EBA/GL/2017/10

19/12/2017

Leitlinien

für die Meldung schwerwiegender Vorfälle gemäß der Richtlinie (EU) 2015/2366 (PSD 2)

1. Einhaltung der Vorschriften und Meldepflichten

Status dieser Leitlinien

1. Das vorliegende Dokument enthält Leitlinien, die gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010 herausgegeben wurden. [1] Gemäß Artikel 16 Artikel 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden und 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. Dazu sollten die zuständigen Behörden gemäß Artikel 2 Absatz 4 der Verordnung (EU) Nr. 1093/2010 die an sie gerichteten Leitlinien in geeigneter Weise in ihre Aufsichtspraktiken (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren) integrieren, einschließlich der Leitlinien in diesem Dokument, die in erster Linie an Institute gerichtet sind.

Meldepflichten

3. Nach Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden der EBA bis zum 19/02/2018 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 zuständige Behörde den Anforderungen nicht nachkommt. Die Mitteilungen sind unter Verwendung des auf der Website der EBA abrufbaren Formulars mit dem Betreff „EBA/GL/2017/10“ an compliance@eba.europa.eu zu senden. Die Mitteilungen sollten durch Personen erfolgen, die befugt sind, entsprechende Meldungen im Auftrag ihrer Behörde zu übermitteln. 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 oben genannten Richtlinie 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 des Vorfalls und die Einzelheiten der Vorfallsmeldungen bewerten sollten, über die sie andere nationale Behörden gemäß Artikel 96 Absatz 2 der genannten Richtlinie unterrichten müssen.

8. Darüber hinaus enthalten diese Leitlinien ebenfalls 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 Richtlinie (EU) 2015/2366.

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, in böswilliger Absicht oder versehentlich 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.

Adressaten

12. Die erste Gruppe der Leitlinien (Abschnitt 4) richtet sich an Zahlungsdienstleister gemäß der Definition in Artikel 4 Absatz 11 der Richtlinie (EU) 2015/2366 sowie an solche, die in Artikel 4 Absatz 1 der Verordnung (EU) Nr. 1093/2010 genannt sind.

13. Die zweite und dritte Gruppe der Leitlinien (Abschnitte 5 und 6) richten sich an die zuständigen Behörden gemäß der Definition in Artikel 4 Absatz 2 Ziffer i der Verordnung (EU) Nr. 1093/2010.

Begriffsbestimmungen

14. Sofern nicht anders angegeben, haben die in der Richtlinie (EU) 2015/2366 verwendeten und definierten Begriffe in den Leitlinien dieselbe Bedeutung. Für die Zwecke dieser Leitlinien gelten darüber hinaus die folgenden Begriffsbestimmungen:

Betriebs- oder Sicherheitsvorfall	Ein einzelnes Ereignis, oder eine Reihe zusammenhängender Ereignisse, das vom Zahlungsdienstleister nicht beabsichtigt wurde und das sich negativ auf die Integrität, die Verfügbarkeit, die Vertraulichkeit, die Authentizität und/oder die Kontinuität von zahlungsbezogenen Diensten auswirkt oder aller Wahrscheinlichkeit nach eine solche negative Auswirkung haben wird
Integrität	Die Eigenschaft, die Korrektheit und Vollständigkeit von Vermögenswerten (einschließlich Daten) zu schützen
Verfügbarkeit	Die Eigenschaft, dass zahlungsbezogene Dienste 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
Kontinuität	Die Eigenschaft, dass die für die Erbringung der zahlungsbezogenen Dienste erforderlichen Prozesse, Aufgaben und Vermögenswerte einer Organisation in vollem Umfang zugänglich und auf einem annehmbaren vordefinierten Niveau funktionsfähig sind
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

15. Diese Leitlinien gelten ab dem 13. Januar 2018.

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. Die Zahlungsdienstleister sollten folgende Vorfälle 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. Die Zahlungsdienstleister sollten einen Betriebs- oder Sicherheitsvorfall anhand der folgenden Kriterien und den zugrunde liegenden Indikatoren bewerten:

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 Anzahl der betroffenen Zahlungsdienstnutzer sollte als absolute Zahl sowie als Prozentsatz der Gesamtzahl der Zahlungsdienstnutzer bestimmt werden.

iii. Dienstausfallzeit

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

iv. 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.

v. Hohe interne Eskalationsstufe

Die Zahlungsdienstleister sollten bestimmen, ob der betreffende Vorfall ihren Führungskräften gemeldet wurde oder diesen höchstwahrscheinlich gemeldet wird.

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

Die Zahlungsdienstleister sollten die systemischen Auswirkungen bestimmen, die der Vorfall höchstwahrscheinlich hat, d. h., inwieweit der Vorfall sich über den ursprünglich betroffenen Zahlungsdienstleister hinaus auf andere Zahlungsdienstleister, Finanzmarktinfrastrukturen und/oder Zahlungskartensysteme auswirken kann.

vii. 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 unmittelbar oder mittelbar von dem Vorfall betroffen waren oder höchstwahrscheinlich 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. Wenn die Zahlungsdienstleister diesen Wert als nicht repräsentativ erachten (z. B. aufgrund der Saisonalität), sollten sie stattdessen eine andere repräsentativere Messzahl verwenden und der zuständigen Behörde im betreffenden Feld des Formblatts (siehe Anhang 1) das diesem Ansatz zugrunde liegende Prinzip mitteilen.

ii. Betroffene Zahlungsdienstnutzer

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 höchstwahrscheinlich 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 erhalten, sollten den Vorfall 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.

iii. 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 höchstwahrscheinlich 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 gezählt werden, und die Zahlungsdienstleister sollten sowohl die Zeitspanne berücksichtigen, innerhalb der sie den für die Ausführung von Zahlungsvorgängen erforderlichen Geschäftsbetrieb unterhalten, als auch die Schließungs- und Wartungszeiten, sofern relevant und anwendbar. Falls der Zahlungsdienstleister den Beginn der Dienstausfallzeit nicht bestimmen kann, sollte er die Ausfallzeit ausnahmsweise ab dem Zeitpunkt zählen, zu dem der Ausfall erkannt wurde.

iv. Wirtschaftliche Auswirkungen

Die Zahlungsdienstleister sollten 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.

v. *Hohe interne Eskalationsstufe*

Die Zahlungsdienstleister sollten erwägen, ob infolge der Auswirkung des Vorfalls auf zahlungsbezogene Dienste der Chief Information Officer (oder eine vergleichbare Position) außerhalb des regelmäßigen Meldeverfahrens sowie fortlaufend während der Dauer des Vorfalls über den Vorfall informiert wurde oder aller Wahrscheinlichkeit nach informiert wird. Des Weiteren sollten die Zahlungsdienstleister in Erwägung ziehen, ob infolge der Auswirkung des Vorfalls auf zahlungsbezogene Dienste ein Krisenmodus ausgelöst wurde oder voraussichtlich ausgelöst wird.

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

Die Zahlungsdienstleister sollten die Auswirkung des Vorfalls auf den Finanzmarkt bewerten, wobei darunter die Finanzmarktinfrastrukturen und/oder die Zahlungskartensysteme 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 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.

vii. *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 sollten die Zahlungsdienstleister die Einschätzung, inwiefern der Vorfall voraussichtlich die Gesellschaft schädigt, als nützlichen Indikator heranziehen, um das dem Vorfall innewohnende Potenzial zur Schädigung ihrer Reputation zu bestimmen. Die Zahlungsdienstleister sollten berücksichtigen, ob i) der Vorfall einen sichtbaren Prozess betraf und daher in den Medien vermutlich Beachtung findet oder bereits gefunden hat (wobei nicht nur herkömmliche Medien wie Zeitungen, sondern auch Blogs, soziale Netze usw. einzubeziehen sind), ob ii) aufsichtsrechtliche Pflichten missachtet wurden oder vermutlich missachtet werden, ob iii) gegen Sanktionen verstoßen wurde oder vermutlich verstoßen wird oder ob iv) ein Vorfall der gleichen 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 aller Wahrscheinlichkeit nach 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** > 100.000 EUR	> 25 % des üblichen Transaktionsvolumens des Zahlungsdienstleisters (in Bezug auf die Anzahl der Transaktionen) **oder** > 5 Mio. EUR
Betroffene Zahlungsdienstnutzer	> 5.000 **und** > 10 % der Zahlungsdienstnutzer des Zahlungsdienstleisters	> 50.000 **oder** > 25 % der Zahlungsdienstnutzer des Zahlungsdienstleisters
Dienstausfallzeit	> 2 Stunden	Nicht anwendbar
Wirtschaftliche Auswirkungen	Nicht anwendbar	> Max. (0,1 % Kernkapital (Tier 1) *, 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

*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. 646/2012.

1.5. Falls Zahlungsdienstleister über keine konkreten Daten verfügen, um ihre Beurteilung, ob ein bestimmter Schwellenwert vor Lösung des Vorfalls erreicht oder aller Wahrscheinlichkeit nach 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 (von nicht schwerwiegend in schwerwiegend) oder nach unten (von schwerwiegend in nicht schwerwiegend) – zu ermitteln.

Leitlinie 2: Meldeverfahren

2.1. Die Zahlungsdienstleister sollten alle relevanten Informationen sammeln, eine Vorfallsmeldung unter Verwendung des in Anhang 1 bereitgestellten Formblatts erstellen und diese Meldung der zuständigen Behörde im Herkunftsmitgliedstaat übermitteln. Das Formblatt sollte gemäß den Anleitungen in Anhang 1 ausgefüllt werden.

2.2. Die Zahlungsdienstleister sollten die zuständige Behörde während der Dauer des Vorfalls unter Verwendung des gleichen Formblatts unterrichten (d. h. für Erst-, Zwischen- und Abschlussmeldungen, wie in den Abschnitten 2.7 bis 2.21 beschrieben). Die

Zahlungsdienstleister sollten das Formblatt, nach bestem Bemühen ausfüllen und sukzessive ergänzen, sobald mehr Informationen im Laufe ihrer internen Untersuchungen zutage treten.

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 alle zusätzlichen und verfügbaren Informationen zukommen lassen, die für die zuständige Behörde als maßgeblich erachtet werden, indem dem Standardformblatt die zusätzlichen Unterlagen in Form eines oder mehrerer Anhänge beigefügt werden.

2.5. 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.

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

Erstmeldung

2.7. Die Zahlungsdienstleister sollten der zuständigen Behörde im Herkunftsmitgliedstaat eine Erstmeldung übermitteln, wenn ein schwerwiegender Betriebs- oder Sicherheitsvorfall erstmalig erkannt wird.

2.8. Die Erstmeldung sollte innerhalb von vier Stunden ab der erstmaligen Erkennung des schwerwiegenden Betriebs- oder Sicherheitsvorfalls 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 der zuständigen Behörde im Herkunftsmitgliedstaat ebenfalls eine Erstmeldung übermitteln, sobald ein zuvor nicht schwerwiegender Vorfall zu einem schwerwiegenden Vorfall 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.

2.10. Die Zahlungsdienstleister sollten in ihre Erstmeldung Übersichtsinformationen (in Abschnitt A des Formblatts) aufnehmen, um so einige grundlegende Merkmale des Vorfalls sowie seine voraussichtlichen Folgen anhand der Informationen anzugeben, die unmittelbar

nach Erkennung oder Neuklassifizierung des Vorfalls verfügbar waren. Liegen keine konkreten Daten vor, sollten Zahlungsdienstleister auf Schätzungen zurückgreifen. Außerdem sollten Zahlungsdienstleister in ihrer Erstmeldung das Datum der nächsten Aktualisierung angeben, die so schnell wie möglich und in keinem Fall später als drei Geschäftstage erfolgen sollte.

Zwischenmeldung

2.11. Die Zahlungsdienstleister sollten jeweils Zwischenmeldungen übermitteln, wenn sie der Auffassung sind, dass sich der Status des Vorfalls wesentlich geändert hat. Allerdings sollten Zwischenmeldungen mindestens zu dem in der vorherigen Meldung (Erstmeldung oder vorherige Zwischenmeldung) angegebenen Datum für die nächste Aktualisierung übermittelt werden.

2.12. Die Zahlungsdienstleister sollten der zuständigen Behörde eine erste Zwischenmeldung mit einer ausführlicheren Beschreibung des Vorfalls und seiner Folgen (Abschnitt B des Formblatts) übermitteln. Darüber hinaus sollten Zahlungsdienstleister zusätzliche Zwischenmeldungen erstellen, um die bereits in den Abschnitten A und B des Formblatts angegebenen Informationen zu aktualisieren, zumindest dann, wenn sie erkennen, dass neue maßgebliche Informationen oder wesentliche Änderungen seit der vorherigen Meldung vorliegen (z. B. ob sich der Vorfall verschlechtert oder abgeschwächt hat, ob neue Ursachen ermittelt wurden oder ob Maßnahmen zur Behebung des Problems ergriffen wurden). In jedem Fall sollten die Zahlungsdienstleister eine Zwischenmeldung auf Ersuchen der zuständigen Behörde im Herkunftsmitgliedstaat erstellen.

2.13. Wie im Fall von Erstmeldungen sollten Zahlungsdienstleister auf Schätzungen zurückgreifen, wenn keine konkreten Daten verfügbar sind.

2.14. Außerdem sollten Zahlungsdienstleister in jeder Meldung das Datum der nächsten Aktualisierung angeben, die so schnell wie möglich und in keinem Fall später als drei Geschäftstage erfolgen sollte. Kann der Zahlungsdienstleister das für die nächste Aktualisierung veranschlagte Datum nicht einhalten, sollte er die zuständige Behörde kontaktieren, um die Gründe für die Verzögerung zu erläutern, eine neue plausible Frist für die Meldung (nicht später als drei Geschäftstage) vorzuschlagen und eine neue Zwischenmeldung zu übermitteln, in der nur die Information auf den neuesten Stand gebracht wird, die sich auf das veranschlagte Datum der nächsten Aktualisierung bezieht.

2.15. Wenn die regulären Tätigkeiten wiederhergestellt wurden und der Geschäftsbetrieb wieder seinen normalen Verlauf nimmt (Wiederherstellung des Regelbetriebs), sollten die Zahlungsdienstleister eine letzte 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 (Service Level Agreement, SLA) festgeschrieben wurden, und keine Notfallmaßnahmen mehr aktiv sind.

2.16. Sollte sich der Geschäftsbetrieb vor Ablauf von vier Stunden seit der Erkennung des Vorfalls wieder normalisiert haben, sollten die Zahlungsdienstleister die Erstmeldung sowie die letzte Zwischenmeldung möglichst zeitgleich innerhalb der Frist von vier Stunden übermitteln (indem sie die Abschnitte A und B im Formblatt ausfüllen).

Abschlussmeldung

2.17. Nachdem die Ursachenanalyse durchgeführt wurde (unabhängig davon, ob Maßnahmen zur Begrenzung der Auswirkungen bereits umgesetzt wurden oder die endgültige Ursache ermittelt wurde) und konkrete Zahlen zur Ersetzung der Schätzungen vorliegen, sollten die Zahlungsdienstleister eine Abschlussmeldung übermitteln.

2.18. Diese Abschlussmeldung sollte der zuständigen Behörde spätestens innerhalb von zwei Wochen übermittelt werden, nachdem der Regelbetrieb wiederhergestellt wurde. Benötigt der Zahlungsdienstleister eine Verlängerung dieser Frist (wenn z. B. noch keine konkreten Zahlen zum Vorfall vorliegen), 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. Angaben in Abschnitt C des Formblatts) innerhalb der Frist von vier Stunden nach der Erkennung des Vorfalls vorlegen können, sollten sie in ihre Erstmeldung möglichst die für die Erst-, die Zwischen- und die Abschlussmeldung maßgeblichen Informationen aufnehmen.

2.20. Die Zahlungsdienstleister sollten in ihren Abschlussmeldungen möglichst vollständige Angaben machen, d. h. i) konkrete Zahlen zum Vorfall statt Schätzungen (sowie jede weitere ggf. erforderliche Aktualisierung der Angaben in den Abschnitten A und B des Formblatts) und ii) Angaben in Abschnitt C des Formblatts, wozu die Hauptursache, sofern bereits bekannt, und eine Übersicht über die Maßnahmen zählen, die zur Behebung des Problems oder zur Verhinderung seines künftigen erneuten Auftretens 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 betreffenden Kriterien nicht mehr erfüllt, um als schwerwiegend klassifiziert zu werden, und nicht davon auszugehen ist, dass der Vorfall diese Kriterien vor seiner Lösung erfüllen wird. In diesem Fall sollte die Abschlussmeldung so schnell wie möglich nach Erkennung dieses Sachverhalts, jedoch in jedem Fall zu dem für die nächste Meldung veranschlagten Datum übermittelt werden. In dieser speziellen Situation sollten die Zahlungsdienstleister Abschnitt C des Formblatts nicht ausfüllen, sondern das Feld „Vorfall als nicht schwerwiegend neu klassifiziert“ ankreuzen und die Gründe für diese Herabstufung 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 Zuordnung 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 CEBS-Leitlinien zum Outsourcing in Bezug auf Kreditinstitute.

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 Betriebs- oder Sicherheitsvorfall betroffen sind), sollten die zuständige Behörde im Herkunftsmitgliedstaat davon in Kenntnis setzen, die Kontaktdaten unter „Betroffene Zahlungsdienstleister“ im Formblatt 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 Störung/Beeinträchtigung der von dem Dritten erbrachten Dienste verursacht wird.

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

d. 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.

e. Es wird sichergestellt, dass bei Feldern des Formblatts, in denen keine gemeinsame Antwort möglich ist (z. B. Abschnitte 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) in Feldern, in denen dies möglich ist, Bereiche angibt, die den für die verschiedenen Zahlungsdienstleister festgestellten oder geschätzten niedrigsten und höchsten Wert wiedergeben.

f. Die Zahlungsdienstleister sollten sicherstellen, dass der Dritte sie 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 hält; dies gilt jedoch nur insoweit, als keine Verletzung der Vertraulichkeit im Hinblick auf Informationen vorliegt, die sich auf andere Zahlungsdienstleister beziehen.

3.3. Die Zahlungsdienstleister sollten ihre Meldepflichten nicht vor Unterrichtung der zuständigen Behörde im Herkunftsmitgliedstaat delegieren. 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 im Einklang mit 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 ihre Meldepflichten

auch ohne externe Unterstützung erfüllen können. Des Weiteren sollten Zahlungsdienstleister sicherstellen, dass ein Vorfall nicht zweimal gemeldet wird, zum einen vom betreffenden Zahlungsdienstleister und ein weiteres Mal von dem Dritten.

Leitlinie 4: Betriebs- und Sicherheitsstrategie

4.1. Die Zahlungsdienstleister sollten sicherstellen, dass in ihrer Betriebs- und Sicherheitsstrategie alle Verantwortlichkeiten für die Meldung von Vorfällen gemäß der PSD2 sowie die umgesetzten Prozesse zur Einhaltung der in den vorliegenden Leitlinien beschriebenen Anforderungen klar definiert sind.

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 Expertenmeinung 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 oder könnte weitreichende Auswirkungen auf Zahlungsdienstnutzer haben.
d. Der Vorfall fand oder findet wahrscheinlich ein großes Interesse in den Medien.

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 nationalen Behörden (d. h. „anderen 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, in der der Informationsaustausch ersucht wird) sowie bei Eingang der Benachrichtigung, dass der Regelbetrieb wiederhergestellt ist(d. h. bei Eingang der letzten Zwischenmeldung).

6.2. Die zuständigen Behörden sollten anderen 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 mindestens die vom Zahlungsdienstleister in den folgenden Feldern des Formblatts (in der Erst- oder der Zwischenmeldung) angegebenen Informationen übermitteln:

- 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 vom Vorfall betroffen sein könnten;
- ggf. Beschreibung der Medienberichterstattung;
- Ursache des Vorfalls.

6.3. Vor dem Austausch von vorfallsbezogenen Informationen mit anderen maßgeblichen nationalen Behörden sollten die zuständigen Behörden bei Bedarf entsprechende 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 anderen maßgeblichen nationalen Behörden Name und Anschrift des Zahlungsdienstleisters mitteilen, der den Vorfall meldet, sofern die betreffenden nationalen Behörden gewährleisten können, dass diese Informationen vertraulich behandelt werden.

6.4. Die zuständigen Behörden sollten die Vertraulichkeit und die Integrität der gespeicherten und mit anderen maßgeblichen nationalen Behörden ausgetauschten Informationen jederzeit wahren und sich gegenüber den anderen 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 Kommunikationsverfahren

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) erhielten (d. h. Erst-, Zwischen- und Abschlussmeldungen).

Leitlinie 8: Kommunikation

8.1. Die zuständigen Behörden sollten die Vertraulichkeit und die Integrität der gespeicherten und mit der EBA und der EZB 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 1 – Formblätter für Meldungen von Zahlungsdienstleistern

CLASSIFICATION: RESTRICTED

Major Incident Report

☐ Initial report	within 4 hours after detection
☐ Intermediate report	maximum of 3 business days from previous report
☐ Last intermediate report	
☐ Final report	within 2 weeks after closing the incident
☐ Incident reclassified as non-major — Please explain:	

Report date	DD/MM/YYYY	Time	HH:MM
Incident identification number, if applicable (for interim and final reports)			

A - Initial report

A 1 - GENERAL DETAILS

Type of report					
Type of report	☐ Individual ☐ Consolidated				
Affected payment service provider (PSP)					
PSP name					
PSP unique identification number, if relevant					
PSP authorisation number					
Head of group, if applicable					
Home country					
Country/countries affected by the incident					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)					
Name of the reporting entity					
Unique identification number, if relevant					
Authorisation number, if applicable					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	

A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION

Date and time of detection of the incident	DD/MM/YYYY, HH:MM		
The incident was detected by (1)		If Other, please explain:	
Please provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member States(s), and if feasible within the applicable reporting deadlines, please provide a translation in English)			
What is the estimated time for the next update?	DD/MM/YYYY, HH:MM		

B - Intermediate report

B 1 - GENERAL DETAILS

Please provide a more DETAILED description of the incident. e.g. information on: - What is the specific issue? - How it happened - How did it develop - Was it related to a previous incident? - Consequences (in particular for payment service users) - Background of the incident detection - Areas affected - Actions taken so far - Service providers/ third party affected or involved - Crisis management started (internal and/or external (Central Bank Crisis management)) - PSP internal classification of the incident	
Date and time of beginning of the incident (if already identified)	DD/MM/YYYY, HH:MM
Incident status	☐ Diagnostics ☐ Recovery ☐ Repair ☐ Restoration
Date and time when the incident was restored or is expected to be restored	DD/MM/YYYY, HH:MM

B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT

Overall impact	☐ Integrity	☐ Confidentiality	☐ Continuity
	☐ Availability	☐ Authenticity	
Transactions affected [2]	Number of transactions affected	☐ Actual figure	☐ Estimation
	As a % of regular number of transactions	☐ Actual figure	☐ Estimation
	Value of transactions affected in EUR	☐ Actual figure	☐ Estimation
	Comments:		
Payment service users affected [3]	Number of payment service users affected	☐ Actual figure	☐ Estimation
	As a %-of total payment service users	☐ Actual figure	☐ Estimation
Service downtime[4]	Total service downtime DD:HH:MM	☐ Actual figure	☐ Estimation
Economic impact [5]	Direct costs in EUR	☐ Actual figure	☐ Estimation
	Indirect costs in EUR	☐ Actual figure	☐ Estimation
High level of internal escalation	☐ YES ☐ YES, AND CRISIS MODE (OR EQUIVALENT) IS LIKELY TO BE CALLED UPON ☐ NO Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe		
Other PSPs or relevant infrastructures potentially affected	☐ YES ☐ NO Describe how this incident could affect other PSPs and/or infrastructures		
Reputational impact	☐ YES ☐ NO Describe how the incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement, etc.)		

B 3 - INCIDENT DESCRIPTION

Type of Incident	☐ Operational	☐ Security	
Cause of incident	☐ Under investigation		
	☐ External attack ☐ Internal attack	→ Type of attack: ☐ Distributed/Denial of Service (D/DoS) ☐ Infection of internal systems ☐ Targeted intrusion ☐ Other If Other, specify	
	☐ External events ☐ Human error ☐ Process failure ☐ System failure ☐ Other	If Other, specify	
Was the incident affecting you directly, or indirectly through a service provider?	☐ Directly	☐ Indirectly	If indirectly, please provide the service provider's name

B 4 - INCIDENT IMPACT

Building(s) affected (Address), if applicable			
Commercial channels affected	☐ Branches ☐ E-banking	☐ Telephone banking ☐ Mobile banking ☐ ATMs	☐ Point of sale ☐ Other
	If Other, specify:		
Payment services affected	☐ Cash placement on a payment account ☐ Cash withdrawal from a payment account ☐ Operations required for operating a payment account ☐ Acquiring of payment instruments	☐ Credit transfers ☐ Direct debits ☐ Card payments ☐ Issuing of payment instruments	☐ Money remittance ☐ Payment initiation services ☐ Account information services ☐ Other
	If Other, specify:		
Functional areas affected	☐ Authentication/authorisation ☐ Communication	☐ Clearing ☐ Direct settlement	☐ Indirect settlement ☐ Other
	If Other, specify:		
Systems and components affected	☐ Application/software ☐ Database	☐ Hardware ☐ Network/infrastructure ☐ Other	
	If Other, specify:		
Staff affected	☐ YES ☐ NO Describe how the incident could affect the staff of the PSP/service provider (e.g. staff not being able to reach the office to support customers, etc.)		

B 5 - INCIDENT MITIGATION

Which actions/measures have been taken so far or are planned to recover from the incident?		
Has the Business Continuity Plan and/or Disaster Recovery Plan been activated?	☐ YES	☐ NO
If so, when?	DD/MM/YYYY, HH:MM	
If so, please describe		
Has the PSP cancelled or weakened some controls because of the incident?	☐ YES	☐ NO
If so, please explain		

C - Final report	
If no intermediate report has been sent, please also complete section B	
C 1 - GENERAL DETAILS	
Please update the information from the intermediate report (summary): - additional actions/measures taken to recover from the incident - final remediation actions taken - root cause analysis - lessons learnt - addittional actions - any other relevant information	
Date and time of closing the incident	DD/MM/YYYY, HH:MM
If the PSP had to cancel or weaken some controls because of the incident, are the original controls back in place?	☐ YES ☐ NO
If so, please explain	
C 2 - ROOT CAUSE ANALYSIS AND FOLLOW-UP	
What was the root cause (if already known)? (possible to attach a file with detailed information)	
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known	
C 3 - ADDITIONAL INFORMATION	
Has the incident been shared with other PSPs for information purposes?	☐ YES ☐ NO
If so, please provide details	
Has any legal action been taken against the PSP?	☐ YES ☐ NO
If so, please provide details	

Notes:

(1) Pull-down menu: payment service user; internal organisation; external organisation; none of the above

(2) Pull-down menu: > 10% of regular level of transactions and > EUR 100,000; > 25% of regular level of transactions or > EUR 5 milion; none of the above

(3) Pull-down menu: > 5,000 and > 10% payment service users; > 50,000 or > 25% payment service users; none of the above

(4) Pull-down menu: > 2 hours; < 2 hours

(5) Pull-down menu: > Max (0,1% Tier 1 capital, EUR 200,000) or > EUR 5 million; none of the above

CONSOLIDATED REPORT - LIST OF PSPs		
PSP Name	**PSP Unique Identification Number**	**PSP Authorisation number**

ANLEITUNGEN FÜR DAS AUSFÜLLEN DER FORMBLÄTTER

Zahlungsdienstleister sollten je nach Meldephase den entsprechenden Abschnitt des Formblatts ausfüllen: für die Erstmeldung Abschnitt A, für Zwischenmeldungen Abschnitt B und für die Abschlussmeldung Abschnitt C. Sofern nichts anderes angegeben ist, sind alle Felder Pflichtfelder.

Kopfdaten

Erstmeldung: Es handelt sich um die erste Meldung, die der Zahlungsdienstleister der zuständigen Behörde im Herkunftsmitgliedstaat übermittelt.

Zwischenmeldung: Dies ist eine Aktualisierung einer vorherigen Meldung (Erst- oder Zwischenmeldung) für denselben Vorfall.

Letzte Zwischenmeldung: Dadurch wird der zuständigen Behörde im Herkunftsmitgliedstaat mitgeteilt, dass der Regelbetrieb wiederhergestellt wurden und der Geschäftsbetrieb wieder seinen normalen Verlauf nimmt; somit werden keine Zwischenmeldungen mehr übermittelt.

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.

Vorfall als nicht schwerwiegend reklassifiziert: Der Vorfall erfüllt die entsprechenden Kriterien nicht mehr, um als schwerwiegend klassifiziert zu werden, und es ist nicht davon auszugehen, dass er diese Kriterien vor seiner Lösung erfüllen wird. Vom Zahlungsdienstleister sollten die Gründe für diese Herabstufung angegeben werden.

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

Ggf. Vorfallidentifikationsnummer (für Zwischen- und Abschlussmeldung): die von der zuständigen Behörde bei Eingang der Erstmeldung zugewiesene Referenznummer zur eindeutigen Identifizierung des Vorfalls, falls zutreffend (d. h., wenn eine solche Referenznummer von der zuständigen Behörde angegeben wird).

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, die die Möglichkeit der konsolidierten Meldung nutzen. Die Felder unter „Betroffener Zahlungsdienstleister“ sollten leer bleiben (mit Ausnahme des Feldes „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: bezieht sich auf den Zahlungsdienstleister, bei dem der Vorfall aufgetreten ist.

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

Ggf. eindeutige Identifikationsnummer des Zahlungsdienstleisters: die maßgebliche eindeutige Identifikationsnummer, anhand der der Zahlungsdienstleister im jeweiligen Mitgliedstaat identifiziert wird. Ist vom Zahlungsdienstleister anzugeben, falls keine Angabe im Feld „Zulassungsnummer des Zahlungsdienstleisters“ erfolgt.

Zulassungsnummer des Zahlungsdienstleisters: die Zulassungsnummer im Herkunftsmitgliedstaat.

Hauptunternehmen der Gruppe: Im Falle einer Gruppe von Unternehmen gemäß Artikel 4 Absatz 40 der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG geben Sie bitte den Namen des Hauptunternehmens an.

Herkunftsstaat: Mitgliedstaat, in dem sich der Sitz des Zahlungsdienstleisters befindet, oder, wenn der Zahlungsdienstleister nach dem für ihn geltenden nationalen Recht keinen Sitz hat, der Mitgliedstaat, in dem sich seine Hauptverwaltung befindet.

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). Hierbei 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 die Meldung im Namen des betroffenen Zahlungsdienstleisters vornimmt, den Vor- und Nachnamen der Person, die in der Abteilung für Vorfalls-/Risikomanagement oder in einem ähnlichen Bereich beim betroffenen Zahlungsdienstleister beschäftigt ist.

E-Mail: 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.

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

Alternativer Ansprechpartner: Vor- und Nachname einer alternativen Person, an die sich die zuständige Behörde bei Anfragen bezüglich des Vorfalls wenden kann, falls der Hauptansprechpartner nicht verfügbar ist. Falls ein Dritter die Meldung im Namen des betroffenen Zahlungsdienstleisters vornimmt, den Vor- und Nachnamen einer alternativen Person in der Abteilung für Vorfalls-/Risikomanagement oder einem vergleichbaren 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 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 Firmenregister.

Ggf. eindeutige Identifikationsnummer: die maßgebliche eindeutige Identifikationsnummer in dem Land, in dem der Dritte seinen Sitz hat, zur Identifizierung der den Vorfall meldenden Stelle. Ist von der meldenden Stelle anzugeben, falls keine Angabe im Feld „Zulassungsnummer“ erfolgt.

Ggf. Zulassungsnummer: ggf. die Zulassungsnummer des Dritten in dem Land, in dem dieser seinen Sitz hat.

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

E-Mail: 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.
Telefon: Telefonnummer, die ggf. zur weiteren Klärung angerufen werden kann. Hierbei kann es sich um eine persönliche oder 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 eine Firmentelefonnummer handeln.

A 2 – Erkennung des Vorfalls und anfängliche Klassifizierung

Datum und Uhrzeit der Erkennung des Vorfalls: Zeitpunkt (Datum und Uhrzeit), zu dem der Vorfall erstmals erkannt wurde.
Vorfall wurde erkannt von: Geben Sie an, ob der Vorfall von einem Zahlungsdienstnutzer oder einer anderen Stelle beim Zahlungsdienstleister (z. B. Innenrevision) oder von einer externen Stelle (z. B. externer Dienstleister) erkannt wurde. Trifft keine der Optionen zu, geben Sie bitte eine Erläuterung im entsprechenden Feld an.
Kurze allgemeine Beschreibung des Vorfalls: Erläutern Sie bitte kurz die maßgeblichsten Probleme des Vorfalls, einschließlich möglicher Ursachen, unmittelbarer Auswirkungen usw.
Voraussichtlicher Zeitpunkt der nächsten Aktualisierung: Geben Sie das ungefähre Datum und die ungefähre Uhrzeit für die Übermittlung der nächsten Aktualisierung (Zwischen- oder Abschlussmeldung) an.

B – Zwischenmeldung

B 1 – Allgemeine Angaben

Ausführlichere Beschreibung des Vorfalls: Bitte beschreiben Sie die wichtigsten Merkmale des Vorfalls, wobei mindestens auf die im Formblatt aufgeführten Punkte eingegangen werden sollte (mit welchem konkreten Problem ist der Zahlungsdienstleister konfrontiert; wie begann der Vorfall und wie hat er sich entwickelt; möglicher Zusammenhang mit einem früheren Vorfall; Folgen, insbesondere für Zahlungsdienstnutzer, usw.).
Datum und Uhrzeit des Beginns des Vorfalls: Zeitpunkt (Datum und Uhrzeit), zu dem der Vorfall begann, sofern bekannt.
Status des Vorfalls:

Diagnose: Die Merkmale des Vorfalls wurden kürzlich ermittelt.
Reparatur: Die beeinträchtigten Elemente werden neu konfiguriert.
Fehlerbehebung: Die fehlerhaften Elemente werden in ihren letzten wiederherstellbaren Zustand zurückgesetzt.
Wiederherstellung: Der zahlungsbezogene Dienst wird wieder bereitgestellt.

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 Geschäftsbetrieb wieder seinen normalen Verlauf genommen hatte oder voraussichtlich nehmen wird.

B 2 – Klassifizierung des Vorfalls/Informationen zum Vorfall

Gesamtauswirkung: Geben Sie bitte an, welche Schutzziele von dem Vorfall betroffen waren. Sie können mehrere Kästchen ankreuzen.

> **Integrität:** die Eigenschaft, die Korrektheit und Vollständigkeit von Vermögenswerten (einschließlich Daten) zu schützen.
>
> **Verfügbarkeit:** die Eigenschaft, dass zahlungsbezogene Dienste 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.
>
> **Kontinuität:** die Eigenschaft, dass die für die Erbringung der zahlungsbezogenen Dienste erforderlichen Prozesse, Aufgaben und Vermögenswerte einer Organisation in vollem Umfang zugänglich und auf einem annehmbaren vordefinierten Niveau funktionsfähig sind.

Betroffene Zahlungsvorgänge: Die Zahlungsdienstleister sollten angeben, welche Schwellenwerte vom Vorfall erreicht oder aller Wahrscheinlichkeit nach 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. Stellen, die Meldungen im Namen mehrerer Zahlungsdienstleister übermitteln (konsolidierte Meldungen), können stattdessen Wertebereiche angeben, die den niedrigsten und den höchsten Wert wiedergeben, der innerhalb der Gruppe der in die Meldung eingeschlossenen Zahlungsdienstleister festgestellt oder geschätzt wurde; die Werte sind durch einen Bindestrich zu trennen. 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 höchstwahrscheinlich 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 der Saisonalität), sollten sie stattdessen eine andere repräsentativere Messzahl verwenden und der zuständigen Behörde im Feld „Anmerkungen“ das diesem Ansatz zugrunde liegende Prinzip mitteilen.

Betroffene Zahlungsdienstnutzer: Die Zahlungsdienstleister sollten angeben, welche Schwellenwerte vom Vorfall erreicht oder aller Wahrscheinlichkeit nach erreicht werden (sofern welche gelten), 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. Stellen, die Meldungen im Namen mehrerer Zahlungsdienstleister übermitteln (konsolidierte Meldungen), können stattdessen Wertebereiche angeben, die den niedrigsten und den höchsten Wert

wiedergeben, der innerhalb der Gruppe der in die Meldung eingeschlossenen Zahlungsdienstleister festgestellt oder geschätzt wurde; die Werte sind durch einen Bindestrich zu trennen. Die Zahlungsdienstleister sollten als „betroffene Zahlungsdienstnutzer“ alle Kunden (inländische oder ausländische, Verbraucher oder Unternehmen) betrachten, 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 höchstwahrscheinlich 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.

Dienstausfallzeit: Die Zahlungsdienstleister sollten angeben, ob die Schwellenwerte durch den Vorfall erreicht oder aller Wahrscheinlichkeit nach 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 kann. Stellen, die Meldungen im Namen mehrerer Zahlungsdienstleister übermitteln (konsolidierte Meldungen), können stattdessen einen Wertebereich angeben, der den niedrigsten und den höchsten Wert wiedergibt, der innerhalb der Gruppe der in die Meldung eingeschlossenen Zahlungsdienstleister festgestellt oder geschätzt wurde; die Werte sind durch einen Bindestrich zu trennen. Die Zahlungsdienstleister sollten den Zeitraum berücksichtigen, in dem eine Aufgabe, ein Prozess oder ein Kanal in Verbindung mit der Bereitstellung von Zahlungsdiensten nicht oder höchstwahrscheinlich 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 gezählt werden, und die Zahlungsdienstleister sollten sowohl die Zeitspanne berücksichtigen, innerhalb der 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 zählen, zu dem der Ausfall erkannt wurde.

Wirtschaftliche Auswirkungen: Die Zahlungsdienstleister sollten angeben, ob die Schwellenwerte vom Vorfall erreicht oder aller Wahrscheinlichkeit nach 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. Stellen, die Meldungen im Namen mehrerer Zahlungsdienstleister übermitteln (konsolidierte Meldungen), können stattdessen einen Wertebereich angeben, der den niedrigsten und den höchsten Wert wiedergibt, der innerhalb der Gruppe der in die Meldung eingeschlossenen Zahlungsdienstleister festgestellt oder geschätzt wurde; die Werte sind durch einen Bindestrich zu trennen. Die Zahlungsdienstleister sollten 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 in Betracht gezogen werden.

> **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. Kosten durch Kundenreklamationen/Entschädigung von Kunden, entgangene Einnahmen infolge verpasster Geschäftschancen, mögliche Prozesskosten).

Hohe interne Eskalationsstufe: Die Zahlungsdienstleister sollten erwägen, ob infolge der Auswirkung des Vorfalls auf zahlungsbezogene Dienste der Chief Information Officer (oder eine vergleichbare Position) außerhalb des regelmäßigen Meldeverfahrens sowie fortlaufend während der Dauer des Vorfalls über den Vorfall informiert wurde oder aller Wahrscheinlichkeit nach informiert wird. Im Falle der delegierten Meldung vollzieht sich die Eskalation innerhalb des Dritten. Des Weiteren sollten die Zahlungsdienstleister in Erwägung ziehen, ob infolge der Auswirkung des Vorfalls auf zahlungsbezogene Dienste ein Krisenmodus ausgelöst wurde oder voraussichtlich ausgelöst wird.

Andere Zahlungsdienstleister/wesentliche Infrastrukturen, die betroffen sein könnten: Die Zahlungsdienstleister sollten die Auswirkung des Vorfalls auf den Finanzmarkt bewerten, wobei darunter die Finanzmarktinfrastrukturen und/oder die Zahlungskartensysteme 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. Als einen nützlichen Indikator sollten die Zahlungsdienstleister dabei insbesondere die Wahrscheinlichkeit einschätzen, ob und wie der Vorfall möglicherweise auch die Gesellschaft schädigt, um das dem Vorfall innewohnende Potenzial zur Schädigung ihrer Reputation zu bestimmen. Die Zahlungsdienstleister sollten berücksichtigen, ob i) der Vorfall einen sichtbaren Prozess betraf und daher in den Medien vermutlich Beachtung findet oder bereits gefunden hat (wobei nicht nur herkömmliche Medien wie Zeitungen, sondern auch Blogs, soziale Netze usw. einzubeziehen sind), ob ii) aufsichtsrechtliche Pflichten missachtet wurden oder vermutlich missachtet werden, ob iii) Sanktionen gebrochen wurden oder vermutlich gebrochen werden oder ob iv) ein Vorfall der gleichen Art bereits zuvor aufgetreten ist.

B 3 – Beschreibung des Vorfalls

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

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

Sicherheit: unbefugter Zugang, unbefugte Nutzung, Offenlegung, Unterbrechung, Änderung oder Zerstörung der Vermögenswerte (Assets) des Zahlungsdienstleisters, was sich auf die Integrität, die Verfügbarkeit, die Vertraulichkeit, die Authentizität und/oder die Kontinuität zahlungsbezogener Dienste auswirkt. Dies kann u. a. durch Cyberangriffe, durch die unzureichende Gestaltung oder Umsetzung von Sicherheitsstrategien oder eine unzureichende physische Sicherheit beim Zahlungsdienstleister verursacht sein.

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: Die Ursache konnte noch nicht festgestellt werden.

Externer Angriff: Die Angriffsquelle liegt außerhalb des Zahlungsdienstleisters und richtet sich absichtlich gegen diesen (z. B. Angriffe durch Schadsoftware).

Interner Angriff: Die Angriffsquelle liegt innerhalb des Zahlungsdienstleisters und richtet sich absichtlich gegen diesen (z. B. interner Betrug).

Art des Angriffs:

Distributed Denial of Service (DDoS): Versuch, die Verfügbarkeit eines Online-Dienstes zu verhindern, indem er mit riesigem Datenverkehr aus mehreren Quellen überschüttet wird.

Infizierung interner Systeme: schädliche Aktivität, die Computersysteme angreift mit dem Versuch, Festplattenspeicher oder Prozessorzeit/-kapazität zu stehlen, auf private Daten zuzugreifen, Daten zu beschädigen, Kontakte mit unerwünschten E-Mails zu überhäufen usw.

Gezieltes Eindringen: unbefugtes Ausspionieren, Ausspähen und Stehlen von Informationen über den Cyberspace als Angriffsvektor.

Sonstiges: jede andere Art des Angriffs, den der Zahlungsdienstleister erleiden kann, entweder direkt oder indirekt durch einen Dienstleister. Dieses Kästchen sollte insbesondere dann angekreuzt werden, wenn ein Angriff auf den Autorisierungs- und Authentifizierungsprozess erfolgte. Im Freitextfeld sollten Einzelheiten angegeben werden.

Externe Ereignisse: Die Ursache steht mit Ereignissen in Zusammenhang, die in der Regel außerhalb der Kontrolle des Unternehmens liegen (z. B. Naturkatastrophen, rechtliche Sachverhalte, geschäftliche Sachverhalte und Abhängigkeit von Diensten).

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).

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

Systemfehler: Die Ursache des Vorfalls steht in Verbindung damit, dass die Gestaltung, Ausführung, Komponenten, Spezifikationen, Integration oder Komplexität der Systeme, die die Zahlungstätigkeit unterstützen, unzureichend sind.

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 vom Vorfall betroffen? Ein Vorfall kann direkt auf einen Zahlungsdienstleister abzielen oder ihn indirekt durch einen Dritten betreffen. Im Falle eines indirekten Vorfalls geben Sie bitte den Namen des oder der Dienstleister/s an.

B 4 – Auswirkungen des Vorfalls

Ggf. betroffene/s Gebäude (Anschrift): Ist ein physisches Gebäude betroffen, geben Sie bitte die entsprechende Anschrift an.

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.

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 zur 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 bewirkenden 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: Zahlungsdienste, die auf Antrag des Zahlungsdienstnutzers einen Zahlungsauftrag in Bezug auf ein bei einem anderen Zahlungsdienstleister geführtes Zahlungskonto auslösen.

Kontoinformationsdienste: Online-Zahlungsdienste 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.

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

Betroffene Funktionsbereiche: Geben Sie den Schritt oder die Schritte des Zahlungsprozesses an, die vom Vorfall betroffen waren. Sie können mehrere Kästchen ankreuzen.

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) zur Übertragung von Geldbeträgen oder Wertpapieren.

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, falls 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.

Betroffene Systeme und Komponenten: Geben Sie an, welcher Teil oder welche Teile von der technischen Infrastruktur des Zahlungsdienstleisters vom Vorfall betroffen waren. Sie können mehrere Kästchen ankreuzen.

Anwendung/Software: Programme, Betriebssysteme usw., die die Bereitstellung von Zahlungsdiensten durch den Zahlungsdienstleister unterstützen.
Datenbank: Datenstruktur zur Speicherung von personenbezogenen Daten und Zahlungsdaten, die für die Ausführung von Zahlungsvorgängen benötigt werden.
Hardware: physische technische Ausrüstung, die die Prozesse ausführt und/oder die Daten speichert, die von Zahlungsdienstleistern für die Erfüllung ihrer zahlungsbezogenen Aktivitäten erforderlich sind.
Netzwerk/Infrastruktur: öffentliche oder private Telekommunikationsnetze, die den Austausch von Daten und Informationen während des Zahlungsprozesses ermöglichen (z. B. das Internet).
Sonstiges: Das betroffene System oder die betroffene Komponente ist oben nicht aufgeführt. Im Freitextfeld sollten weitere Einzelheiten angegeben werden.

Personal war betroffen: Geben Sie an, ob sich der Vorfall auf das Personal des Zahlungsdienstleisters auswirkte, und wenn ja, geben Sie bitte Einzelheiten im Freitextfeld an.

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.
Wurden 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 maßgeblichsten Einzelheiten der jeweiligen Vorgehensweise an (z. B. wann die Aktivierung des Plans erfolgte und welche Maßnahmen im jeweiligen Plan festgeschrieben sind).
Wurden vom Zahlungsdienstleister einige Sicherheitsmaßnahmen oder Überwachungsprozesse infolge des Vorfalls außer Kraft gesetzt oder abgeschwächt? Geben Sie bitte an, ob der Zahlungsdienstleister in Reaktion auf den Vorfall einige Kontrollen außer Kraft setzen musste (z. B. die Einstellung des Vier-Augen-Prinzips), und falls ja, geben Sie die entsprechenden Gründe zur Rechtfertigung der Abschwächung oder Außerkraftsetzung von Kontrollen an.

C – Abschlussmeldung

C 1 – Allgemeine Angaben

Aktualisierung der Informationen aus der Zwischenmeldung (Zusammenfassung): Machen Sie bitte weitere Angaben zu den ergriffenen Maßnahmen, um den Vorfall zu beheben und sein erneutes Auftreten zu verhindern, zur Ursachenanalyse, zu den gewonnenen Erkenntnissen usw.

Datum und Uhrzeit des Abschlusses des Vorfalls: Geben Sie den Zeitpunkt (Datum und Uhrzeit) an, zu dem der Vorfall als abgeschlossen betrachtet wurde.

Wurden die ursprünglichen Sicherheitsmaßnahmen oder Überwachungsprozesse wieder eingerichtet? Falls der Zahlungsdienstleister diese infolge des Vorfalls außer Kraft setzen oder abschwächen musste, geben Sie an, ob diese wieder eingerichtet wurden, und geben Sie weitere Informationen im Freitextfeld an.

C 2 – Ursachenanalyse und Folgemaßnahmen

Welches war die Hauptursache, sofern bereits bekannt? Geben Sie bitte die Hauptursache für den Vorfall an oder, falls diese noch nicht bekannt ist, geben Sie die vorläufigen Schlussfolgerungen aus der Ursachenanalyse an. Die Zahlungsdienstleister können eine Datei mit detaillierten Informationen beifügen, wenn dies als notwendig erachtet wird.

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 anderen Zahlungsdienstleistern 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 eine Klage vor Gericht vor, oder hat er seine Zulassung verloren).