Nationale Identifikationsnummer des Zahlungsdienstleisters: die eindeutige nationale Identifikationsnummer, mit der die zuständige Behörde des Herkunftsmitgliedstaats den Zahlungsdienstleister in ihrem nationalen Register eindeutig kennzeichnet.

[2] Die Alpha-2-Ländercodes nach der Norm ISO-3166 finden Sie unter https://www.iso.org/iso-3166-country-codes.html.

Hauptunternehmen der Gruppe: Im Falle einer Gruppe von Unternehmen gemäß Artikel 4 Absatz 40 der PSD2 geben Sie bitte den Namen des Hauptunternehmens an.

Vom Vorfall betroffenes Land/betroffene Länder: das Land oder die Länder, in denen die Auswirkungen des Vorfalls spürbar sind (wenn z. B. mehrere Zweigniederlassungen eines Zahlungsdienstleisters in verschiedenen Ländern betroffen sind), unabhängig davon, wie schwerwiegend der Vorfall in dem anderen Land/den anderen Ländern ist. Bei dem betroffenen Land kann, muss es sich aber nicht um den Herkunftsmitgliedstaat handeln.

Hauptansprechpartner: Vor- und Nachname der für die Meldung des Vorfalls zuständigen Person oder, falls ein dritter Zahlungsdienstleister die Meldung im Namen des betroffenen Zahlungsdienstleisters vornimmt, Vor- und Nachname der Person, die beim betroffenen Zahlungsdienstleister für die Abteilung für Vorfalls-/Risikomanagement oder einen ähnlichen Bereich verantwortlich ist.

E-Mail: die E-Mail-Adresse, an die ggf. Anfragen zur weiteren Klärung gesendet werden können. Hierbei kann es sich um eine persönliche oder eine Firmen-E-Mail-Adresse handeln.

Telefonnummer des Ansprechpartners: Telefonnummer, die ggf. zur weiteren Klärung angerufen werden kann. Hierbei kann es sich um eine persönliche oder um eine Firmentelefonnummer handeln.

Alternativer Ansprechpartner: Vor- und Nachname einer alternativen Person, an die sich die zuständige Behörde bei Anfragen bezüglich des Vorfalls wenden kann, wenn der Hauptansprechpartner nicht verfügbar ist. Falls ein dritter Zahlungsdienstleister die Meldung im Namen des betroffenen Zahlungsdienstleisters vornimmt, Vor- und Nachname einer alternativen Person in der Abteilung für Vorfalls-/Risikomanagement oder einem ähnlichen Bereich beim betroffenen Zahlungsdienstleister.

E-Mail: E-Mail-Adresse des alternativen Ansprechpartners, an die ggf. Anfragen zur weiteren Klärung gesendet werden können. Hierbei kann es sich um eine persönliche oder eine Firmen-E-Mail-Adresse handeln.

Telefon: Telefonnummer des alternativen Ansprechpartners, die ggf. zur weiteren Klärung angerufen werden kann. Hierbei kann es sich um eine persönliche oder um eine Firmentelefonnummer handeln.

Meldende Stelle: Hier sollten Angaben gemacht werden, falls ein Dritter den Meldepflichten im Namen des betroffenen Zahlungsdienstleisters nachkommt.

Name der meldenden Stelle: vollständiger Name der Stelle, die den Vorfall meldet, entsprechend dem Eintrag im gültigen offiziellen nationalen Unternehmensregister.

Nationale Identifikationsnummer: die eindeutige nationale Identifikationsnummer in dem Land, in dem der Dritte seinen Sitz hat, zur eindeutigen Identifizierung der den Vorfall meldenden Stelle. Wenn es sich bei dem meldenden Dritten um einen Zahlungsdienstleister handelt, sollte als nationale Identifikationsnummer die eindeutige nationale Identifikationsnummer angegeben werden, die von der zuständigen Behörde des Herkunftsmitgliedstaats im nationalen Register verwendet wird.

Hauptansprechpartner: Vor- und Nachname der für die Meldung des Vorfalls zuständigen Person.

E-Mail: die E-Mail-Adresse, an die ggf. Anfragen zur weiteren Klärung gesendet werden können. Hierbei kann es sich um eine persönliche oder eine Firmen-E-Mail-Adresse handeln.

Telefonnummer des Ansprechpartners: Telefonnummer, die ggf. zur weiteren Klärung angerufen werden kann. Hierbei kann es sich um eine persönliche oder um eine Firmentelefonnummer handeln.

Alternativer Ansprechpartner: Vor- und Nachname einer alternativen Person innerhalb der den Vorfall meldenden Stelle, an die sich die zuständige Behörde wenden kann, wenn der Hauptansprechpartner nicht verfügbar ist.

E-Mail: E-Mail-Adresse des alternativen Ansprechpartners, an die ggf. Anfragen zur weiteren Klärung gesendet werden können. Hierbei kann es sich um eine persönliche oder eine Firmen-E-Mail-Adresse handeln.

Telefon: Telefonnummer des alternativen Ansprechpartners, die ggf. zur weiteren Klärung angerufen werden kann. Hierbei kann es sich um eine persönliche oder um eine Firmentelefonnummer handeln.

A 2 - Erkennung und Klassifizierung des Vorgangs

Datum und Uhrzeit der Erkennung des Vorfalls: Zeitpunkt (Datum und Uhrzeit), zu dem der Vorfall erstmals erkannt wurde.

Datum und Uhrzeit der Klassifizierung des Vorfalls: Zeitpunkt (Datum und Uhrzeit), zu dem der Vorfall erstmals klassifiziert wurde.

Vorfall wurde erkannt von: Geben Sie an, ob der Vorfall von einem Zahlungsdienstnutzer oder innerhalb des Zahlungsdienstleisters (z. B. Innenrevision) oder von einer sonstigen, externen Stelle (z. B. externer Dienstleister) erkannt wurde. Trifft keine der Optionen zu, geben Sie bitte eine Erläuterung im entsprechenden Feld an.

Art des Vorfalls: Geben Sie nach bestem Wissen und nach Maßgabe der verfügbaren Informationen an, ob es sich um einen Betriebsvorfall oder einen Sicherheitsvorfall handelt.

Betrieb: Der Vorfall lässt sich auf ungeeignete oder fehlerhafte Prozesse oder Systeme, auf unangemessenes menschliches Verhalten oder menschliches Versagen oder auf höhere Gewalt zurückführen, was sich auf die Integrität, die Verfügbarkeit, die Vertraulichkeit und/oder die Authentizität zahlungsbezogener Dienste auswirkt.

Sicherheit: unbefugter Zugang, unbefugte Nutzung, Offenlegung, Unterbrechung, Änderung oder Vernichtung der Vermögenswerte (Assets) des Zahlungsdienstleisters, was sich auf die Integrität, die Verfügbarkeit, die Vertraulichkeit und/oder die Authentizität zahlungsbezogener Dienste auswirkt. Dies kann u. a. eintreten, wenn die Sicherheit der Netz- oder Informationssysteme bei dem betroffenen Zahlungsdienstleister verletzt wird.

Kriterien für die Meldung eines schwerwiegenden Vorfalls: Bitte geben Sie an, welche Kriterien für die Meldung eines schwerwiegenden Vorfalls ausschlaggebend waren. Es können mehrere Kriterien ausgewählt werden: betroffene Zahlungsvorgänge, betroffene Zahlungsdienstnutzer, Dienstausfallzeit, Verletzung der Sicherheit von Netz- oder Informationssystemen, wirtschaftliche Auswirkungen, hohe interne Eskalationsstufe, andere Zahlungsdienstleister oder maßgebliche Infrastrukturen, die möglicherweise betroffen sind, und/oder Reputationsschäden.

Kurze allgemeine Beschreibung des Vorfalls: Erläutern Sie bitte kurz die maßgeblichsten Probleme des Vorfalls, einschließlich möglicher Ursachen, unmittelbarer Auswirkungen usw.

Auswirkungen in anderen EU-Mitgliedstaaten, sofern gegeben: Erläutern Sie bitte kurz, welche Auswirkungen der Vorfall in einem anderen Mitgliedstaat hatte (z. B. auf Zahlungsdienstnutzer, Zahlungsdienstleister und/oder Zahlungsinfrastrukturen). Bitte fügen Sie eine Übersetzung ins Englische bei, wenn dies innerhalb der Meldefristen möglich ist.

Meldung an andere Behörden: Falls zum Zeitpunkt der Meldung bekannt, geben Sie bitte an, ob der Vorfall im Rahmen anderer Meldesysteme an andere Behörden gemeldet wurde oder gemeldet werden wird. Bitte nennen Sie in diesem Fall die entsprechenden Behörden.

Gründe für die verspätete Übermittlung der Erstmeldung: Bitte geben Sie an, aus welchen Gründen Sie länger als 24 Stunden benötigten, um den Vorfall zu klassifizieren.

B Zwischenmeldung

B 1 – Allgemeine Angaben

Nähere Beschreibung des Vorfalls: Beschreiben Sie bitte die Hauptmerkmale des Vorfalls unter Nennung der Angaben zu dem spezifischen Problem und seinem Hintergrund, der Beschreibung seiner Entstehung

und seines Verlaufs sowie der Folgen insbesondere für die Zahlungsdienstnutzer usw. Bitte machen Sie ggf. auch Angaben zur Kommunikation mit den Zahlungsdienstnutzern.

Besteht ein Zusammenhang zu früheren Vorfällen?: Geben Sie bitte an, ob der Vorfall mit früheren Vorfällen in Zusammenhang steht, sofern entsprechende Informationen vorliegen. Wenn ein solcher Zusammenhang besteht, geben Sie bitte die früheren Vorfälle an.

Waren weitere Dienstleister/Dritte betroffen oder beteiligt?: Geben Sie bitte an, ob weitere Dienstleister/Dritte von dem Vorfall betroffen oder daran beteiligt waren, sofern entsprechende Informationen vorliegen. Wenn andere Dienstleister/Dritte beteiligt oder betroffen waren, führen Sie diese bitte auf und machen Sie nähere Angaben.

Wurde das (interne und/oder externe) Krisenmanagement ausgelöst?: Bitte geben Sie an, ob das (interne oder externe) Krisenmanagement ausgelöst wurde. Wenn das Krisenmanagement ausgelöst wurde, machen Sie bitte nähere Angaben.

Datum und Uhrzeit des Beginns des Vorfalls: Zeitpunkt (Datum und Uhrzeit), zu dem der Vorfall begann, sofern bekannt.

Zeitpunkt (Datum und Uhrzeit), zu dem der Vorfall behoben wurde oder voraussichtlich behoben wird: Geben Sie den Zeitpunkt (Datum und Uhrzeit) an, zu dem der Vorfall unter Kontrolle war oder voraussichtlich sein wird und zu dem der Regelbetrieb wiederhergestellt war oder voraussichtlich wiederhergestellt sein wird.

Betroffene Funktionsbereiche: Geben Sie an, welche Schritte des Zahlungsprozesses von dem Vorfall betroffen waren, z. B. Authentifizierung/Autorisierung, Kommunikation, Clearing, direkte Abwicklung, indirekte Abwicklung oder andere.

> **Authentifizierung/Autorisierung:** Verfahren, mit deren Hilfe der Zahlungsdienstleister die Identität eines Zahlungsdienstnutzers oder die berechtigte Verwendung eines bestimmten Zahlungsinstruments überprüfen kann, einschließlich der Verwendung der personalisierten Sicherheitsmerkmale des Nutzers und des Einverständnisses des Zahlungsdienstnutzers (oder eines im Namen dieses Nutzers handelnden Dritten) zum Transfer von Geldmitteln.
>
> **Kommunikation:** Informationsfluss zum Zweck der Identifizierung, Authentifizierung, Benachrichtigung und Information zwischen dem kontoführenden Zahlungsdienstleister und Zahlungsauslösedienstleistern, Kontoinformationsdienstleistern, Zahlern, Zahlungsempfängern und anderen Zahlungsdienstleistern.
>
> **Clearing:** Verfahren der Übermittlung, Abstimmung und in einigen Fällen der Bestätigung von Überweisungsaufträgen vor der Verrechnung; dies kann auch die Aufrechnung von Aufträgen und die Erstellung von Schlusspositionen für die Verrechnung umfassen.
>
> **Direkte Abwicklung:** Abschluss einer Transaktion oder einer Verarbeitung mit dem Ziel, die Verpflichtungen der Teilnehmer durch den Transfer von Geldmitteln zu erfüllen, wenn dieser Vorgang vom betroffenen Zahlungsdienstleister selbst ausgeführt wird.
>
> **Indirekte Abwicklung:** Abschluss einer Transaktion oder einer Verarbeitung mit dem Ziel, die Verpflichtungen der Teilnehmer durch den Transfer von Geldmitteln zu erfüllen, wenn dieser Vorgang von einem anderen Zahlungsdienstleister im Namen des betroffenen Zahlungsdienstleisters ausgeführt wird.
>
> **Sonstiges:** Der betroffene Funktionsbereich ist oben nicht aufgeführt. Im Freitextfeld sollten weitere Einzelheiten angegeben werden.

Änderungen gegenüber früheren Meldungen: Bitte geben Sie an, welche Informationen gegenüber früheren Meldungen zum selben Vorfall (Erstmeldung oder Zwischenmeldungen) geändert wurden.

B 2 – Klassifizierung des Vorfalls/Informationen zum Vorfall

Betroffene Zahlungsvorgänge: Die Zahlungsdienstleister sollten angeben, welche Schwellenwerte durch den Vorfall erreicht wurden oder wahrscheinlich erreicht werden (sofern relevant), einschließlich der entsprechenden Zahlen: Anzahl der betroffenen Zahlungsvorgänge, Prozentsatz der betroffenen

Zahlungsvorgänge im Verhältnis zur Anzahl der Zahlungsvorgänge, die mit denselben vom Vorfall betroffenen Zahlungsdiensten ausgeführt wurden, sowie Gesamtwert der Zahlungsvorgänge. Die Zahlungsdienstleister sollten spezifische Werte für diese Variablen angeben. Hierbei kann es sich um konkrete Zahlen oder um Schätzungen handeln. Als generelle Regel sollten die Zahlungsdienstleister als „betroffene Zahlungsvorgänge" alle inländischen und grenzüberschreitenden Zahlungsvorgänge erachten, die unmittelbar oder mittelbar von dem Vorfall betroffen waren oder wahrscheinlich betroffen sein werden. Insbesondere sollten darunter solche Vorgänge fallen, 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 (unabhängig davon, ob der Betrag wiedererlangt wurde). Des Weiteren sollten die Zahlungsdienstleister als übliches Volumen der Zahlungsvorgänge den jährlichen Tagesdurchschnitt der mit denselben Zahlungsdiensten ausgeführten inländischen und grenzüberschreitenden Zahlungsvorgänge erachten, die von dem Vorfall betroffen waren, wobei für die Berechnungen das Vorjahr als Bezugszeitraum heranzuziehen ist. Falls die Zahlungsdienstleister diesen Wert als nicht repräsentativ erachten (z. B. aufgrund siasonaler Schwankungen), sollten sie stattdessen eine andere, repräsentativere Messzahl verwenden und der zuständigen Behörde im Feld „Anmerkungen" das diesem Ansatz zugrunde liegende Prinzip mitteilen. In Fällen, in denen Zahlungsvorgänge in anderen Währungen als dem Euro von dem Vorfall betroffen sind, sollten die betroffenen Zahlungsdienstleister bei der Berechnung der Schwellenwerte und bei der Meldung des Werts der Transaktionen deren Betrag in der anderen Währung in Euro umrechnen und dabei den täglichen Euro-Referenzkurs der EZB von dem der Vorfallsmeldung vorausgegangenen Tag verwenden.

Betroffene Zahlungsdienstnutzer: Die Zahlungsdienstleister sollten angeben, welche Schwellenwerte durch den Vorfall erreicht wurden oder wahrscheinlich erreicht werden (sofern relevant), einschließlich der entsprechenden Zahlen: Gesamtzahl der betroffenen Zahlungsdienstnutzer und Prozentsatz der betroffenen Zahlungsdienstnutzer im Verhältnis zu ihrer Gesamtzahl. Die Zahlungsdienstleister sollten spezifische Werte für diese Variablen angeben. Hierbei kann es sich um konkrete Zahlen oder um Schätzungen handeln. Die Zahlungsdienstleister sollten als „betroffene Zahlungsdienstnutzer" alle Kunden (inländische oder ausländische, Verbraucher oder Unternehmen) erachten, 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 wahrscheinlich genutzt haben oder hätten, sollten die Zahlungsdienstleister Schätzungen heranziehen, die auf früheren Aktivitäten beruhen. Im Falle von Gruppen sollte jeder Zahlungsdienstleister nur die eigenen Zahlungsdienstnutzer berücksichtigen. Falls ein Zahlungsdienstleister Anderen operationelle Dienste bereitstellt, sollte dieser Zahlungsdienstleister nur die eigenen Zahlungsdienstnutzer (sofern vorhanden) berücksichtigen. Die Zahlungsdienstleister, welche diese operationellen Dienste erhalten, sollten den Vorfall ebenfalls in Bezug auf ihre eigenen Zahlungsdienstnutzer bewerten. Des Weiteren sollten Zahlungsdienstleister als Gesamtzahl der Zahlungsdienstnutzer die aggregierte Anzahl der inländischen und grenzüberschreitenden Zahlungsdienstnutzer verwenden, die zum Zeitpunkt des Vorfalls vertraglich an sie 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.

Verletzung der Sicherheit von Netz- oder Informationssystemen: Die Zahlungsdienstleister sollten feststellen, 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.

Dienstausfallzeit: Die Zahlungsdienstleister sollten angeben, ob die Schwellenwerte durch den Vorfall erreicht wurden oder wahrscheinlich erreicht werden, einschließlich der entsprechenden Zahlen:

gesamte Dienstausfallzeit. Die Zahlungsdienstleister sollten spezifische Werte für diese Variable angeben. Hierbei kann es sich um konkrete Zahlen oder um Schätzungen handeln. Die Zahlungsdienstleister sollten den Zeitraum 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 i) die Auslösung und/oder Ausführung eines Zahlungsdienstes und/oder ii) der Zugang zu einem Zahlungskonto verhindert werden. Die Dienstausfallzeit sollte ab dem Zeitpunkt des Ausfalls gemessen werden, und die Zahlungsdienstleister sollten sowohl die Zeitspanne berücksichtigen, innerhalb derer sie den für die Ausführung von Zahlungsvorgängen erforderlichen Geschäftsbetrieb unterhalten, als auch die Schließungs- und Wartungszeiten, sofern relevant und anwendbar. Wenn der Beginn der Dienstausfallzeit vom Zahlungsdienstleister nicht bestimmt werden kann, sollte die Ausfallzeit ausnahmsweise ab dem Zeitpunkt gemessen werden, zu dem der Ausfall erkannt wurde.

Wirtschaftliche Auswirkungen: Die Zahlungsdienstleister sollten angeben, ob die Schwellenwerte durch den Vorfall erreicht wurden oder wahrscheinlich erreicht werden, einschließlich der entsprechenden Zahlen: direkte Kosten und indirekte Kosten. Die Zahlungsdienstleister sollten spezifische Werte für diese Variablen angeben. Hierbei kann es sich um konkrete Zahlen oder um Schätzungen handeln. Die Zahlungsdienstleister sollten sowohl die Kosten in Betracht ziehen, die unmittelbar mit dem Vorfall in Verbindung gebracht werden können, als auch diejenigen, die mittelbar mit dem Vorfall in Zusammenhang stehen. Unter anderem sollten veruntreute Gelder oder Vermögenswerte, Kosten für den Ersatz von Hard- oder Software, sonstige forensische oder Wiederherstellungskosten, Gebühren aufgrund der Nichteinhaltung vertraglicher Verpflichtungen, Sanktionen, Auslandsverbindlichkeiten und entgangene Einnahmen berücksichtigt werden. Im Hinblick auf indirekte Kosten sollten nur die bereits bekannten oder die aller Wahrscheinlichkeit nach entstehenden Kosten berücksichtigt werden. In Fällen, in denen die Kosten in anderen Währungen als dem Euro anfallen, sollten die betroffenen Zahlungsdienstleister bei der Berechnung der Schwellenwerte und bei der Meldung des Werts der wirtschaftlichen Auswirkungen den Kostenbetrag in der anderen Währung in Euro umrechnen und dabei den täglichen Euro-Referenzkurs der EZB von dem der Vorfallsmeldung vorausgegangenen Tag verwenden.

> **Direkte Kosten:** Geldbetrag (in Euro) der vom Vorfall direkt verursachten Kosten, einschließlich des zur Behebung des Vorfalls benötigten Betrags (z. B. veruntreute Gelder oder Vermögenswerte, Kosten für den Ersatz von Hard- und Software, Gebühren aufgrund der Nichteinhaltung vertraglicher Verpflichtungen).
>
> **Indirekte Kosten:** Geldbetrag (in Euro) der vom Vorfall indirekt verursachten Kosten (z. B. durch Kundenreklamationen/Entschädigung von Kunden, mögliche Prozesskosten).

Hohe interne Eskalationsstufe: Die Zahlungsdienstleister sollten prüfen, ob aufgrund der Beeinträchtigung zahlungsbezogener Dienste das Leitungsorgan im Sinne der EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken nach Maßgabe der Leitlinie 60 Buchstabe d besagter Leitlinien außerhalb des regelmäßigen Meldeverfahrens sowie fortlaufend während der Dauer des Vorfalls über den Vorfall informiert wurde oder wahrscheinlich informiert werden wird. Des Weiteren sollten die Zahlungsdienstleister in Erwägung ziehen, ob infolge der Auswirkungen des Vorfalls auf zahlungsbezogene Dienste ein Krisenmodus ausgelöst wurde oder wahrscheinlich ausgelöst werden wird.

Andere Zahlungsdienstleister/maßgebliche Infrastrukturen, die möglicherweise betroffen sind: Die Zahlungsdienstleister sollten die Auswirkungen des Vorfalls auf den Finanzmarkt bewerten, wobei darunter die Finanzmarktinfrastrukturen und/oder die Zahlungssysteme zu verstehen sind, auf die sich der betroffene Zahlungsdienstleister sowie andere Zahlungsdienstleister stützen. Insbesondere sollte bewertet werden, 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 Stabilität

des Finanzsystems insgesamt beeinträchtigt hat oder wahrscheinlich beeinträchtigen wird. Dabei sollten die Zahlungsdienstleister verschiedene Aspekte berücksichtigen, z. B. ob die betroffene Komponente oder Software urheberrechtlich geschützt 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.

Reputationsschäden: Die Zahlungsdienstleister sollten den Grad der Sichtbarkeit betrachten, den der Vorfall nach ihrem besten Wissen auf dem Markt erlangt hat oder wahrscheinlich erlangen wird. Insbesondere die Wahrscheinlichkeit, dass der Vorfall auch die Gesellschaft schädigt, sollte den Zahlungsdienstleistern als geeigneter Indikator dienen, um das ihm innewohnende Potenzial zur Schädigung ihrer Reputation zu bestimmen. Die Zahlungsdienstleister sollten berücksichtigen, ob i) die Zahlungsdienstnutzer und/oder andere Zahlungsdienstleister sich über nachteilige Auswirkungen des Vorfalls beschwert haben, ii) der Vorfall einen sichtbaren Prozess im Zusammenhang mit Zahlungsdiensten betraf und daher in den Medien wahrscheinlich Beachtung findet oder bereits gefunden hat (nicht nur in herkömmlichen Medien wie Zeitungen, sondern auch in Blogs, sozialen Netzwerken usw.), wobei einige wenige negative Kommentare von Followern in diesem Zusammenhang nicht als „Beachtung in den Medien“ zu werten sind, sondern nur ein ausgearbeiteter Bericht oder eine signifikante Anzahl negativer Kommentare/Warnungen, iii) vertragliche Verpflichtungen nicht erfüllt wurden oder wahrscheinlich nicht erfüllt werden, sodass die Veröffentlichung rechtlicher Schritte gegen den Zahlungsdienstleister zu erwarten ist, iv) aufsichtsrechtliche Pflichten nicht eingehalten wurden, sodass aufsichtsbehördliche Maßnahmen oder Sanktionen verhängt werden, die öffentlich bekannt wurden oder wahrscheinlich werden, und ob v) ein Vorfall ähnlicher Art bereits zuvor aufgetreten ist.

B 3 – Beschreibung des Vorfalls

Art des Vorfalls: Betriebsvorfall oder Sicherheitsvorfall. Nähere Erläuterungen finden Sie im entsprechenden Feld der Erstmeldung.

Ursache des Vorfalls: Geben Sie die Ursache des Vorfalls an oder, falls diese noch nicht bekannt ist, die wahrscheinlichste Ursache. Sie können mehrere Kästchen ankreuzen.

In Untersuchung: Bitte kreuzen Sie dieses Feld an, wenn die Ursache derzeit noch nicht bekannt ist.

Böswillige Handlung: Handlungen, mit denen der Zahlungsdienstleister vorsätzlich geschädigt wird. Hierzu gehören Schadsoftware, Ausspähen, Eindringen in IT-Systeme, (Distributed-)Denial-of-Service-Angriffe (D/DoS), vorsätzliche interne Handlungen, vorsätzliche physische Beschädigung von außen, Verletzungen der Datensicherheit, betrügerische Handlungen und anderes. Weitere Einzelheiten sind Abschnitt C 2 der Vorlage zu entnehmen.

Prozessfehler: Der Vorfall ist auf eine unzulängliche Gestaltung oder Ausführung des Zahlungsprozesses, der Prozesssteuerungen und/oder der unterstützenden Prozesse zurückzuführen (z. B. eines für Änderung/Migration, Testen, Konfiguration, Kapazität oder Überwachung eingesetzten Prozesses).

Systemfehler: Die Ursache des Vorfalls hängt damit zusammen, dass die Gestaltung, Ausführung, Komponenten, Spezifikationen, Integration oder Komplexität der Systeme, die die Zahlungstätigkeit unterstützen, unzulänglich sind.

Menschliches Versagen: Der Vorfall wurde durch einen unbeabsichtigten Fehler einer Person verursacht, entweder als Teil des Zahlungsverfahrens (z. B. Hochladen der falschen Zahlungs-Batchdatei in das Zahlungssystem) oder auf irgendeine Weise damit verbunden (z. B. durch eine unbeabsichtigte Unterbrechung der Stromversorgung, wodurch die Zahlungstätigkeit ausgesetzt wurde).

Externe Ereignisse: Die Ursache steht mit Ereignissen in Zusammenhang, die in der Regel außerhalb der Kontrolle des Unternehmens liegen (z. B. Naturkatastrophen, Fehler bei einem technischen Dienstleister).

Sonstiges: Der Vorfall lässt sich auf keine der oben stehenden Ursachen zurückführen. Im Freitextfeld sollten weitere Einzelheiten angegeben werden.

Waren Sie direkt oder indirekt durch einen Dienstleister von dem Vorfall betroffen?: Falls entsprechende Informationen verfügbar sind, geben Sie bitte an, ob der Vorfall den Zahlungsdienstleister direkt betraf oder indirekt vermittels eines Dritten. Falls Sie indirekt betroffen waren, geben Sie bitte den Namen des/der Dienstleister(s) an.

B 4 – Auswirkungen des Vorfalls

Gesamtauswirkung: Bitte geben Sie an, welche Schutzziele von dem Betriebs- oder Sicherheitsvorfall betroffen waren. Sie können mehrere Kästchen ankreuzen.

Integrität: die Eigenschaft, die Richtigkeit und Vollständigkeit von Vermögenswerten (einschließlich Daten) zu schützen.

Verfügbarkeit: die Eigenschaft, dass zahlungsbezogene Dienste im vorab festgelegten akzeptablen 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.

Authentizität: die Eigenschaft einer Quelle, tatsächlich das zu sein, was sie zu sein vorgibt.

Betroffene Geschäftskanäle: Geben Sie den Kanal oder die Kanäle an, über die die Interaktion mit den Zahlungsdienstnutzern erfolgt und die vom Vorfall betroffen waren. Sie können mehrere Kästchen ankreuzen.

Zweigniederlassungen: eine Geschäftsstelle, die nicht die Hauptverwaltung ist und die einen Teil eines Zahlungsdienstleisters bildet, keine Rechtspersönlichkeit hat und unmittelbar sämtliche oder einen Teil der Geschäfte betreibt, die mit der Tätigkeit eines Zahlungsdienstleisters verbunden sind. Alle Geschäftsstellen eines Zahlungsdienstleisters mit Hauptverwaltung in einem anderen Mitgliedstaat, die sich in ein und demselben Mitgliedstaat befinden, gelten als eine einzige Zweigniederlassung.

E-Banking: die Nutzung von Computern zur Ausführung von Finanzgeschäften über das Internet.

Telefonbanking: die Ausführung von Finanzgeschäften über das Telefon.

Mobile Banking: die Nutzung einer speziellen Bankanwendung auf einem Smartphone oder einem ähnlichen Gerät zur Ausführung von Finanzgeschäften.

Geldautomaten: elektromechanische Geräte, die Zahlungsdienstnutzern die Abhebung von Bargeld von ihren Konten und/oder den Zugang zu anderen Diensten ermöglichen.

Verkaufsstelle: realer Geschäftsraum des Händlers, in denen der Zahlungsvorgang veranlasst wird.

E-Commerce: die Nutzung einer virtuellen Verkaufsstelle zur Veranlassung des Zahlungsvorgangs (z. B. Nutzung des Internets zur Veranlassung von Zahlungen mithilfe von Überweisungen, Zahlungskarten, Transfer von elektronischem Geld zwischen E-Geld-Konten.

Sonstiges: Der betroffene Geschäftskanal ist oben nicht aufgeführt. Im Freitextfeld sollten weitere Einzelheiten angegeben werden.

Betroffene Zahlungsdienste: Geben Sie die Zahlungsdienste an, die infolge des Vorfalls nicht korrekt funktionieren. Sie können mehrere Kästchen ankreuzen.

Bareinzahlung auf ein Zahlungskonto: die Übergabe von Bargeld an einen Zahlungsdienstleister zwecks Gutschrift des Betrags auf einem Zahlungskonto.

Barabhebung von einem Zahlungskonto: der bei einem Zahlungsdienstleister von seinem Zahlungsdienstnutzer eingegangene Auftrag zur Bereitstellung von Bargeld und Belastung des Zahlungskontos des Zahlungsdienstnutzers mit dem entsprechenden Betrag.

Zur Führung eines Zahlungskontos erforderliche Vorgänge: alle Vorgänge, die für ein Zahlungskonto auszuführen sind, um es zu aktivieren, zu deaktivieren und/oder zu verwalten (z. B. Eröffnen oder Sperren eines Kontos).

Annahme und Abrechnung von Zahlungsvorgängen (Acquiring): ein den Transfer von Geldbeträgen zum Zahlungsempfänger bewirkender Zahlungsdienst eines Zahlungsdienstleisters, der mit einem Zahlungsempfänger eine vertragliche Vereinbarung über die Annahme und die Verarbeitung von Zahlungsvorgängen schließt.

Überweisung: ein auf Aufforderung des Zahlers ausgelöster Zahlungsdienst zur Erteilung einer Gutschrift auf das Zahlungskonto des Zahlungsempfängers zulasten des Zahlungskontos des Zahlers in Ausführung eines oder mehrerer Zahlungsvorgänge durch den Zahlungsdienstleister, der das Zahlungskonto des Zahlers führt.

Lastschrift: Zahlungsdienst zur Belastung des Zahlungskontos des Zahlers, wenn ein Zahlungsvorgang vom Zahlungsempfänger aufgrund der Zustimmung des Zahlers gegenüber dem Zahlungsempfänger, dessen Zahlungsdienstleister oder seinem eigenen Zahlungsdienstleister ausgelöst wird.

Kartenzahlung: Zahlungsdienst, der auf der Infrastruktur und den Geschäftsregeln eines Zahlungskartensystems beruht, um mithilfe einer Karte oder eines Telekommunikations-, Digital- oder IT-Geräts oder einer entsprechenden Software eine Zahlung auszuführen, wenn sich daraus eine Debit- oder eine Kreditkartentransaktion ergibt. Nicht als kartengebundene Zahlungsvorgänge zu betrachten sind Vorgänge, die an andere Arten von Zahlungsdiensten geknüpft sind.

Ausgabe von Zahlungsinstrumenten: Zahlungsdienst, bei dem ein Zahlungsdienstleister eine vertragliche Vereinbarung mit einem Zahler schließt, um diesem ein Zahlungsinstrument zur Auslösung und Verarbeitung der Zahlungsvorgänge des Zahlers zur Verfügung zu stellen.

Finanztransfer: Zahlungsdienst, bei dem ohne Einrichtung eines Zahlungskontos auf den Namen des Zahlers oder des Zahlungsempfängers ein Geldbetrag eines Zahlers nur zum Transfer eines entsprechenden Betrags an einen Zahlungsempfänger oder an einen anderen, im Namen des Zahlungsempfängers handelnden Zahlungsdienstleister entgegengenommen wird und/oder bei dem der Geldbetrag im Namen des Zahlungsempfängers entgegengenommen und diesem verfügbar gemacht wird.

Zahlungsauslösedienste: Zahlungsdienst, der auf Antrag des Zahlungsdienstnutzers einen Zahlungsauftrag in Bezug auf ein bei einem anderen Zahlungsdienstleister geführtes Zahlungskonto auslöst.

Kontoinformationsdienste: Online-Zahlungsdienst zur Mitteilung konsolidierter Informationen über ein Zahlungskonto oder mehrere Zahlungskonten, das/die ein Zahlungsdienstnutzer entweder bei einem anderen Zahlungsdienstleister oder bei mehr als einem Zahlungsdienstleister hält.

B 5 – Begrenzung der Auswirkungen des Vorfalls

Welche Maßnahmen wurden bisher ergriffen oder sind geplant, um den Vorfall zu beheben?: Geben Sie bitte Einzelheiten zu den Maßnahmen an, die ergriffen wurden oder geplant sind, um vorübergehend auf den Vorfall zu reagieren.

Wurde(n) der Plan zur Fortführung des Geschäftsbetriebs und/oder der Plan zur Wiederherstellung des Normalbetriebs aktiviert?: Geben Sie bitte an, ob ein solcher Plan aktiviert wurde, und wenn ja,

geben Sie die wichtigsten Einzelheiten der jeweiligen Vorgehensweise an (z. B. wann die Aktivierung des Plans erfolgte und welche darin vorgesehenen Maßnahmen ergriffen wurden).

C – Abschlussmeldung

C 1 – Allgemeine Angaben

Aktualisierung der Informationen aus der Erstmeldung und den Zwischenmeldungen (Zusammenfassung): Machen Sie bitte weitere Angaben zum Vorfall, insbesondere zu den spezifischen Änderungen gegenüber den Informationen in der letzten Zwischenmeldung. Bitte schließen Sie auch sonstige relevante Informationen ein.

Sind alle ursprünglichen Kontrollen in Kraft?: Geben Sie bitte an, ob der Zahlungsdienstleister zu irgendeinem Zeitpunkt während des Vorfalls einige Kontrollen außer Kraft setzen musste. Falls ja, geben Sie bitte an, ob alle Kontrollen wieder in Kraft sind, und falls nein, erläutern Sie bitte im Freitextfeld, welche Kontrollen nicht wieder in Kraft sind und wie viel Zeit für ihre Wiederherstellung noch erforderlich ist.

C 2 – Ursachenanalyse und Folgemaßnahmen

Welches war die Hauptursache des Vorfalls, sofern bereits bekannt?: Geben Sie bitte an, worin die Hauptursache des Vorfalls bestand, oder, falls diese noch nicht bekannt ist, die wahrscheinlichste solche Ursache. Sie können mehrere Kästchen ankreuzen. (Bitte achten Sie darauf, zwischen der Hauptursache und den Auswirkungen des Vorfalls zu unterscheiden.)

- **Böswillige Handlung:** externe oder interne Handlungen, mit denen der Zahlungsdienstleister vorsätzlich geschädigt wird. Diese werden in folgende Kategorien eingeteilt:
  - **Schadsoftware:** z. B. ein Computervirus, Computerwurm, Trojaner, Spionage-Software.
  - **Ausspähen:** z. B. Portscanning, Sniffing, Social Engineering.
  - **Eindringen:** z. B. Kompromittierung privilegierter oder nicht privilegierter Benutzerkonten, Kompromittierung von Anwendungen, Bots.
  - **(Distributed) Denial of Service (D/DoS):** Versuch, die Verfügbarkeit eines Online-Diensts zu blockieren, indem er mit riesigem Datenverkehr aus mehreren Quellen überschüttet wird.
  - **Vorsätzliche interne Handlungen:** z. B. Sabotage oder Diebstahl.
  - **Vorsätzliche physische Beschädigung von außen:** z. B. Sabotage, physische Angriffe auf Anlagen/Rechenzentren.
  - **Verletzung der Datensicherheit:** unbefugter Zugriff auf Informationen, unbefugte Änderung von Informationen.
  - **Betrügerische Handlungen:** unbefugte Verwendung von Ressourcen, Urheberrechtsverletzungen, Maskerade, Phishing.
  - **Sonstiges (bitte angeben):** Der Vorfall lässt sich auf keine der oben stehenden Ursachen zurückführen. Im Freitextfeld sollten weitere Einzelheiten angegeben werden.
- **Prozessfehler:** Der Vorfall ist auf eine unzulängliche Gestaltung oder Ausführung des Zahlungsprozesses, der Prozesssteuerungen und/oder der unterstützenden Prozesse zurückzuführen (z. B. eines für Änderung/Migration, Testen, Konfiguration, Kapazität oder Überwachung eingesetzten Prozesses). Diese werden in folgende Kategorien eingeteilt:
  - **Mangelhafte Überwachung und Kontrolle:** z. B. in Bezug auf den laufenden Betrieb, das Auslaufen von Zertifikaten, Lizenzen oder Patches, maximale Zählerwerte, Datenbank-Füllstände, Benutzerrechteverwaltung oder Vieraugenprinzip.
  - **Kommunikationsprobleme:** z. B. zwischen Marktteilnehmern oder innerhalb der Organisation.
  - **Unsachgemäßer Betrieb:** z. B. kein Austausch von Zertifikaten oder voller Cache.

Unzulängliches Change Management: z. B. nicht erkannte Konfigurationsfehler, keine Beachtung von Aktualisierungen bei der Einführung von neuer Software, Wartungsprobleme oder unvorhergesehene Fehler.

Unzulängliche interne Verfahren und interne Dokumentation: z. B. keine Transparenz im Hinblick auf Funktionen und Prozesse, Auftreten von Funktionsfehlern oder keine Dokumentation.

Wiederherstellungsprobleme: z. B. Probleme beim Notfallmanagement oder unzureichende Redundanz.

Sonstiges (bitte angeben): Der Vorfall lässt sich auf keine der oben stehenden Ursachen zurückführen. Im Freitextfeld sollten weitere Einzelheiten angegeben werden.

Systemfehler: Die Ursache des Vorfalls hängt damit zusammen, dass die Gestaltung, Ausführung, Komponenten, Spezifikationen, Integration oder Komplexität der Systeme, die die Zahlungstätigkeit unterstützen, unzulänglich sind. Diese werden in folgende Kategorien eingeteilt:

Hardwarefehler: Ausfall physischer technischer Ausrüstung, die die Prozesse ausführt und/oder die Daten speichert, die von Zahlungsdienstleistern für die Erfüllung ihrer zahlungsbezogenen Aktivitäten erforderlich sind (z. B. Ausfall von Festplatten, Rechenzentren oder anderer Infrastruktur).

Netzfehler: Ausfall von öffentlichen oder privaten Telekommunikationsnetzen, die dem Austausch von Daten und Informationen (z. B. über das Internet) während des Zahlungsprozesses dienen.

Datenbankfehler: Probleme mit der Datenstruktur zur Speicherung von personenbezogenen Daten und Zahlungsdaten, die für die Ausführung von Zahlungsvorgängen benötigt werden.

Software-/Anwendungsfehler: Ausfall (z. B. Fehlfunktionen, unbekannte Funktionen) von Programmen, Betriebssystemen usw., mit denen die Bereitstellung von Zahlungsdiensten durch den Zahlungsdienstleister unterstützt wird.

Physische Beschädigung: z. B. versehentliche Beschädigung durch ungeeignete Bedingungen oder Bauarbeiten.

Sonstiges (bitte angeben): Der Vorfall lässt sich auf keine der oben aufgeführten Ursachen zurückführen. Im Freitextfeld sollten weitere Einzelheiten angegeben werden.

Menschliches Versagen: Der Vorfall wurde durch einen unbeabsichtigten Fehler einer Person verursacht, entweder als Teil des Zahlungsverfahrens (z. B. Hochladen der falschen Zahlungs-Batchdatei in das Zahlungssystem) oder auf irgendeine Weise damit verbunden (z. B. durch eine unbeabsichtigte Unterbrechung der Stromversorgung, wodurch die Zahlungstätigkeit ausgesetzt wurde). Diese werden in folgende Kategorien eingeteilt:

Versehen: z. B. Fehler, Irrtümer, Unterlassungen, Mangel an Erfahrung und Wissen.

Versäumnis: z. B. aufgrund mangelnder Qualifikationen, Kenntnisse, Erfahrung oder Sensibilisierung.

Unzureichende Ressourcen: z. B. Personalmangel oder mangelnde Verfügbarkeit von Personal.

Sonstiges (bitte angeben): Der Vorfall lässt sich auf keine der oben aufgeführten Ursachen zurückführen. Im Freitextfeld sollten weitere Einzelheiten angegeben werden.

Externes Ereignis: Die Ursache hängt mit Ereignissen zusammen, die außerhalb der Kontrolle des Unternehmens liegen. Diese werden in folgende Kategorien eingeteilt:

Fehler eines Dienstleisters/Anbieters technischer Dienste: z. B. Stromausfall, Internetausfall, rechtliche Probleme, geschäftliche Probleme, Abhängigkeit zwischen Diensten.

Höhere Gewalt: z. B. Ausfall des Stromnetzes, Feuer, Naturereignisse wie Erdbeben, Hochwasser, Starkniederschläge oder Sturm.

Sonstiges (bitte angeben): Der Vorfall lässt sich auf keine der oben aufgeführten Ursachen zurückführen. Im Freitextfeld sollten weitere Einzelheiten angegeben werden.

Sonstiges: Der Vorfall lässt sich auf keine der oben stehenden Ursachen zurückführen. Im Freitextfeld sollten weitere Einzelheiten angegeben werden.

Sonstige relevante Informationen zur Hauptursache: Geben Sie bitte weitere Einzelheiten zur Hauptursache an, einschließlich der vorläufigen Schlussfolgerungen aus der Ursachenanalyse.

Wichtigste ergriffene oder geplante Abhilfemaßnahmen, um ein erneutes Auftreten des Vorfalls künftig zu verhindern, sofern bereits bekannt: Geben Sie bitte die wichtigsten Maßnahmen an, die ergriffen wurden oder geplant sind, um ein erneutes Auftreten des Vorfalls künftig zu verhindern.

C 3 – Zusätzliche Informationen

Wurde der Vorfall einem anderen Zahlungsdienstleister zu Informationszwecken mitgeteilt?: Geben Sie bitte an, welche Zahlungsdienstleister formell oder informell kontaktiert wurden, um sie über den Vorfall zu unterrichten. Geben Sie Einzelheiten zu den informierten Zahlungsdienstleistern, die mitgeteilten Informationen und die Gründe für diesen Informationsaustausch an.

Wurden rechtliche Schritte gegen den Zahlungsdienstleister unternommen?: Geben Sie bitte an, ob zum Zeitpunkt der Abschlussmeldung infolge des Vorfalls rechtliche Schritte gegen den Zahlungsdienstleister unternommen wurden (liegt z. B. eine Klage vor Gericht vor, oder hat er seine Zulassung verloren).

Bewertung der Wirksamkeit der ergriffenen Maßnahmen: Stellen Sie bitte, sofern verfügbar, eine Eigenbewertung in Bezug auf die Wirksamkeit der während der Vorfallsdauer ergriffenen Maßnahmen bereit, in der auch die Lehren aus dem Vorfall behandelt werden.