EBA/GL/2017/10

18/12/2017

Насоки

относно докладването на значими инциденти съгласно Директива (ЕС) 2015/2366 (ДПУ 2)

1. Спазване на насоките задълженията за докладване

Статут на насоките

1. Този документ съдържа насоки, издадени съгласно член 16 от Регламент (ЕС) № 1093/2010 [1] . Съгласно член 16, параграф 3 от Регламент (ЕС) № 1093/2010, компетентните органи и финансовите институции полагат всички усилия за спазване на насоките.

2. В насоките е представено становището на ЕБО за подходящите надзорни практики в Европейската система за финансов надзор или за това как правото на Съюза следва да се прилага в дадена област. Компетентните органи, както са дефинирани в член 4, параграф 2 от Регламент (ЕС) № 1093/2010, за които се отнасят тези насоки, трябва да ги спазват, като ги включат в практиките си по подходящ начин (напр. като изменят своята правна рамка или надзорни процеси), включително когато насоките са насочени основно към институциите.

Изисквания за отчетност

3. Съгласно член 16, параграф 3 от Регламент (ЕС) № 1093/2010, най-късно до 19.02.2018 компетентните органи са длъжни да уведомят ЕБО дали спазват или възнамеряват да спазват тези насоки, в противен случай - за причините за неспазване. При липса на уведомление в този срок ЕБО счита, че компетентните органи не спазват изискването за отчетност. Уведомленията трябва да се изпратят чрез подаване на формата, намираща се на уебсайта на ЕБО, на адрес compliance@eba.europa.eu, като се посочи референтен номер ‘EBA/GL/2017/10. Уведомленията следва да се подават от лица, оправомощени да докладват за наличието на съответствие от името на техните компетентни органи. Всяка промяна в статута на спазването трябва също да се отчита пред ЕБО.

4. Уведомленията се публикуват на уебсайта на ЕБО в съответствие с член 16, параграф 3.

[1] Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета от 24 ноември 2010 година за създаване на Европейски надзорен орган (Европейски банков орган), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/78/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр.12).

2. Предмет, обхват и определения

Предмет

5. Настоящите насоки произтичат от мандата, даден на ЕБО съгласно член 96, параграф 3 от Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета от 25 ноември 2015 г. за платежните услуги във вътрешния пазар, за изменение на директиви 2002/65/ЕО, 2009/110/ЕО и 2013/36/ЕО и Регламент (ЕС) № 1093/2010 и за отмяна на Директива 2007/64/ЕО (ДПУ 2).

6. По-специално настоящите насоки определят критериите за класифициране на значими операционни или свързани със сигурността инциденти от страна на доставчиците на платежни услуги, както и формата и процедурите, които те трябва да следват, когато съобщават за подобни инциденти на компетентния орган в държавата членка по произход, както е предвидено в член 96, параграф 1 от горепосочената директива.

7. В допълнение, настоящите насоки разглеждат начина, по който компетентните органи следва да оценяват значението на инцидента и данните в докладите за инцидента, които те трябва да предоставят на други национални органи съгласно член 96, параграф 2 от същата директива.

8. Насоките разглеждат също предоставянето на информация на ЕБО и ЕЦБ за докладваните инциденти, което има за цел да насърчи използването на общ и съгласуван подход.

Обхват на прилагане

9. Настоящите насоки се прилагат по отношение на класификацията и докладването на значими операционни или свързани със сигурността инциденти в съответствие с член 96 от Директива (ЕС) 2015/2366.

10. Те са приложими за всички инциденти, включени в определението за „значим операционен или свързан със сигурността инцидент“, което обхваща както външните, така и вътрешните събития, които биха могли да бъдат злонамерени или случайни.

11. Настоящите насоки се прилагат и в случаите, когато значимият операционен или свързан със сигурността инцидент е с произход извън Съюза (напр. инцидентът е възникнал в дружество майка или дъщерно дружество, установени извън Съюза) и засяга платежните услуги, които се предоставят от доставчик на платежни услуги в Съюза пряко (услугата, свързана с плащане, се извършва от засегнатото дружество извън Съюза) или непряко (способността на доставчика на платежни услуги да продължи да извършва платежната дейност е застрашена по друг начин в резултат на инцидента).

Адресати

12. Първата група насоки (раздел 4) е предназначена за доставчици на платежни услуги съгласно определението в член 4, параграф 11 от Директива (ЕС) 2015/2366 и както е посочено в член 4, параграф 1 от Регламент (ЕС) № 1093/2010.

13. Втората и третата група насоки (раздели 5 и 6) са предназначени за компетентните органи, както са определени в член 4, параграф 2, буква и) от Регламент (ЕС) № 1093/2010.

Определения

14. Освен ако не е посочено друго, термините, използвани и определени в Директива (ЕС) 2015/2366, имат същото значение в насоките. Освен това за целите на настоящите насоки се прилагат следните определения:

Операционен или свързан със сигурността инцидент	Единично събитие или поредица от свързани събития, които не са планирани от доставчика на платежни услуги и които имат или вероятно ще окажат неблагоприятно въздействие върху целостта, достъпността, поверителността, автентичността и/или непрекъснатостта на услугите, свързани с плащанията.
Цялост	Характеристиката, че активите (вкл. данните) са запазили точността и целостта си.
Достъпност	Характеристиката на услугите, свързани с плащания, която ги прави достъпни и използваеми от ползвателите на платежни услуги.
Поверителност	Характеристиката, че информацията не е достъпна или оповестена на неоправомощени лица, дружества или процеси.
Автентичност	Характеристиката на даден източник да е това, което твърди, че е.
Непрекъснатост	Характеристиката на процесите, задачите и активите на дадена организация, които са необходими, за да е възможно при предоставянето на услуги, свързани с плащания, те да бъдат напълно достъпни и да функционират на приемливи, предварително зададени нива.
Услуги, свързани с плащания	Всяка стопанска дейност по смисъла на член 4, параграф 3 от ДПУ 2 и всички необходими технически помощни задачи за правилното предоставяне на платежните услуги.

3. Въвеждане

Дата на прилагане

15. Настоящите насоки се прилагат от 13 януари 2018 г.

4. Насоки, предназначени за доставчиците на платежни услуги, относно съобщаването на значими операционни или свързани със сигурността инциденти на компетентния орган в тяхната държава членка по произход

Насока 1: Класифициране като значим инцидент

1.1. Доставчиците на платежни услуги следва да класифицират като значими операционните или свързаните със сигурността инциденти, които изпълняват

a. един или повече критерии с „по-висока степен на въздействие“, или

б. три или повече критерии с „по-ниска степен на въздействие“,

както е посочено в насока 1.4, и след извършване на оценката, описана в настоящите насоки.

1.2. Доставчиците на платежни услуги следва да оценят даден операционен или свързан със сигурността инцидент по следните критерии и свързаните с тях показатели:

i. Засегнати операции

Доставчиците на платежни услуги следва да определят общата стойност на засегнатите операции и броя на изложените на риск плащания като процент от обичайното ниво на платежните операции, извършвани със засегнатите платежни услуги.

ii. Засегнати ползватели на платежни услуги

Доставчиците на платежни услуги следва да определят броя на засегнатите ползватели на платежни услуги, както като абсолютна стойност, така и като процент от общия брой на ползвателите на платежни услуги.

iii. Прекъсване на услугата

Доставчиците на платежни услуги следва да определят периода от време, през който услугата вероятно няма да бъде достъпна за ползвателя на платежни услуги или през който платежното нареждане, по смисъла на член 4, параграф 13 от ДПУ 2, не може да бъде изпълнено от доставчика на платежни услуги.

iv. Икономическо въздействие

Доставчиците на платежни услуги следва да определят паричните разходи, свързани с инцидента комплексно, като вземат предвид както абсолютната стойност, така и (ако е приложимо) относителното значение на тези разходи във връзка с размера на доставчика на платежни услуги (т.е. капитала от първи ред на доставчика на платежни услуги).

v. Високо ниво на вътрешно ескалиране

Доставчиците на платежни услуги следва да определят дали инцидентът е докладван или е вероятно да бъде докладван на ръководните лица.

vi. Други ДПУ или свързани инфраструктури, които са потенциално засегнати

Доставчиците на платежни услуги следва да определят последиците, които инцидентът вероятно ще има върху системите, т.е. потенциалът му да се разпростре отвъд първоначално засегнатия доставчик на платежни услуги към други доставчици на платежни услуги, инфраструктури на финансовите пазари и/или схеми за картови плащания.

vii. Влияние върху репутацията

Доставчиците на платежни услуги следва да определят как инцидентът може да подкопае доверието на потребителите в доставчика на платежната услуга и в по-общ план в засегнатата услуга или пазара като цяло.

1.3. Доставчиците на платежни услуги следва да изчислят стойността на показателите съгласно следната методология:

i. Засегнати операции

Като общо правило, доставчиците на платежни услуги следва да разглеждат като „засегнати операции“ всички вътрешни и трансгранични операции, които са или вероятно ще бъдат пряко или косвено засегнати от инцидента, по-специално операциите, които не са могли да бъдат започнати или обработени; операциите, при които съдържанието на платежното съобщение е променено; и операциите, които са наредени неправомерно (без значение дали средствата са възстановени).

Освен това доставчиците на платежни услуги следва да разглеждат обичайното ниво на платежните операции като дневната средно-годишна стойност на вътрешните и трансграничните платежни операции, извършвани със същите платежни услуги, които са били засегнати от инцидента, приемайки предходната година за референтен период за изчисленията. Ако доставчиците на платежни услуги не считат тази стойност за представителна (напр. поради сезонност), те следва да използват друг, по-представителен измерител и да съобщят на компетентния орган основния мотив за избора на този подход в съответното поле на формуляра (вж. приложение 1).

ii. Засегнати ползватели на платежни услуги

Доставчиците на платежни услуги следва да разглеждат като „засегнати ползватели на платежни услуги“ всички клиенти (независимо дали са местни или от чужбина, потребители или предприятия), които имат договор със засегнатия доставчик на платежни услуги, даващ им достъп до засегнатата платежна услуга, и които са засегнати или вероятно ще понесат последствията от инцидента. Доставчиците на платежни услуги следва да използват прогнозни цифри, базирани на минала дейност, за да определят броя на ползвателите на платежни услуги, които е вероятно да са използвали платежната услуга през жизнения цикъл на инцидента.

В случай на групи всеки доставчик на платежни услуги следва да вземе предвид само собствените си ползватели на платежни услуги. В случай на доставчик на платежни услуги, предоставящ операционни услуги на трети лица, този доставчик на платежни услуги следва да вземе предвид само собствените си ползватели на платежни услуги (ако има такива), а доставчиците на платежни услуги, които получават тези операционни услуги, следва да направят оценка на инцидента във връзка с собствените им ползватели на платежни услуги.

Освен това доставчиците на платежни услуги следва да приемат за общ брой на ползвателите на платежни услуги общия брой на вътрешните и трансграничните ползватели на платежни услуги, които са договорно задължени към тях по време на инцидента (или като алтернатива последните налични данни) и имат достъп до засегнатата платежна услуга, независимо от техния размер или дали са считани за активни или пасивни ползватели на платежни услуги.

iii. Прекъсване на услугата

Доставчиците на платежни услуги следва да вземат предвид периода от време, през който всяка задача, процес или канал, свързани с предоставянето на платежни услуги, са или вероятно ще бъдат неоперативни и следователно възпрепятстват (i) започването и/или изпълнението на платежна услуга и/или (ii) достъпа до платежна сметка. Доставчиците на платежни услуги следва да отчитат прекъсването на услугата от момента, в който започне прекъсването, и да вземат предвид както времевите интервали, през които осъществяват дейност и които са необходими за извършването на платежни услуги, така и неработните часове и периодите за поддръжка, когато това е уместно и приложимо. Ако доставчиците на платежни услуги не са в състояние да преценят кога е започнало прекъсването на услугата, по изключение те следва да отчитат прекъсването на услугата от момента на откриването му.

iv. Икономическо въздействие

Доставчиците на платежни услуги следва да вземат предвид както разходите, които могат да бъдат пряко свързани с инцидента, така и разходите, които са непряко свързани с инцидента. Наред с другото, доставчиците на платежни услуги следва да вземат предвид иззетите средства или активи, разходите за подмяна на хардуер или софтуер, другите разходи за съдебно-техническа експертиза или разходите за отстраняване, таксите, дължащи се на неизпълнение на договорни задължения, санкциите, външните задължения и загубата на приходи. По отношение на непреките

разходи доставчиците на платежни услуги следва да вземат под внимание единствено разходите, които вече са известни или има голяма вероятност да бъдат реализирани.

v. *Високо ниво на вътрешно ескалиране*

Доставчиците на платежни услуги следва да преценят дали, в резултат на въздействието от инцидента върху услугите, свързани с плащания, главното длъжностно лице, отговарящо за информацията (или сходна длъжност), е уведомено или вероятно ще бъде уведомено за инцидента, извън процедурата за периодично и непрекъснато уведомяване през целия жизнен цикъл на инцидента. Освен това доставчиците на платежни услуги следва да преценят дали, в резултат на въздействието на инцидента върху услугите, свързани с плащания, е задействан или е вероятно да бъде задействан кризисен режим.

vi. *Други ДПУ или свързани инфраструктури, които са потенциално засегнати*

Доставчиците на платежни услуги следва да направят оценка на въздействието на инцидента върху финансовия пазар, който представлява инфраструктурите на финансовите пазари и/или схемите за картови плащания, които подпомагат тях и другите доставчици на платежни услуги. По-конкретно доставчиците на платежни услуги следва да оценят дали инцидентът е възникнал или има вероятност да възникне при други доставчици на платежни услуги, независимо от това дали е засегнал или вероятно ще засегне гладкото функциониране на инфраструктурите на финансовите пазари и дали е изложил на риск, или има вероятност да застраши доброто функциониране на финансовата система като цяло. Доставчиците на платежни услуги следва да вземат предвид различните измерения, например дали засегнатият компонент/софтуер е защитен или общодостъпен, дали изложената на риск мрежа е вътрешна или външна и дали доставчикът на платежни услуги е прекратил или има вероятност да спре да изпълнява своите задължения в областта на инфраструктурите на финансовите пазари, на които е член.

vii. *Влияние върху репутацията*

Доставчиците на платежни услуги следва да разгледат степента на прозрачност, която, доколкото им е известно, инцидентът има или вероятно ще има на пазара. По-конкретно доставчиците на платежни услуги следва да разгледат вероятността инцидентът да причини вреди на обществото, като добър показател за потенциала му да засегне репутацията им. Доставчиците на платежни услуги следва да отчетат дали (i) инцидентът е засегнал прозрачен процес и следователно е вероятно да бъде отразен или вече е отразен в медиите (като се имат предвид не само традиционните медии, напр. вестници, но също и блогове, социални мрежи и др.), (ii) регулаторни задължения, които са или има вероятност да са неизпълнени, (iii) санкции, които са или е вероятно да бъдат нарушени, или (iv) същият вид инцидент е възниквал и преди.

1.4. Доставчиците на платежни услуги следва да оценят даден инцидент, като определят за всеки отделен критерий дали съответните прагове в таблица 1 са достигнати или вероятно ще бъдат достигнати, преди инцидентът да бъде разрешен.

Таблица 1: Прагове

Критерии	По-ниска степен на въздействие	По-висока степен на въздействие
Засегнати операции	> 10 % от обичайните операции на доставчика на платежни услуги (от гледна точка на броя операции) **и** > 100 000 EUR	> 25 % от обичайните операции на доставчика на платежни услуги (от гледна точка на броя операции) **или** > 5 млн. евро
Засегнати ползватели на платежни услуги	> 5 000 **и** > 10 % от ползвателите на платежни услуги на доставчика на платежни услуги	> 50 000 **или** > 25 % от ползвателите на платежни услуги на доставчика на платежни услуги
Прекъсване на услугата	> 2 часа	Неприложимо
Икономическо въздействие	Неприложимо	> макс. (0,1 % за капитал от ред 1, * 200 000 EUR) **или** > 5 млн. евро
Високо ниво на вътрешно ескалиране	Да	Да. Вероятно е да бъде поискан кризисен режим (или еквивалентен)
Други ДПУ или свързани инфраструктури, които са потенциално засегнати	Да	Неприложимо
Влияние върху репутацията	Да	Неприложимо

* Капитал от първи ред съгласно определението в член 25 от Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета от 26 юни 2013 г. относно пруденциалните изисквания за кредитните институции и инвестиционните посредници и за изменение на Регламент (ЕС) № 648/2012.

1.5. Доставчиците на платежни услуги следва да прибягват до прогнози, ако не разполагат с действителни данни, които да подкрепят решенията им относно това дали даден праг е достигнат или вероятно ще бъде достигнат, преди инцидентът да бъде разрешен (напр. това може да се случи по време на етапа на първоначалното разследване).

1.6. Доставчиците на платежни услуги следва да извършват тази оценка непрекъснато през целия жизнен цикъл на инцидента, за да идентифицират всяка възможна промяна в статуса — в посока нагоре (от незначими към значими) и в посока надолу (от значими към незначими).

Насока 2: Процес на уведомяване

2.1. Доставчиците на платежни услуги следва да съберат цялата значима информация, да изготвят доклад за инцидента, като използват образеца в приложение 1, и да го предоставят на компетентния орган в държавата членка по произход. Доставчиците на платежни услуги трябва да попълнят образеца, като следват инструкциите в приложение 1.

2.2. Доставчиците на платежни услуги следва да използват един и същ образец за информиране на компетентния орган през целия жизнен цикъл на инцидента (т.е. за първоначални, междинни и окончателни доклади, както е описано в точки 2.7—2.21). Доставчиците на платежни услуги следва да попълват образеца на стъпки при полагане на максимални усилия, докато постъпва нова информация в хода на вътрешните разследвания.

2.3. Доставчиците на платежни услуги следва също така да предоставят на компетентния орган в държавата членка по произход, ако е приложимо, копие от информацията, която е предоставена (или която ще бъде предоставена) на потребителите, както е предвидено в член 96, параграф 1, втора алинея от ДПУ 2, веднага след като тя стане достъпна.

2.4. Доставчиците на платежни услуги следва да предоставят на компетентния орган в държавата членка по произход всяка допълнителна информация, ако е налична и е счетена за релевантна от компетентния орган, като приложат допълнителни документи към стандартния образец под формата на едно или няколко приложения.

2.5. Доставчиците на платежни услуги следва да предприемат последващи действия във връзка с евентуални искания от страна на компетентния орган в държавата членка по произход да предоставят допълнителна информация или разяснения относно вече предоставените документи.

2.6. Доставчиците на платежни услуги следва да пазят по всяко време поверителността и целостта на информацията, която се обменя с компетентния орган в тяхната държава членка по произход, както и да се легитимират правилно пред компетентния орган в тяхната държава членка по произход.

Първоначален доклад

2.7. Доставчиците на платежни услуги следва да подадат първоначален доклад до компетентния орган в държавата членка по произход при първоначалното откриване на значим операционен или свързан със сигурността инцидент.

2.8. Доставчиците на платежни услуги следва да изпратят първоначалния доклад до компетентния орган в рамките на 4 часа от момента, в който значимия операционен или свързан със сигурността инцидент бъде открит за първи път, или, ако е известно, че каналите за докладване на компетентния орган не са достъпни или не функционират по това време, веднага щом отново станат достъпни/започнат да функционират.

2.9. Доставчиците на платежни услуги следва да подават първоначален доклад до компетентния орган в държавата членка по произход и в случаите, когато предишен незначим инцидент се превърне в значим инцидент. В този конкретен случай доставчиците на платежни услуги следва да изпратят първоначалния доклад до компетентния орган незабавно след като се установи промяната в статуса, или, ако е известно, че каналите за докладване на компетентния орган не са достъпни или не функционират по това време, веднага щом отново станат достъпни/започнат да функционират.

2.10. Доставчиците на платежни услуги следва да включват в първоначалните си доклади обща информация (т.е. раздел А от образеца), която описва някои от основните характеристики на инцидента и очакваните последици, въз основа на наличната информация веднага след като той бъде открит или прекласифициран. Когато не са налични фактически данни, доставчиците на платежни услуги следва да прибягват до прогнозни цифри. Доставчиците на платежни услуги следва също така да включат в първоначалния си доклад датата на следващата актуализация, която трябва да бъде във възможно най-кратък срок и при никакви обстоятелства да не надхвърля 3 работни дни.

Междинен доклад

2.11. Доставчиците на платежни услуги следва да предоставят междинни доклади всеки път, когато счетат, че е налице значима промяна в статуса и най-малкото преди датата на следващата актуализация, посочена в предишния доклад (първоначалния доклад или предходния междинен доклад).

2.12. Доставчиците на платежни услуги следва да подадат до компетентния орган първи междинен доклад с по-подробно описание на инцидента и неговите последици (раздел Б от образеца). Освен това доставчиците на платежни услуги следва да изготвят допълнителни междинни доклади, като актуализират вече предоставената информация най-малко в раздели А и Б на образеца, когато разберат за нова значима информация или значителни промени след предходното уведомление (напр. дали инцидентът се е разраснал или е намалял, установени ли са нови причини или предприети ли са действия за отстраняването на проблема). Във всички случаи доставчиците на платежни услуги следва да изготвят междинен доклад по искане на компетентния орган в държавата членка по произход.

2.13. Както при първоначалните доклади, ако не са налични действителни данни, доставчиците на платежни услуги следва да използват прогнозни.

2.14. Освен това доставчиците на платежни услуги следва да включат във всеки доклад датата на следващата актуализация, която трябва да бъде във възможно най-кратък срок и при никакви обстоятелства да не надхвърля 3 работни дни. Ако доставчикът на платежни услуги не е в състояние да спази датата, предвидена за следващата актуализация, той следва да се свърже с компетентния орган, за да обясни причините за закъснението, да предложи нов реалистичен краен срок за представяне на актуализирания доклад (не повече от 3 работни дни) и да изпрати нов междинен доклад, като изрично актуализира информацията за датата, предвидена за следващата актуализация.

2.15. Доставчиците на платежни услуги следва да изпратят последния междинен доклад, когато обичайните дейности са възобновени и протичат нормално, като информират компетентния орган за това обстоятелство. Доставчиците на платежни услуги следва да приемат, че стопанската дейност отново протича нормално, когато дейността/операциите са възстановени на същото ниво на обслужване/условия, определени от доставчика на платежни услуги или определени външно чрез споразумение за нивото на обслужване (СНО) по отношение на времето за обработка, капацитета, изискванията за сигурност и т.н., а извънредните мерки са преустановени.

2.16. Ако стопанската дейност се върне към нормалния си ход преди да са изминали 4 часа от откриването на инцидента, доставчиците на платежни услуги следва да се стремят да подадат първоначалния и последния междинен доклад едновременно (т.е. да попълнят раздели А и Б от образеца) в срок до 4 часа.

Окончателен доклад

2.17. Доставчиците на платежни услуги следва да изпратят окончателен доклад, след като бъде извършен анализ на първопричините (независимо дали вече са приложени мерки за редуциране на риска, или е установена окончателната първопричина) и са налице действителни данни, които да заместят всички прогнози.

2.18. Доставчиците на платежни услуги следва да предоставят окончателния доклад на компетентния орган в максимален срок от 2 седмици, след като бъде счетено, че стопанската дейност протича нормално. Доставчиците на платежни услуги, които се нуждаят от удължаване на този срок (напр. ако все още няма налични действителни данни за последствията), следва да се свържат с компетентния орган преди изтичането на срока и да предоставят подходяща обосновка за закъснението, както и нова прогнозна дата за окончателния доклад.

2.19. Ако доставчиците на платежни услуги могат да предоставят цялата информация, която се изисква в окончателния доклад (т.е. раздел В на образеца), в рамките на 4-часовия период след откриването на инцидента, те следва да се стремят да предоставят в първоначалния доклад информацията, свързана с първоначалния, последния междинен и окончателния доклад.

2.20. Доставчиците на платежни услуги следва да се стремят да включват в окончателните си доклади изчерпателна информация, т.е. (i) действителни данни за последствията вместо прогнози (както и всякакви други актуализации, които са необходими в раздели А и Б на образеца) и (ii) раздел В на образеца, който включва първопричината, ако вече е известна, и обобщение на предприетите или планираните мерки за отстраняване на проблема и предотвратяване на повторната му поява в бъдеще.

2.21. Доставчиците на платежни услуги следва също така да изпратят окончателен доклад, ако, в резултат на непрекъснатото оценяване на инцидента, установят, че вече докладван инцидент повече не отговаря на критериите за значим инцидент и не се очаква да ги изпълни, преди инцидентът да бъде разрешен. В такива случаи доставчиците на платежни услуги следва да изпратят окончателния доклад веднага след като това обстоятелство бъде установено и при всички случаи преди датата, предвидена за следващия доклад. В този конкретен случай, вместо да попълнят раздел В на образеца, доставчиците на платежни услуги следва да поставят отметка в кутийката „инцидент, прекласифициран като незначим“ и да обяснят причините, обосноваващи това понижаване на значимостта.

Насока 3: Делегирани и консолидирани доклади

3.1. Ако е разрешено от компетентния орган, доставчиците на платежни услуги, които желаят да делегират задълженията за докладване съгласно ДПУ 2 на трета страна, следва да уведомят компетентния орган в държавата членка по произход и да гарантират изпълнението на следните условия:

а. официалният договор или, ако е приложимо, съществуващите вътрешни договорености в рамките на групата, които са в основата на делегираното докладване между доставчика на платежни услуги и третата страна, недвусмислено определят разпределянето на отговорностите на всички страни. По-конкретно следва да е ясно посочено, че, независимо от евентуалното делегиране на задълженията за докладване, засегнатият доставчик на платежни услуги продължава да носи пълната отговорност и следва да се отчита по отношение на изпълнението на изискванията, изложени в член 96 от ДПУ 2, и съдържанието на информацията, предоставена на компетентния орган в държавата членка по произход.

б. Делегирането отговаря на изискванията за възлагане на външни изпълнители на изпълнението на важни оперативни функции, както е посочено в

i. член 19, параграф 6 от ДПУ 2 по отношение на платежните институции и институциите за електронни пари, приложимо mutatis mutandis в съответствие с член 3 от Директива 2009/110/ЕО (ДМОС); или

ii. насоките на КЕБНО относно възлагането на дейности на външни изпълнители във връзка с кредитните институции.

в. Информацията се предоставя на компетентния орган в държавата членка по произход предварително и във всички случаи, спазвайки всякакви крайни срокове и процедури, установени от компетентния орган, когато е приложимо.

г. Поверителността на чувствителните данни, качеството, последователността, целостта и надеждността на информацията, която се предоставя на компетентния орган, е надлежно осигурена.

3.2. Доставчиците на платежни услуги, които желаят да позволят на определените трети страни да изпълняват задълженията за докладване в консолидиран вид (т.е. чрез представяне на един единствен доклад, отнасящ се до няколко доставчици на платежни услуги, които са засегнати от същия значим операционен или свързан със сигурността инцидент), следва да информират компетентния орган в държавата членка по произход, да добавят информацията за контакт, включена под „Засегнати доставчици“ в образеца, и да се уверят, че са изпълнени следните условия:

а. настоящата разпоредба е включена в договора, който е в основата на делегираното докладване.

б. консолидираното докладване зависи от това дали инцидентът е причинен от прекъсване на услугите, предоставяни от третата страна.

в. консолидираното докладване е ограничено до доставчици на платежни услуги, установени в една и съща държава членка.

г. третата страна оценява значимостта на инцидента за всеки засегнат доставчик на платежни услуги и включва в консолидирания доклад само онези доставчици на платежни услуги, за които инцидентът е класифициран като значим; също така в случай на съмнение, даден доставчик на платежни услуги е включен в консолидирания доклад, докато не възникнат доказателства за това, че не трябва да бъде включен.

д. когато в образеца има полета, в които не е възможно да бъде попълнен общ отговор (напр. раздел Б 2, Б 4 или В 3), третата страна или i) ги попълва поотделно за всеки засегнат доставчик на платежни услуги, като упоменава допълнително самоличността на всеки доставчик на платежни услуги, за когото се отнася информацията, или ii) използва диапазони в полетата, в които това е възможно, които представляват най-ниските и най-високите стойности, наблюдавани или прогнозирани за различните доставчици на платежни услуги.

e. доставчиците на платежни услуги следва да гарантират, че третата страна ги държи информирани по всяко време относно цялата информация, свързана с инцидента, и всички взаимодействия, които третата страна може да има с компетентния орган, и тяхното съдържание, но само доколкото това е съвместимо с избягването на всякакво нарушаване на поверителността по отношение на информацията, която се отнася до други доставчици на платежни услуги.

3.3. Доставчиците на платежни услуги не трябва да делегират своите задължения за докладване, преди да уведомят компетентния орган в държавата членка по произход или след като са били информирани, че споразумението за възлагане на дейност на външен изпълнител не отговаря на изискванията в насока 3.1, буква б).

3.4. Доставчиците на платежни услуги, които желаят да оттеглят делегирането на своите задълженията за докладване, следва да съобщят това решение на компетентния орган в държавата членка по произход, в съответствие със сроковете и процедурите, установени от последния. Доставчиците на платежни услуги следва също така да информират компетентния орган в държавата членка по произход за всяко съществено развитие, засягащо определената трета страна и способността ѝ да изпълни задълженията за докладване.

3.5. Доставчиците на платежни услуги следва да приключат по същество задълженията си за докладване, без да прибягват до външна помощ, винаги когато определената трета страна не успее да уведоми компетентния орган в държавата членка по произход за значим операционен или свързан със сигурността инцидент в съответствие с член 96 от ДПУ 2 и настоящите насоки. Освен това доставчиците на платежни услуги следва да гарантират, че инцидентът не е докладван два пъти, веднъж от въпросния доставчик на платежни услуги и втори път от третата страна.

Насока 4: Операционна политика и политика по сигурността

4.1. Доставчиците на платежни услуги следва да гарантират, че тяхната обща операционна политика и политика по сигурността определят ясно всички задължения за докладване на инциденти по ДПУ 2, както и процедурите за изпълнение на изискванията, определени в настоящите насоки.

5. Насоки, предназначени за компетентните органи, относно критериите за оценка на значението на инцидента и данните в докладите за инцидента, които да бъдат предоставени на други национални органи

Насока 5: Оценка на значението на инцидента

5.1. Компетентните органи в държавата членка по произход следва да оценят значението на значим операционен или свързан със сигурността инцидент за други национални органи, въз основа на собственото си експертно становище и приложат следните критерии като основни показатели за значимостта на дадения инцидент:

   а. причините за инцидента са в регулаторния обхват на другия национален орган (т.е. неговата сфера на компетентност).
   б. последиците от инцидента оказват въздействие върху целите на друг национален орган (напр. запазването на финансова стабилност).
   в. инцидентът засяга или би могъл да засегне ползвателите на платежни услуги в широк мащаб.
   г. инцидентът е вероятно да бъде или вече е широко отразен в медиите.

5.2. Компетентните органи в държавата членка по произход следва да извършват тази оценка непрекъснато през целия жизнен цикъл на инцидента, за да установяват всяка евентуална промяна, която би могла да направи значим даден инцидент, който преди това не е бил считан за такъв.

Насока 6: Информация, която следва да се предоставя

6.1. Независимо от всички други правни изисквания за предоставяне на информация относно инциденти на други национални органи, компетентните органи следва да предоставят информация относно значими операционни или свързани със сигурността инциденти на националните органи, които са установени след прилагането на насока 5.1 (т.е. „другите съответни национални органи“), най-малко към момента на получаване на първоначалния доклад (или доклада, който е довел до предоставянето на информация) и когато бъдат уведомени, че стопанската дейност отново протича нормално (т.е. последния междинен доклад).

6.2. Компетентните органи следва да предоставят на други съответни национални органи информацията, която е необходима, за да се добие ясна представа какво се е случило и какви са потенциалните последици. За целта те следва да предоставят най-малко информацията, подадена от доставчика на платежни услуги в следните полета на образеца (в първоначалния или в междинния доклад):

- дата и час на откриване на инцидента;
- дата и час на започване на инцидента;
- дата и час, когато инцидентът е разрешен или се очаква да бъде разрешен;
- кратко описание на инцидента (включващо нечувствителни части от подробното описание);
- кратко описание на мерките, които са предприети или планирани за възстановяване след инцидента;
- описание на начина, по който инцидентът може да окаже влияние върху други доставчици на платежни услуги и/или инфраструктури;
- описание на медийното отразяване (ако има такова);
- причина за инцидента.

6.3. Компетентните органи следва да извършват подходящо запазване на анонимността, ако е необходимо, и да изключват всяка информация, която би могла да бъде обект на поверителност или на ограничения на правата на интелектуалната собственост, преди да предоставят каквато и да е информация относно инциденти на други съответни национални органи. Независимо от това, компетентните органи следва да предоставят на съответните национални органи името и адреса на докладващия доставчик на платежни услуги, ако въпросните национални органи могат да гарантират, че информацията ще бъде третирана като поверителна.

6.4. Компетентните органи следва винаги да запазват поверителността и неприкосновеността на информацията, която се съхранява и обменя с други съответни национални органи, и да се легитимират надлежно пред другите национални органи. По-конкретно компетентните органи следва да третират цялата информация, получена съгласно настоящите насоки, в съответствие със задълженията за опазване на професионалната тайна, определени в ДПУ 2, без да се засяга приложимото право на Съюза и националните изисквания.

6. Насоки, предназначени за компетентните органи, относно критериите за оценка на съответните данни в докладите за инцидента, които следва да бъдат предоставени на ЕБО и ЕЦБ, и относно формата и процедурите за тяхното съобщаване

Насока 7: Информация, която следва да се предоставя

7.1. Компетентните органи следва винаги да предоставят на ЕБО и ЕЦБ всички доклади, получени от (или от името на) доставчици на платежни услуги, които са засегнати от значим операционен или свързан със сигурността инцидент (т.е. първоначални, междинни и окончателни доклади).

Насока 8: Комуникация

8.1. Компетентните органи следва винаги да запазват поверителността и неприкосновеността на информацията, която се съхранява и обменя с ЕБО и ЕЦБ, и да се легитимират надлежно пред ЕБО и ЕЦБ. По-конкретно компетентните органи следва да третират цялата информация, получена съгласно настоящите насоки, в съответствие със задълженията за опазване на професионалната тайна, определени в ДПУ 2, без да се засяга приложимото право на Съюза и националните изисквания.

8.2. За да се избегнат забавяния при предаването на свързана с инциденти информация на ЕБО/ЕЦБ и за да се сведат до минимум рисковете от операционни прекъсвания, компетентните органи следва да поддържат подходящи средства за комуникация.

Приложение 1 — Образци за докладване за доставчици на платежни услуги

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 ☐ Telephone banking ☐ Point of sale ☐ E-banking ☐ Mobile banking ☐ Other ☐ ATMs If Other, specify:
Payment services affected	☐ Cash placement on a payment account ☐ Credit transfers ☐ Money remittance ☐ Cash withdrawal from a payment account ☐ Direct debits ☐ Payment initiation services ☐ Operations required for operating a payment account ☐ Card payments ☐ Account information services ☐ Acquiring of payment instruments ☐ Issuing of payment instruments ☐ Other If Other, specify:
Functional areas affected	☐ Authentication/authorisation ☐ Clearing ☐ Indirect settlement ☐ Communication ☐ Direct settlement ☐ Other If Other, specify:
Systems and components affected	☐ Application/software ☐ Hardware ☐ Database ☐ 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? If so, when? If so, please describe	☐ YES ☐ NO DD/MM/YYYY, HH:MM
Has the PSP cancelled or weakened some controls because of the incident? If so, please explain	☐ YES ☐ NO

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**

УКАЗАНИЯ ЗА ПОПЪЛВАНЕ НА ОБРАЗЦИТЕ

Доставчиците на платежни услуги следва да попълнят съответните раздели на образеца в зависимост от фазата на докладване, в която се намират: раздел А за първоначалния доклад, раздел Б за междинните доклади и раздел В за окончателния доклад. Всички полета са задължителни, освен ако не е посочено друго.

Заглавие

Първоначален доклад: това е първото уведомление, което доставчикът на платежни услуги подава до компетентния орган в държавата членка по произход.

Междинен доклад: това е актуализация на предишен (първоначален или междинен) доклад за същия инцидент.

Последен междинен доклад: уведомява компетентния орган в държавата членка по произход, че обичайните дейности са възстановени и протичат нормално и по тази причина няма да бъдат подавани други междинни доклади.

Окончателен доклад: това е последният доклад, който доставчикът на платежни услуги изпраща относно инцидента, тъй като i) вече е извършен анализ на първопричините и прогнозните цифри могат да бъдат заменени с действителни стойности или (ii) инцидентът повече не се счита за значим.

Инцидент, прекласифициран като незначим: инцидентът вече не отговаря на критериите, за да се счита за значим, и не се очаква да ги изпълни, преди да бъде разрешен. Доставчиците на платежни услуги следва да обяснят причините за това понижаване на значимостта.

Дата и час на доклада: точните дата и час на предаване на доклада на компетентния орган.

Идентификационен номер на инцидент, ако е приложимо (за междинни и окончателни доклади): референтният номер, издаден от компетентния орган по време на първоначалния доклад, за да се идентифицира еднозначно инцидента, ако е приложимо (т.е. ако компетентният орган е издал такъв номер).

А — Първоначален доклад

А 1 — Обща информация

Вид на доклада:

Индивидуален: докладът е свързан с един доставчик на платежни услуги.

Консолидиран: докладът е свързан с няколко доставчика на платежни услуги, като използва варианта за консолидирано докладване. Полетата под „Засегнат доставчик на платежни услуги“ се оставят празни (с изключение на полето „Държава/държави, засегнати от инцидента“), а списъкът на доставчиците на платежни услуги, включени в доклада, следва да бъде предоставен чрез попълване на съответната таблица (Консолидиран доклад — Списък с доставчици на платежни услуги).

Засегнат доставчик на платежни услуги (ДПУ): отнася се до доставчика на платежни услуги, който е засегнат от инцидента.

Наименование на ДПУ: пълното наименование на доставчика на платежни услуги, който е предмет на процедурата за докладване, както е посочен в приложимия официален национален регистър на доставчици на платежни услуги.

Уникален идентификационен номер на ДПУ, ако е приложимо: съответният уникален идентификационен номер, използван във всяка държава членка за идентифициране на доставчика на платежни услуги; предоставя се от доставчика, ако полето „Номер на лиценз на доставчика на платежни услуги“ не е попълнено.

Номер на лиценз на ДПУ: номер на лиценз в държавата членка по произход.

Ръководно звено на група: в случай на групи от предприятия, както са определени в член 4, параграф 40 от Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета от 25 ноември 2015 г. за платежните услуги във вътрешния пазар, за изменение на директиви 2002/65/ЕО, 2009/110/ЕО и 2013/36/ЕО и Регламент (ЕС) № 1093/2010 и за отмяна на Директива 2007/64/ЕО, посочете наименованието на главното предприятие.

Държава по произход: държавата членка, в която се намира седалището на доставчика на платежни услуги; или ако доставчикът на платежни услуги няма седалище съгласно националното законодателство — държавата членка, в която се намира главното му управление.

Държава/държави, засегнати от инцидента: държавата или държавите, в които се е проявило въздействието на инцидента (напр. засегнати са няколко клона на доставчик на платежни услуги, разположени в различни държави). Може да е или да не е същата като държавата членка по произход.

Основно лице за контакт: собствено име и фамилия на лицето, което отговаря за докладването на инцидента или, ако трета страна докладва от името на засегнатия доставчик на платежни услуги, собствено име и фамилия на лицето, отговарящо за управлението на инциденти/отдел „Рискове“ или подобна област, в засегнатия доставчик на платежни услуги.

Ел. поща: адресът на електронна поща, на който могат да бъдат изпращани всички искания за допълнителни разяснения, ако е необходимо. Може да бъде лична или служебна електронна поща.

Телефон: телефонният номер за връзка в случай на искания за допълнителни разяснения, ако е необходимо. Може да бъде личен или служебен телефонен номер.

Допълнително лице за контакт: собствено име и фамилия на друго лице, с което компетентният орган би могъл да се свърже, за да отправи запитване относно инцидент, ако основното лице за контакт не е на разположение. Ако трета страна докладва от името на засегнатия доставчик на платежни услуги, собствено име и фамилия на друго лице от отдела за управление на инциденти/отдел „Рискове“ или подобна област в засегнатия доставчик на платежни услуги.

Ел. поща: адресът на електронна поща на другото лице за контакт, на който могат да бъдат изпращани всички искания за допълнителни разяснения, ако е необходимо. Може да бъде лична или служебна електронна поща.

Телефон: телефонният номер за връзка с другото лице за контакт в случай на искания за допълнителни разяснения, ако е необходимо. Може да бъде личен или служебен телефонен номер.

Докладващо предприятие: този раздел следва да се попълни, ако трета страна изпълнява задълженията за докладване от името на засегнатия доставчик на платежни услуги.

Наименование на докладващото предприятие: пълно наименование на предприятието, което докладва инцидента, както е посочено в приложимия официален национален търговски регистър.

Уникален идентификационен номер, ако е приложимо: съответният уникален идентификационен номер, използван в държавата, в която се намира третата страна, за идентифициране на предприятието, което докладва инцидента; предоставя се от докладващото предприятие, ако полето „Номер на лиценз“ не е попълнено.

Номер на лиценз, ако е приложимо: номерът на лиценза на третата страна, в държавата, в която се намира, ако е приложимо.
Основно лице за контакт: собствено име и фамилия на лицето, отговарящо за докладването на инцидента.
Ел. поща: адресът на електронна поща, на който могат да бъдат изпращани всички искания за допълнителни разяснения, ако е необходимо. Може да бъде лична или служебна електронна поща.
Телефон: телефонният номер за връзка в случай на искания за допълнителни разяснения, ако е необходимо. Може да бъде личен или служебен телефонен номер.
Допълнително лице за контакт: собствено име и фамилия на друго лице в предприятието, което докладва инцидента, с което компетентният орган би могъл да се свърже, ако основното лице за контакт не е на разположение.
Ел. поща: адресът на електронна поща на другото лице за контакт, на който могат да бъдат изпращани всички искания за допълнителни разяснения, ако е необходимо. Може да бъде лична или служебна електронна поща.
Телефон: телефонният номер на другото лице за контакт, на който могат да бъдат отправени всякакви искания за допълнителни разяснения, ако е необходимо. Може да бъде личен или служебен телефонен номер.

А 2 — Откриване на инциденти и първоначална класификация

Дата и час на откриване на инцидента: датата и часът, в които инцидентът е установен за първи път.
Инцидент е открит от: посочете дали инцидентът е установен от ползвател на платежни услуги, друго лице в рамките на доставчика на платежни услуги (напр. звеното за вътрешен одит) или от външно лице (напр. външен доставчик на услуги). Ако не е нито един от горепосочените, дайте обяснение в съответното поле.
Кратко и общо описание на инцидента: обяснете накратко най-важните елементи на инцидента, като обхванете възможните причини, непосредствените въздействия и др.
Кога е планирана следващата актуализация? посочете датата и часа, за когато е предвидено предаването на следващата актуализация (междинен или окончателен доклад).

Б — Междинен доклад

Б 1 — Обща информация

По-подробно описание на инцидента: опишете основните характеристики на инцидента, като обхванете най-малко елементите, посочени във въпросника (какъв е конкретният проблем, пред който е изправен доставчика на платежни услуги, как е започнал и как се е развил, възможна връзка с предходен инцидент, последици, особено за ползвателите на платежни услуги и др.).
Дата и час на започване на инцидента: датата и часът, в които инцидентът е започнал, ако са известни.
Статус на инцидента:

Диагностициране: установени са характеристиките на инцидента.
Поправка: атакуваните елементи се конфигурират повторно.
Възстановяване: повредените елементи се възстановяват в последното им възстановимо състояние.
Разрешаване: услугата, свързана с плащане, се предоставя отново.

Дата и час когато инцидентът е разрешен или се очаква да бъде разрешен: посочете датата и часа, когато инцидентът е бил или се очаква да бъде под контрол, а стопанската дейност протича или се очаква да протича нормално.

Б 2 — Класифициране на инцидента/информация за инцидента

Общо въздействие: посочете кои аспекти са засегнати от инцидента. Могат да бъдат отметнати няколко кутийки.

Цялост: характеристиката, че активите (вкл. данните) са запазили точността и пълнотата си.

Достъпност: характеристиката, че свързаните с плащания услуги са достъпни и използваеми от ползвателите на платежни услуги.

Поверителност: характеристиката, че информацията не е достъпна или разкрита на неоправомощени лица, единици или процеси.

Автентичност: характеристиката на даден източник да е това, което твърди, че е.

Непрекъснатост: характеристиката на процесите, задачите и активите на дадена организация, които са необходими за предоставянето на свързани с плащанията услуги, да бъдат напълно достъпни и да действат на приемливи, предварително зададени нива.

Засегнати операции: Доставчиците на платежни услуги следва да посочат кои прагове са достигнати или вероятно ще бъдат достигнати от инцидента, ако има такива, и съответните цифри: брой на засегнатите операции, процент на засегнатите операции спрямо броя на платежните операции, извършвани със същите платежни услуги, които са засегнати от инцидента, и общата стойност на операциите. Доставчиците на платежни услуги следва да предоставят конкретни стойности за тези променливи, които може да бъдат или действителни, или прогнозни стойности. Предприятията, които докладват от името на няколко доставчици на платежни услуги (т.е. консолидирано докладване), могат вместо това да предоставят диапазони, които представляват най-ниските и най-високите стойности, наблюдавани или прогнозирани в рамките на групата на включените в доклада доставчици, разделени с тире. Като общо правило, доставчиците на платежни услуги следва да разглеждат като „засегнати операции“ всички вътрешни и трансгранични операции, които са или вероятно ще бъдат пряко или косвено засегнати от инцидента, и по-специално онези операции, които не са могли да бъдат започнати или обработени, операции, при които съдържанието на платежното съобщение е променено, и операции, които са наредени неправомерно (без значение дали средствата са възстановени). Освен това доставчиците на платежни услуги следва да разглеждат обичайното ниво на платежните операции като дневната средно-годишна стойност на вътрешните и трансграничните платежни операции, извършвани със същите платежни услуги, които са засегнати от инцидента, като приемат предходната година за референтен период за изчисленията. Ако доставчиците на платежни услуги не считат тази стойност за представителна (напр. поради сезонност), те следва да използват друг, по-представителен измерител и да съобщят на компетентния орган основния мотив за избор на този подход в полето „Коментари“.

Засегнати ползватели на платежни услуги: Доставчиците на платежни услуги следва да посочат кои прагове са достигнати или вероятно ще бъдат достигнати от инцидента, ако има такива, и съответните цифри: общ брой на засегнатите ползватели на платежни услуги и процент на засегнатите ползватели на платежни услуги спрямо общия брой ползватели на платежни услуги. Доставчиците на платежни услуги следва да предоставят конкретни стойности за тези променливи, които може да бъдат или действителни, или прогнозни стойности. Предприятията, които докладват от името на няколко доставчици на платежни

услуги (т.е. консолидирано докладване), могат вместо това да предоставят диапазони, които представляват най-ниските и най-високите стойности, наблюдавани или прогнозирани в рамките на групата на включените в доклада доставчици, разделени с тире. Доставчиците на платежни услуги следва да разглеждат като „засегнати ползватели на платежни услуги“ всички клиенти (независимо дали са местни или от чужбина, потребители или предприятия), които имат договор със засегнатия доставчик на платежни услуги, който им дава достъп до засегнатата платежна услуга, и които са засегнати или вероятно ще понесат последствията от инцидента. Доставчиците на платежни услуги следва да използват прогнозни цифри, базирани на минала дейност, за да определят броя на ползвателите на платежни услуги, които е вероятно да са използвали платежната услуга по време на жизнения цикъл на инцидента. В случай на групи всеки доставчик на платежни услуги следва да вземе предвид само собствените си ползватели на платежни услуги. В случай на доставчик на платежни услуги, предоставящ операционни услуги на трети лица, този доставчик на платежни услуги следва да вземе предвид само своите собствени ползватели на платежни услуги (ако има такива), а доставчиците на платежни услуги, които получават тези операционни услуги, следва също да направят оценка на инцидента във връзка с техните собствени ползватели на платежни услуги. Освен това доставчиците на платежни услуги следва да приемат за общ брой на ползвателите на платежни услуги общия брой вътрешни и трансгранични ползватели на платежни услуги, които са договорно задължени към тях по време на инцидента (или, като алтернатива, последните налични данни) и имат достъп до засегнатата платежна услуга, независимо от техния размер или независимо дали са считани за активни или пасивни ползватели на платежни услуги.

Прекъсване на услугата: Доставчиците на платежни услуги следва да посочат дали прагът е достигнат или вероятно ще бъде достигнат от инцидента, както и съответната цифра: сумарно време на прекъсване на услугата. Доставчиците на платежни услуги следва да предоставят конкретни стойности за тази променлива, които може да бъдат или действителни, или прогнозни стойности. Предприятията, които докладват от името на няколко доставчици на платежни услуги (т.е. консолидирано докладване), могат вместо това да предоставят диапазони, които представляват най-ниските и най-високите стойности, наблюдавани или прогнозирани в рамките на групата на включените в доклада доставчици, разделени с тире. Доставчиците на платежни услуги следва да вземат предвид периода от време, през който всяка задача, процес или канал, свързани с предоставянето на платежни услуги, са или вероятно ще бъдат неоперативни и, следователно, възпрепятстват (i) започването и/или изпълнението на платежна услуга и/или (ii) достъпа до платежна сметка. Доставчиците на платежни услуги следва да отчитат прекъсването на услугата от момента, в който започне прекъсването, и следва да разглеждат както времевите интервали, през които осъществяват дейност и които са необходими за извършването на платежни услуги, така и неработните часове и периодите за поддръжка, ако е уместно и приложимо. Ако доставчиците на платежни услуги не са в състояние да преценят кога е започнало прекъсването на услугата, по изключение следва да отчитат прекъсването на услугата от момента на откриването на инцидента.

Икономическо въздействие: Доставчиците на платежни услуги следва да посочат дали прагът е достигнат или вероятно ще бъде достигнат от инцидента, както и съответните цифри: преки и непреки разходи. Доставчиците на платежни услуги следва да предоставят конкретни стойности за тези променливи, които може да бъдат или действителни, или прогнозни стойности. Предприятията, които докладват от името на няколко доставчици на платежни услуги (т.е. консолидирано докладване), могат вместо това да предоставят диапазони, които представляват най-ниските и най-високите стойности, наблюдавани или прогнозирани в рамките на групата на включените в доклада доставчици, разделени с тире.

Доставчиците на платежни услуги следва да вземат предвид както разходите, които могат да бъдат пряко свързани с инцидента, така и разходите, които са непряко свързани с инцидента. Наред с другото, доставчиците на платежни услуги следва да вземат предвид иззетите средства или активи, разходите за подмяна на хардуер или софтуер, другите разходи за съдебно-технически експертизи или отстраняване, таксите, дължащи се при неизпълнение на договорни задължения, санкциите, външните задължения и загубата на приходи. По отношение на непреките разходи, доставчиците на платежни услуги следва да вземат под внимание единствено разходите, които са вече известни или има голяма вероятност да се реализират.

Преки разходи: парична сума (евро), пряко начислена за инцидента, включително средствата, необходими за отстраняване на инцидента (напр. иззети средства или активи, разходи за подмяна на хардуер и софтуер, такси, дължащи се на неизпълнение на договорни задължения).

Непреки разходи: парична сума (евро), непряко начислена за инцидента (напр. обезщетения за потребители/разходи за компенсации, приходи, загубени в резултат на пропуснати възможности за извършване на стопанска дейност, потенциални съдебни разноски).

Високо ниво на вътрешно ескалиране: Доставчиците на платежни услуги следва да преценят дали, в резултат на въздействието на инцидента върху услугите, свързани с плащания, главното длъжностно лице, отговарящо за информацията (или сходна длъжност), е уведомено или вероятно ще бъде уведомено за инцидента, извън процедурата за периодично и непрекъснато уведомяване по време на целия жизнен цикъл на инцидента. В случай на делегирано докладване ескалирането настъпва в рамките на третата страна. Освен това доставчиците на платежни услуги следва да преценят дали, в резултат на въздействието на инцидента върху услугите, свързани с плащания, е задействан или е вероятно да бъде задействан кризисен режим.

Други ДПУ или инфраструктури, които са потенциално засегнати: доставчиците на платежни услуги следва да направят оценка на въздействието на инцидента върху финансовия пазар, който представлява инфраструктурите на финансовите пазари и/или схемите за картови плащания, които подпомагат тях и другите доставчици на платежни услуги. По-конкретно доставчиците на платежни услуги следва да оценят дали инцидентът е възникнал или е вероятно да възникне при други доставчици на платежни услуги, независимо дали е засегнал или вероятно ще засегне гладкото функциониране на инфраструктурите на финансовия пазар и дали е изложил на риск или вероятно ще застраши доброто функциониране на финансовата система като цяло. Доставчиците на платежни услуги следва да вземат предвид различните измерения, например дали засегнатият компонент/софтуер е защитен или общодостъпен, дали изложената на риск мрежа е вътрешна или външна и дали доставчикът на платежни услуги е прекратил или вероятно ще спре да изпълнява своите задължения в областта на инфраструктурите на финансовите пазари, на които е член.

Влияние върху репутацията: Доставчиците на платежни услуги следва да разгледат степента на прозрачност, която, доколкото им е известно, инцидентът има или вероятно ще има на пазара. По-конкретно доставчиците на платежни услуги следва да разгледат вероятността инцидентът да причини вреди на обществото, като добър показател за потенциала му да засегне репутацията им. Доставчиците на платежни услуги следва да отчетат дали (i) инцидентът е засегнал прозрачен процес и следователно е вероятно да бъде отразен или вече е отразен в медиите (като се имат предвид не само традиционните медии, напр. вестници, но също блогове, социални мрежи и др.), (ii) регулаторни задължения, които

са или има вероятност да бъдат неизпълнени, (iii) санкции, които са или е вероятно да бъдат нарушени, или (iv) същият вид инцидент е възниквал и преди.

Б 3 — Описание на инцидента

Вид на инцидента: посочете дали, доколкото ви е известно, инцидентът е операционен или е свързан със сигурността.

Операционен: инцидент, произтичащ от неадекватни или неуспешни процеси, хора и системи, или поради събития с непреодолима сила, които оказват влияние върху целостта, достъпността, поверителността, автентичността и/или непрекъснатостта на свързани с плащания услуги.

Свързан със сигурността: нерегламентиран достъп, използване, оповестяване, прекъсване, изменение или унищожаване на активите на доставчика на платежни услуги, което оказва влияние върху целостта, достъпността, поверителността, автентичността и/или непрекъснатостта на свързаните с плащания услуги. Наред с другото, това може да се случи, когато доставчикът на платежни услуги стане жертва на кибератаки, неподходящо проектиране или изпълнение на политиките за сигурност, или недостатъчна физическа сигурност.

Причина за инцидента: посочете причината за инцидента или, ако още не е известна, посочете най-вероятната причина за него. Могат да бъдат отметнати няколко кутийки.

Предмет на разследване: причината още не е определена.

Външна атака: източникът на причината е външен и е умишлено насочен към доставчика на платежни услуги (напр. зловреден софтуер).

Вътрешна атака: източникът на причина идва отвътре и е умишлено насочен към доставчика на платежни услуги (напр. вътрешна измама).

Вид на атаката:

Разпределена атака тип отказ на услуга/Отказ на услуга (DDoS/DoS): опит да се направи недостъпна дадена онлайн услуга, като бъде претоварена с трафик от множество източници.

Заразяване на вътрешни системи: увреждащо действие, което атакува компютърни системи, като се опитва да открадне пространство на харддиска или от времето на използване на централния процесор, да получи достъп до лична информация, да повреди данни, да изпраща спам на контакти и др.

Целенасочено проникване: неупълномощено действие за следене, наблюдение и кражба на информация през киберпространството.

Друго: всякакъв друг вид атака, която доставчикът на платежни услуги може да е изпитал пряко или чрез доставчик на услуги. По-конкретно, ако е имало атака, насочена към процеса за идентифициране и оправомощаване, тази кутийка следва да бъде отметната. В полето за свободен текст следва да се добавят подробности.

Външни събития: причината е свързана със събития, които като цяло са извън контрола на организацията (напр. природни бедствия, правни въпроси, проблеми с дейността и зависимости на услугата).

Човешка грешка: инцидентът е причинен от непреднамерена грешка на дадено лице, или като част от процедурата на плащане (напр. качване на грешна партида за плащанията в платежната система), или свързано по някакъв начин с нея (напр. захранването е прекъснато случайно и платежната дейност е в режим на изчакване).

Неизправност в процеса: причината за инцидента е в лошото проектиране или изпълнение на процеса на плащане, контрола на процеса и/или съпътстващите процеси (напр. процес за промяна/миграция, тестване, конфигурация, капацитет, мониторинг).

Неизправност на системата: причината за инцидента е свързана с неподходящото проектиране, изпълнение, компоненти, спецификации, интеграция или сложност на системите, които спомагат за извършването на платежната дейност.

Друго: причината за инцидента не е нито една от горепосочените. В полето за свободен текст следва да се предостави допълнителна информация.

Инцидентът засяга ли ви пряко или косвено чрез доставчик на услуги?: даден инцидент може да е насочен пряко към доставчик на платежни услуги или да го засяга непряко, чрез трета страна. В случай на непряко въздействие, посочете името на доставчика(ците) на услуги.

Б 4 — Въздействие на инцидента

Засегната сграда/сгради (адрес), ако е приложимо: ако е засегната физическа сграда, посочете адреса ѝ.

Засегнати търговски канали: посочете канала или каналите за взаимодействие с ползватели на платежни услуги, които са били засегнати от инцидента. Могат да бъдат отметнати няколко кутийки.

Клонове: място на дейност (различно от главното управление), което е част от доставчик на платежни услуги, няма правосубектност и извършва пряко някои или всички от операциите, присъщи за дейността на доставчик на платежни услуги. Всички места на дейност, установени в една и съща държава членка от доставчик на платежни услуги с главно управление в друга държава членка, следва да се считат за един клон.

Електронно банкиране: използването на компютри за осъществяване на финансови операции по интернет.

Телефонно банкиране: използването на телефони за осъществяване на финансови операции.

Мобилно банкиране: използването на специално приложение за банкиране чрез смартфон или подобно устройство за осъществяване на финансови операции.

Банкомати: електромеханични устройства, които позволяват на ползвателите на платежни услуги да теглят пари в брой от сметките си и/или да имат достъп до други услуги.

Място на продажба: физическите помещения на търговеца, където е инициирана платежната операция.

Друго: засегнатият търговски канал не е нито един от горепосочените. В полето за свободен текст следва да се предостави допълнителна информация.

Засегнати платежни услуги: посочете платежните услуги, които не функционират правилно в резултат на инцидента. Могат да бъдат отметнати няколко кутийки.

Внасяне на пари в брой по платежна сметка: предоставянето на пари в брой на доставчик на платежни услуги с цел той да ги кредитира по платежна сметка.

Теглене на пари в брой от платежна сметка: искането, получено от даден доставчик на платежни услуги от страна на ползвателя на платежни услуги да му/ѝ предостави пари в брой и да дебитира неговата/нейната платежната сметка със съответната сума.

Операции, необходими за обслужването на платежна сметка: действията, които трябва да бъдат извършени по платежната сметка с цел нейното активиране, деактивиране и/или поддръжка (напр. откриване, блокиране).

Придобиване на платежни инструменти: платежна услуга, състояща се от доставчик на платежни услуги, който се договоря с получател да получава и обработва платежни операции, които водят до прехвърлянето на средства към получателя.

Кредитни преводи: платежна услуга по заверяване на платежна сметка на получателя чрез една или няколко платежни операции, извършвани по платежна сметка на платеца от доставчика на платежни услуги, който води платежната сметка на платеца, въз основа на дадено от платеца нареждане.

Директен дебит: платежна услуга по задължаване на платежна сметка на платец, когато платежната операция се извършва по инициатива на получателя въз основа на даденото от платеца съгласие на получателя, на доставчика на платежни услуги на получателя или на доставчика на платежни услуги на самия платец.

Картови плащания: платежна услуга, базирана на инфраструктурата на платежна картова схема и на правилата за извършване на платежна операция чрез всякакви картови, телекомуникационни, цифрови или информационно-технологични устройства или софтуер, когато това води до операция с дебитна или кредитна карта. От платежните операции, свързани с карти, се изключват операциите на основата на други видове платежни услуги.

Издаване на платежни инструменти: платежна услуга, състояща се от доставчик на платежни услуги, който се договаря с платеца да му предостави платежен инструмент за иницииране и обработка на платежните операции на платеца.

Наличен паричен превод: платежна услуга, при която средствата се получават от платеца, без да са открити платежни сметки на името на платеца или на получателя, с единствената цел прехвърляне на съответната сума на получателя или на друг доставчик на платежни услуги, действащ от името на получателя, и/или когато тези средства се получават от името на получателя и са му предоставени на разположение.

Услуги по иницииране на плащане: платежни услуги, при които се инициира платежно нареждане по искане на ползвателя на платежни услуги по отношение на платежна сметка, държана при друг доставчик на платежни услуги.

Услуги по предоставяне на информация за сметка: онлайн платежни услуги, при които се предоставя обобщена информация за една или повече платежни сметки, държани от ползвателя на платежни услуги, при друг доставчик на платежни услуги или при повече от един доставчик на платежни услуги.

Друго: засегнатата платежна услуга не е нито една от горепосочените. В полето за свободен текст следва да се предостави допълнителна информация.

Засегнати функционални области: посочете етапа или етапите на процеса на плащане, които са засегнати от инцидента. Могат да бъдат отметнати няколко кутийки.

Идентифициране/оправомощаване: процедури, които позволяват на доставчика на платежни услуги да провери самоличността на ползвателя на платежната услуга или валидността на използването на конкретен платежен инструмент, включващо използването на персонализираните средства за сигурност на ползвателя и получаване на съгласие от ползвателя на платежни услуги (или трета страна, която действа от името на този ползвател) за прехвърляне на средства или ценни книжа.

Комуникации: обмен на информация с цел идентифициране, оправомощаване, уведомяване и изпращане на информация между доставчика на платежни услуги,

обслужващ сметки, и доставчиците на услуги по иницииране на плащане, доставчиците на услуги по предоставяне на информация за сметка, платци, получатели и други доставчици на платежни услуги.

Клиринг: процес на предаване, съгласуване и, в някои случаи, потвърждаване на нареждания за превод преди сетълмент, потенциално включващ нетирането на нареждания и установяването на окончателни позиции за сетълмент.

Директен сетълмент: извършването на дадена операция или обработване с цел изпълнение на задълженията на участниците в нея чрез прехвърляне на средства, когато това действие се извършва от самия засегнат доставчик на платежни услуги.

Индиректен сетълмент: извършването на дадена операция или обработване с цел изпълнение на задълженията на участниците в нея чрез прехвърляне на средства, когато това действие се извършва от друг доставчик на платежни услуги от името на засегнатия доставчик на платежни услуги.

Друго: засегнатата функционална област не е нито една от горепосочените. В полето за свободен текст следва да се предостави допълнителна информация.

Засегнати системи и компоненти: посочете коя част или части от технологичната инфраструктура на доставчика на платежни услуги са засегнати от инцидента. Могат да бъдат отметнати няколко кутийки.

Приложение/софтуер: програми, операционни системи и др., които спомагат за предоставянето на платежни услуги от доставчика на платежни услуги.

База данни: информационна структура, която съхранява лични данни и информация за плащания, които са необходими за извършването на платежни операции.

Хардуер: физическо технологично оборудване, което извършва процесите и/или съхранява данните, от които доставчиците на платежни услуги се нуждаят, за да извършват своите дейности, свързани с плащанията.

Мрежа/инфраструктура: телекомуникационни мрежи, публични или частни, които позволяват обмена на данни и информация в процеса на плащане (напр. интернет).

Друго: засегнатите система и компонент не са нито едно от горепосочените. В полето за свободен текст следва да се предостави допълнителна информация.

Засегнат персонал: посочете дали инцидентът е оказал въздействие върху персонала на доставчика на платежни услуги и, ако да, опишете как в полето за свободен текст.

Б 5 — Смекчаване на инцидента

Какви действия/мерки са предприети до момента или се планират за възстановяване след инцидента?: опишете действията, които са предприети или се планира да бъдат предприети за временно разрешаване на инцидента.

Задействани ли са планът за осигуряване на непрекъснатост на стопанската дейност и/или планът за възстановяване при бедствия?: посочете дали това е така и, ако да, предоставете най-важните подробности за това, което се е случило (т.е. кога са задействани и в какво се състоят тези планове).

Отменил или отслабил ли е ДПУ някакви мерки за контрол поради инцидента?: посочете дали доставчикът на платежни услуги е трябвало да отмени някои контролни механизми (напр. да спре използването на „принципа на четирите очи“), за да се справи с инцидента и, ако да, предоставете подробности относно основните причини, които оправдават отслабването или отмяната на мерките за контрол.

В — Окончателен доклад

В 1 — Обща информация

Моля, актуализирайте информацията от междинния доклад (резюме): предоставете допълнителна информация относно действията, предприети за възстановяване от инцидента и предотвратяване на повторната му поява, анализ на първопричините, извлечени поуки и др.

Дата и час на приключване на инцидента: посочете датата и часа, когато инцидентът е счетен за приключен.

Прилагат ли се отново първоначалните мерки за контрол?: ако доставчикът на платежни услуги е трябвало да отмени или отслаби някои мерки за контрол поради инцидента, посочете дали тези мерки за контрол се прилагат отново и предоставете всяка допълнителна информация в полето за свободен текст.

В 2 — Анализ на първопричината и последващи действия

Каква е първопричината, ако вече е известна?: обяснете коя е първопричината за инцидента или, ако още не е известна, предварителните заключения въз основа на анализа на първопричината. Ако счетат за необходимо, доставчиците на платежни услуги могат да приложат файл с подробна информация..

Основни корективни действия/мерки, предприети или планирани за предотвратяване на повторно възникване на инцидента в бъдеще, ако вече са известни: опишете основните действия, които са предприети или се планира да бъдат предприети за предотвратяване на повторна поява на инцидента в бъдеще.

В 3 — Допълнителна информация

Споделян ли е инцидентът с други ДПУ за информационни цели? обобщете с кои доставчици на платежни услуги е осъществена връзка, официално или неофициално, за да бъдат информирани относно инцидента, като предоставите подробности за доставчиците на платежни услуги, които са били уведомени, информацията, която е споделена, и основните причини за споделяне на тази информация.

Предприети ли са правни действия срещу ДПУ?: посочете дали към момента на попълване на окончателния доклад срещу доставчика на платежни услуги са предприети правни действия (напр. срещу него са заведени съдебни искове или той е загубил лиценза си) в резултат на инцидента.