EBA/GL/2021/03

10 юни 2021 г.

Преразгледани насоки

относно докладването на значими инциденти съгласно ДПУ2

1. Спазване на насоките и задължения за докладване

Статут на насоките

1. Настоящият документ съдържа насоки, издадени съгласно член 16 от Регламента за ЕБО[1]. В съответствие с член 16, параграф 3 от Регламента за ЕБО, 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 определени в член 4, параграф 2 от Регламента за ЕБО, за които се отнасят тези насоки, следва 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 предназначени основно за институциите.

Изисквания за докладване

3. Съгласно член 16, параграф 3 от Регламента за ЕБО компетентните органи трябва да уведомят ЕБО дали спазват или възнамеряват да спазват тези насоки, а в противен случай да изложат причините за неспазването им до [07.11.2021]. Ако в посочения срок не постъпи уведомление, ЕБО ще счита, че компетентните органи не спазват насоките. Уведомленията следва да се изпращат чрез подаване на образеца, достъпен на уебсайта на ЕБО, като се посочи референтен номер „EBA/GL/2021/03“. Уведомленията трябва да се подават от лица, имащи подходящи правомощия да отчитат спазване 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 г. 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/ЕС и Регламент (ЕС) № 1093/2010 и за отмяна на Директива 2007/64/ЕО (ДПУ2).

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, както е предвидено в член 96, параграф 1 от ДПУ2, за подобни инциденти на компетентния орган в държавата членка по произход.

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 ДПУ2.

8. Насоките разглеждат също предоставянето на детайли за докладваните инциденти до ЕБО и ЕЦБ, 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 ДПУ2.

10. Настоящите насоки 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 също в случаите, когато значимият операционен или свързан със сигурността инцидент е с произход извън ЕС (напр. инцидентът е с произход от предприятието майка или дъщерно предприятие, установени извън Съюза) и засяга пряко платежните услуги, които се предоставят от доставчик на платежни услуги в Съюза (услугата, свързана с плащане, се извършва от засегнатото предприятие 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).

12. Настоящите насоки се прилагат и за значими инциденти, засягащи функции, възложени от доставчици на платежни услуги на трети страни.

Адресати

13. Първата група от насоки (раздел 4) е предназначена за доставчици на платежни услуги съгласно определението в член 4, параграф 11 от ДПУ2 и както е посочено в член 4, параграф 1 от Регламент (ЕС) № 1093/2010.

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

Определения

15. Освен ако не е посочено друго, термините, използвани и дефинирани в ДПУ2, имат същото значение в насоките. В допълнение, 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 и/или автентичността на услугите, свързани с плащанията.
Цялост	Характеристиката, че активите (включително данните) са запазили точността и пълнотата си.
Достъпност	Характеристиката на услуги, свързани с плащанията да са напълно достъпни и използваеми от ползвателите на платежни услуги в съответствие с приемливи нива, предварително определени от доставчика на платежни услуги.
Поверителност	Характеристиката, че информацията не е достъпна или разкрита на неоправомощени лица, дружества или процеси.
Автентичност	Характеристиката на даден източник да е това, което твърди, че е.
Услуги, свързани с плащанията	Всяка стопанска дейност по смисъла на член 4, параграф 3 от ДПУ2 и всички необходими технически помощни задачи за правилното предоставяне на платежните

услуги.

3. Въвеждане

Датата на прилагане:

16. Настоящите насоки се прилагат от 1 януари 2022 г.

Отмяна

17. Следните насоки се отменят, считано от 1 януари 2022 г.:

Насоки относно докладването на значими инциденти съгласно Директива (ЕС) 2015/2366 (ДПУ2) (EBA/GL/2017/10)

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

а) един или повече критерия с „по-висока степен на въздействие“; или

б) три или повече критерия 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. Нарушаване на сигурността на мрежите или информационните системи

Доставчиците на платежни услуги следва да определят дали злонамерено действие е застрашило сигурността на мрежите или информационните системи, свързани с предоставянето на платежни услуги.

iv. 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 ДПУ2, не може да бъде изпълнено от доставчика на платежни услуги.

v. 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).

vi. 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.

vii. Други доставчици на платежни услуги 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 платежни схеми.

viii. Влияние върху репутацията

Доставчиците на платежни услуги следва да определят как инцидентът може да подкопае доверието на ползвателите 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 инициирани или обработени; операциите, при които съдържанието на платежното съобщение е променено; и операциите, които са наредени неправомерно (без значение дали средствата са възстановени), или при които правилното изпълнение е било възпрепятствано или затруднено по друг начин от инцидента.

За операционни инциденти, засягащи способността за иницииране и/или обработване на операции, доставчиците на платежни услуги следва да докладват само за инциденти с продължителност над един час. Продължителността на инцидента

следва да се измерва от момента на възникване на инцидента до момента, в който са възстановени обичайните дейности/операции до нивото на услугата, която е предоставяна преди инцидента.

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 образеца (вж. приложението).

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, предоставящ 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 със собствените им ползватели на платежни услуги.

За операционни инциденти, засягащи способността за иницииране и/или обработване на операции, доставчиците на платежни услуги следва да докладват само за инцидентите, засягащи ползвателите на платежни услуги, с продължителност над един час. Продължителността на инцидента следва да се измерва от момента на възникване на инцидента до момента, в който са възстановени обичайните дейности/операции до нивото на услугата, която е предоставяна преди инцидента.

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 последната налична цифра) и имат достъп до засегнатата платежна услуга, независимо от техния размер или дали са считани за активни или пасивни ползватели на платежни услуги.

iii. Нарушаване на сигурността на мрежите или информационните системи

Доставчиците на платежни услуги следва да определят дали злонамереното действие е застрашило наличността, автентичността, целостта или поверителността на мрежовите или информационните системи (включително данни), свързани с предоставянето на платежни услуги.

iv. 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 прекъснати и следователно възпрепятстват (i) иницииране и/или изпълнението на платежна услуга и/или (ii) достъпа до платежна сметка. Доставчиците на платежни услуги следва да отмерват 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 относимо и приложимо. Ако доставчиците на платежни услуги не са в състояние да преценят кога е започнало прекъсването на услугата, по изключение те следва да отмерват прекъсването на услугата от момента на откриването му.

v. 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 незаконно присвоените средства или активи, разходите за подмяна на хардуер или софтуер, другите разходи за съдебно-техническа експертиза или 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.

vi. *Високо ниво на вътрешно ескалиране*

Доставчиците на платежни услуги следва да преценят дали, в резултат на въздействието върху услугите, свързани с плащания, ръководният орган, определен в Насоките на ЕБО относно управлението на риска в областта на ИКТ и сигурността, е уведомен или вероятно ще бъде уведомен за инцидента съгласно насока 60, буква г) от Насоките на ЕБО относно управлението на риска в областта на ИКТ и сигурността, 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.

vii. *Други доставчици на платежни услуги 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 платежните схеми, които подкрепят тях и останалите доставчици на платежни услуги. По-конкретно доставчиците на платежни услуги следва да оценят дали инцидентът е възникнал или вероятно ще 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 вероятно ще застраши стабилното 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.

viii. *Влияние върху репутацията*

Доставчиците на платежни услуги следва да разгледат степента на видимост, 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 вземат предвид дали i) ползвателите на платежни услуги и/или други доставчици на платежни услуги са се оплакали от неблагоприятното въздействие на инцидента, ii) инцидентът е засегнал видим процес, свързан с платежни услуги, и следователно има вероятност да получи или вече е получил медийно отразяване (като се имат предвид не само традиционните медии, като например вестници, но и блогове, социални мрежи и др.), iii) са били или вероятно ще бъдат пропуснати договорни задължения, водещи до публикуване на правни действия срещу доставчика на платежни услуги, iv) не са спазени регулаторни изисквания, което е довело до налагането на надзорни мерки или санкции, които са или е вероятно да са направени публично достояние, и v) преди е възниквал подобен тип инцидент.

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** продължителност на инцидента > 1	> 25% от обичайните операции на доставчика на платежни услуги (от гледна точка на броя операции)

	час* **или** > 500 000 EUR **и** продължителност на инцидента > 1 час*	**или** > 15 000 000 EUR
Засегнати ползватели на платежни услуги	> 5 000 **и** продължителност на инцидента > 1 час* **или** > 10 % от ползвателите на платежни услуги на доставчика на платежни услуги **и** продължителност на инцидента > 1 час*	> 50 000 **или** > 25% от ползвателите на платежни услуги на доставчика на платежни услуги
Прекъсване на услугата	> 2 часа	Не е приложимо
Нарушаване на сигурността на мрежите или информационните системи	Да	Не е приложимо
Икономическо въздействие	Не е приложимо	> Макс. (0,1 % капитал от първи ред**, 200 000 EUR) **или** > 5 000 000 EUR
Високо ниво на вътрешно ескалиране	Да	Да. Вероятно е да бъде задействан кризисен режим (или еквивалентен)
Други ДПУ или свързани инфраструктури, които са потенциално засегнати	Да	Не е приложимо
Влияние върху репутацията	Да	Не е приложимо

* Прагът относно продължителността на инцидента за период, по-дълъг от един час, се прилага само за операционни инциденти, които засягат способността на доставчика на платежни услуги да инициира и/или обработва операции.

**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 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 незначим към значим) и в посока надолу (от значим към незначим). Всяко прекласифициране на инцидента от значим на незначим следва да се съобщава на компетентния орган в съответствие с изискванията на насока 2.21 и без ненужно забавяне.

Насока 2: Процес на уведомяване

2.1. Доставчиците на платежни услуги следва да съберат цялата относима информация, да изготвят доклад за инцидента, като попълнят образеца в приложението, и да го предоставят на компетентния орган в държавата членка по произход. Доставчиците на платежни услуги трябва да попълнят всички полета на образеца, като следват инструкциите, предоставени в приложението.

2.2. Доставчиците на платежни услуги следва да използват един и същ образец, когато представят първоначалния, междинния и окончателния доклад, свързан със същия инцидент. Поради това доставчиците на платежни услуги следва постепенно да попълват един образец и да актуализират, когато е приложимо, информацията, предоставена с предходни доклади.

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 ползвателите, както е предвидено в член 96, параграф 1, втора алинея от ДПУ2, веднага след като тя стане достъпна.

2.4. Доставчиците на платежни услуги следва, при поискване от компетентния орган в държавата членка по произход, да предоставят всякакви допълнителни документи, допълващи подадената информация със стандартизирания образец. 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.

2.5. Всяка допълнителна информация, съдържаща се в документите, предоставени от доставчиците на платежни услуги на компетентния орган по инициатива на доставчика на платежни услуги или по искане на компетентния орган в съответствие с насока 2.4, следва да бъде отразена от доставчика на платежни услуги в образеца в съответствие с насока 2.1.

2.6. Доставчиците на платежни услуги следва да запазват по всяко време поверителността и целостта на информацията, която се обменя, 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, след като операционен или свързан със сигурността инцидент е класифициран като значим. Компетентните органи следва своевременно да потвърдят получаването на първоначалния доклад и да определят уникален референтен код, който недвусмислено идентифицира инцидента. Доставчиците на платежни услуги следва да посочат този референтен код, когато представят актуализация на първоначалния доклад или на междинните и окончателните доклади, свързани със същия инцидент, освен ако междинният и окончателният доклад са представени заедно с първоначалния доклад.

2.8. Доставчиците на платежни услуги следва да изпратят първоначалния доклад на компетентния орган в срок от четири часа от момента, в който операционният инцидент или инцидентът, свързан със сигурността, бъде класифициран като значим. Ако е известно, че каналите за докладване на компетентния орган не са на разположение или не се използват по това време, доставчиците на платежни услуги следва да изпратят първоначалния доклад веднага, щом каналите станат достъпни/започнат да функционират отново.

2.9. Доставчиците на платежни услуги следва да класифицират инцидента в съответствие с насоки 1.1 и 1.4 своевременно след установяване на инцидента, но не по-късно от 24 часа след откриването на инцидента и без ненужно забавяне, след като доставчикът на платежни услуги разполага с информацията, необходима за класифицирането на инцидента. Ако е необходимо по-дълго време за класифициране на инцидента, доставчиците на платежни услуги следва да обяснят причините за това в първоначалния доклад, представен на компетентния орган.

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

2.11. Доставчиците на платежни услуги следва да предоставят в първоначалните си доклади обща информация (т.е. раздел А от образеца), която описва някои от основните характеристики на инцидента и предвидените последствия, въз основа на информацията, която е налична веднага, след като той е класифициран като значим. Когато не са налични действителни данни, доставчиците на платежни услуги следва да прибягват до прогнози.

Междинен доклад

2.12. Доставчиците на платежни услуги следва да подадат междинния 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 (времето за обработка, капацитета, изискванията за сигурност и т.н.), и когато извънредните мерки са преустановени. Междинният доклад следва да съдържа по-подробно описание на инцидента и последствията от него (раздел Б от образеца).

2.13. Ако обичайните дейности все още не са възстановени, доставчиците на платежни услуги следва да предоставят междинен доклад на компетентния орган в срок от три работни дни от подаването на първоначалния доклад.

2.14. Доставчиците на платежни услуги следва да актуализират вече предоставената в раздели А и Б на образеца информация, когато разберат за значителни промени след подаването на предходния доклад (напр. дали инцидентът се е разраснал или се е ограничил, установени ли са нови причини или предприети ли са действия за отстраняването на проблема). Това включва случаите, когато инцидентът не е бил разрешен в рамките на три работни дни, поради което доставчиците на платежни услуги би трябвало да подадат допълнителен междинен доклад. Във всички случаи доставчиците на платежни услуги следва да подадат допълнителен междинен доклад по искане на компетентния орган в държавата членка по произход.

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

2.16. Ако стопанската дейност се върне към нормалното си състояние, преди да са изминали четири часа от класифицирането на инцидента като значим, доставчиците на платежни услуги следва да се стремят да подадат първоначалния и междинния доклад едновременно (т.е. да попълнят раздели А и Б от образеца) в срок до четири часа.

Окончателен доклад

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

2.18. Доставчиците на платежни услуги следва да предоставят окончателния доклад на компетентния орган в максимален срок от 20 работни дни, 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 или не са установени първопричините), 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 четири-часовия период след класифицирането на инцидента като значим, те следва да се стремят да предоставят едновременно информацията, свързана с първоначалния, междинния и окончателния доклад.

2.20. Доставчиците на платежни услуги следва да включват в окончателния си доклад изчерпателна информация, т.е. i) действителни цифри 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 вече 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 в рамките на срока за подаване на следващия доклад. В такива ситуации, вместо да попълват раздел В на образеца, доставчиците на платежни услуги следва да поставят отметка в квадратчето „инцидент, прекласифициран като незначим“ и да дадат обяснение за причините, обосноваващи това прекласифициране.

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 ДПУ2 на трета страна, следва да уведомят компетентния орган в държавата членка по произход и да гарантират изпълнението на следните условия:

a) 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, предвидени в член 96 от ДПУ2, и съдържанието на информацията, предоставена на компетентния орган в държавата членка по произход;

б) делегирането отговаря на изискванията за възлагане на дейности на външни изпълнители на изпълнението на важни оперативни функции, както е посочено във:

i. член 19, параграф 6 от ДПУ2 по отношение на платежните институции и институциите за електронни пари, приложимо mutatis mutandis в съответствие с член 3 от Директива 2009/110/ЕО; или

ii. насоките на ЕБО за възлагане на дейности на външни изпълнители (EBA/GL/2019/02) по отношение на всички доставчици на платежни услуги;

в) информацията се предоставя на компетентния орган в държавата членка по произход предварително и при всички случаи, спазвайки всички 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 лица да изпълняват задълженията за докладване по консолидиран начин (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 предоставят информацията за контакт, включена под „Засегнат доставчик на платежни услуги“ 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, инцидентът да 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) да е предоставен списък на всички доставчици на платежни услуги, засегнати от инцидента;

д) да е гарантирано, че 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 да е гарантирано, че 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;

е) да е гарантирано, че когато в образеца има полета, в които не е възможно да бъде попълнен общ отговор (напр. раздел Б2, Б4 или В3), 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 общите стойности, наблюдавани или прогнозирани за различните доставчици на платежни услуги;

ж) третата страна държи доставчика на платежни услуги информиран по всяко време относно цялата информация, свързана с инцидента, и всички взаимодействия, които третата страна може да има с компетентния орган, и нейното съдържание, но само доколкото това е възможно, за да се избегне 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, при спазване на 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 изпълнят 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 ДПУ2 и настоящите насоки. Доставчиците на платежни услуги следва да гарантират също, че инцидентът не е докладван два пъти, веднъж от въпросния доставчик на платежни услуги и втори път от третата страна.

3.6. Доставчиците на платежни услуги следва да гарантират, че в случаите, когато инцидентът е предизвикан от прекъсване на услугите, предоставяни от доставчик на техническа услуга (или инфраструктура), което засяга множество доставчици на платежни услуги, делегираното докладване се отнася до индивидуалните данни на доставчика на платежни услуги (освен в случай на консолидирано докладване).

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 съгласно ДПУ2, както и въведените процеси 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, като вземат за основа 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) последствията 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 установят 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, най-малко към момента на получаване на първоначалния доклад (или доклада, който е довел до предоставяне на информацията) и когато

бъдат уведомени, че стопанската дейност отново протича нормално (т.е. междинния доклад).

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

- Дата и час на класифициране на инцидента като значим
- 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 (ако има такова) на медийното отразяване
- 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 инцидента на съответните 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, и да се легитимират надлежно пред съответните национални органи. По-конкретно компетентните органи следва да третират цялата информация, получена съгласно настоящите насоки, в съответствие със задълженията за опазване на професионалната тайна, предвидени в ДПУ2, 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 посредством стандартизиран файл, достъпен на уебсайта на ЕБО.

Насока 8: Комуникация

8.1. Компетентните органи следва винаги да запазват поверителността и неприкосновеността на информацията, която се съхранява и обменя, 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 ДПУ2, 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 използването на подходящи средства за комуникация.

Приложение — Образец за докладване за доставчици на платежни услуги

Първоначален доклад

Първоначален доклад	в рамките на 4 часа от класифицирането на инцидента като значим	Reset dropdown selections
Дата на доклада (ДД/ММ/ГГГГ)		Час (ЧЧ:ММ)
Референтен код на инцидента		

A — Първоначален доклад									
A 1 — ОБЩА ИНФОРМАЦИЯ									
Вид на отчета									
Вид на отчета									
Засегнат доставчик на платежни услуги (ДПУ)									
Наименование на ДПУ									
Национален идентификационен номер на ДПУ									
Ръководно звено на група, ако е приложимо									
Държава/държави, засегната/и от инцидента	☐ AT	☐ DE	☐ FR	☐ IE	☐ LV	☐ PT			
	☐ BE	☐ DK	☐ LI	☐ IS	☐ MT	☐ RO			
	☐ BG	☐ EE	☐ GR	☐ ИТ	☐ NL	☐ SE			
	☐ CY	☐ ES	☐ HR	☐ LT	☐ HE	☐ SI			
	☐ CZ	☐ FI	☐ HU	☐ LU	☐ PL	☐ SK			
Главно лице за връзка				Ел. поща			Телефон		
Допълнително лице за контакт				Ел. поща			Телефон		
Докладващо предприятие (попълнете този раздел, ако докладващото предприятие не е засегнатият ДПУ, в случай на делегирано докладване)									
Наименование на докладващия субект									
Национален идентификационен номер									
Главно лице за връзка				Ел. поща			Телефон		
Допълнително лице за контакт				Ел. поща			Телефон		
A 2 — ОТКРИВАНЕ НА ИНЦИДЕНТИ и КЛАСИФЦИРАНЕ									
Дата и час на откриване на инцидента (ДД/ММ/ГГГГ ЧЧ:ММ)									
Дата и час на класифицирането на инцидента (ДД/ММ/ГГГГ ЧЧ:ММ)									
Инцидентът е открит от				Ако сте избрали „Друго“, обяснете:					
Вид на инцидента									
Критерии за задействане на доклада за значими инциденти	☐ Засегнати операции	☐ Засегнати ползватели на платежни услуги	☐ Прекъсване на услугата	☐ Нарушаване на сигурността на мрежите или информационните	☐ Икономическо	☐ Високо ниво на вътрешно ескалиране	☐ Други ДПУ или инфраструктури, които са потенциално засегнати	☐ Влияние върху	
Кратко и общо описание на инцидента									
Въздействие в други държави – членки на ЕС, ако е приложимо									
Докладване пред други органи				Ако сте избрали „Да“, обяснете:					
Причини за късно подаване на първоначалния доклад									

Междинен доклад

Доклад за значим инцидент

Междинен доклад	максимум 3 работни дни от подаване на първоначалния доклад	Reset dropdown selections

Дата на доклада (*ДДММГГГГ*) | Час (*чч:мм*)

Референтен код на инцидента

Б — Междинен доклад

Б 1 — ОБЩА ИНФОРМАЦИЯ

По-подробно описание на инцидента:	
Какъв е конкретният проблем?	
Как е започнал инцидентът?	
Как се е развил?	
Какви са последиците (по-специално за ползвателите на платежни услуги)?	
Съобщено ли е за инцидента на ползвателите на платежни услуги?	Ако сте избрали „Да", обяснете:
Свързан ли е с предишен(и) инцидент(и)?	Ако сте избрали „Да", обяснете:
Засегнати ли са или са участвали други доставчици на услуги/трети страни?	Ако сте избрали „Да", обяснете:
Започнато ли е управлението на кризи (вътрешно и/или външно)?	Ако сте избрали „Да", обяснете:
Дата и час на започване на инцидента (ако вече са известни) (*ДДММГГГГ чч:мм*)	
Дата и час, когато инцидентът е разрешен или се очаква да бъде разрешен (*ДДММГГГГ чч:мм*)	
Засегнати функционални области	☐ Идентифициране/оправомощаване ☐ Директен сетълмент ☐ Комуникации ☐ Индиректен сетълмент ☐ Клиринг ☐ Други — Ако сте избрали „Друго"
Промени, направени в предходни доклади	

Б 2 — КЛАСИФИЦИРАНЕ на ИНЦИДЕНТА/ИНФОРМАЦИЯ ЗА ИНЦИДЕНТА

Засегнати операции [2]	ниво на въздействие Брой на засегнатите операции Като % от обичайния брой операции Стойност на засегнатите операции в EUR Продължителност на инцидента (приложимо само за оперативни инциденти) Коментари:
Засегнати ползватели на платежни услуги [3]	ниво на въздействие Брой на засегнатите ползватели на платежни услуги Като % от общия брой ползватели на платежни услуги
Нарушаване на сигурността на мрежите или информационните системи	Опишете по какъв начин са засегнати мрежата или информационните системи
Прекъсване на услугата	Сумарно време на прекъсване на услугата: Дни: Часове: Минути:
Икономическо въздействие	ниво на въздействие Преки разходи в EUR Непреки разходи в EUR
Високо ниво на вътрешно ескалиране	Опишете нивото на вътрешното ескалиране на инцидента, като посочите дали е задействан или е вероятно да бъде задействан кризисен режим (или еквивалентен), и ако е така, опишете
Други ДПУ или инфраструктури, които са потенциално засегнати	Опишете как инцидентът може да засегне други ДПУ и/или инфраструктури
Влияние върху репутацията	Опишете как инцидентът може да окаже влияние върху репутацията на ДПУ (напр. медийно отразяване, публикуване на правни действия или нарушения на правото...)

Б 3 — ОПИСАНИЕ НА ИНЦИДЕНТА

Вид на инцидента	☐ Предмет на разследване
Причина за инцидента	☐ Злонамерени действия ☐ Неизправност в процеса ☐ Неизправност на системата ☐ Човешки грешки ☐ Външни събития ☐ Друго Ако сте избрали „Друго", обяснете:
Инцидентът засяга ли Ви пряко или косвено чрез доставчик на услуги?	посочете наименованието на доставчика на услуги:

Б 4 — ВЪЗДЕЙСТВИЕ НА ИНЦИДЕНТА

Общо въздействие	☐ Цялост	☐ Поверителност	
	☐ Достъпност	☐ Автентичност	
Засегнати търговски канали	☐ Клонове	☐ Телефонно банкиране	☐ Място на продажба
	☐ Електронно банкиране	☐ Мобилно банкиране	☐ Други
	☐ Електронна търговия	☐ Банкомати	
Засегнати платежни услуги	Ако сте избрали „Друго", обяснете:		
	☐ Внасяне на пари в брой по платежна сметка	☐ Кредитни преводи	☐ Наличен паричен
	☐ Теглене на пари в брой от платежна сметка	☐ Директни дебити	☐ Услуги по
	☐ Операции, необходими за обслужването на платежна	☐ Картови плащания	☐ Услуги по предоставяне на информация за сметка
	☐ Приемане на платежни инструменти	☐ Издаване на платежни инструменти	

Б 5 — СМЕКЧАВАНЕ НА ИНЦИДЕНТА

Какви действия/мерки са предприети до момента или се планират за възстановяване след инцидента?	
Задействани ли са планът за осигуряване на непрекъснатост на стопанската дейност и/или планът за възстановяване при катастрофични събития?	
Ако „Да", кога? (*ДДММГГГГ чч:мм*)	
Ако сте посочили „Да", опишете	

Окончателен доклад

Доклад за значим инцидент

Моля, изберете типа доклад:

в рамките на 20 работни дни от подаване на междинния доклад

Ако сте избрали „Да", опишете:
(приложимо за инциденти, прекласифицирани като незначими)

Reset dropdown selections

Дата на доклада (ДД.ММ.ГГГГ)
Референтен код на инцидента:
Час (чч:мм)

В — Окончателен доклад	
Ако не е бил изпратен междинен доклад, попълнете и раздел Б	
В 1 — ОБЩА ИНФОРМАЦИЯ	
Актуализиране на информацията от първоначалния доклад и междинния(ите) доклад(и)	
Промени, направени в предходни доклади	
Всякаква друга свързана информация	
Въведени ли са всички първоначални проверки? Ако сте посочили „Не", посочете проверките и допълнителния период, необходим за тяхното възстановяване	
В 2 — АНАЛИЗ НА ПЪРВОПРИЧИНАТА И ПОСЛЕДВАЩИ ДЕЙСТВИЯ	
Каква е първопричината (ако вече е известна)?	☐ Злонамерени ☐ Неизправност в ☐ Неизправност на ☐ човешка грешка ☐ Външно събитие ☐ Друго
Моля посочете:	☐ Злоумишлен код ☐ Събиране на информация ☐ Проникване ☐ Разпределена атака тип отказ на услуга/Отказ на услуга (D/DoS) ☐ Умишлени вътрешни ☐ Умишлени външни материални щети ☐ Сигурност на информационното ☐ Измамни действия ☐ Друго ☐ Пропуски в наблюдението и контрола ☐ Въпроси, свързани с ☐ Неправилна експлоатация ☐ Неадекватно управление на промените ☐ Неадекватност на вътрешните процедури и документация ☐ Въпроси, свързани с ☐ Друго ☐ Неизправност ☐ Повреда на ☐ Въпроси, ☐ Неизправност на софтуера/приложната ☐ Материални ☐ Друго ☐ Непредвидени ☐ Бездействие ☐ Недостатъчни ресурси ☐ Друго ☐ Неизправност на доставчик/доставчик на техническа услуга ☐ Непреодолима ☐ Друго Ако сте избрали „Друго", обяснете:
Друга информация от значение за първопричината	
Основни корективни действия/мерки, предприети или планирани за предотвратяване на повторно възникване на инцидента в бъдеще, ако вече са известни	
В 3 — ДОПЪЛНИТЕЛНА ИНФОРМАЦИЯ	
Споделян ли е инцидентът с други ДПУ за информационни цели?	Ако сте посочили да „Да", посочете подробности:
Предприети ли са правни действия срещу ДПУ?	Ако сте посочили да „Да", посочете подробности:
Оценка на ефективността на предприетите действия	Моля, посочете подробности:

УКАЗАНИЯ ЗА ПОПЪЛВАНЕ НА ОБРАЗЕЦА

Доставчиците на платежни услуги (ДПУ) 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. ДПУ следва да използват един и същ образец, когато представят първоначалния, междинния и окончателния доклад, свързан със същия инцидент. Всички полета са задължителни, освен ако не е ясно 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: съдържа по-подробно описание на инцидента и последствията от него. Той е актуализация на първоначалния доклад (и, когато е приложимо, на предходен междинен доклад) за същия инцидент.

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

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 прекласифициране.

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

Референтен номер на инцидента (приложим за междинни и окончателни доклади, както и за актуализациите на първоначалния доклад): референтният код, издаден от компетентния орган по време на първоначалния доклад, който идентифицира еднозначно инцидента. Всеки компетентен орган следва да включи като представка двусимволния ISO код[2] на съответната държава членка.

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 ДПУ в рамките на една и съща държава членка, които са засегнати от един и същ значим операционен инцидент или инцидент, свързан със сигурността, които използват 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 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 доставчиците на платежни услуги.

Национален идентификационен номер на ДПУ: уникалният национален идентификационен номер, използван от компетентния орган на държавата членка по

[2] Направете справка с двусимволните кодове на държавите съгласно ISO-3166 на адрес: https://www.iso.org/iso-3166-country-codes.html

произход в националния му регистър за недвусмислено идентифициране на ДПУ.

Ръководно звено на група: в случай на групи от предприятия, както са определени в член 4, параграф 40 от ДПУ2, посочете наименованието на главното предприятие.

Държава/държави, засегната/и 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), независимо от сериозността на инцидента в другата държава/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 ДПУ, собствено име и фамилия на лицето, отговарящо за управлението на инциденти/отдела по риска или подобна област в засегнатия ДПУ.

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, чрез който могат да бъдат отправяни 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/отдела по риска 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 на другото лице за контакт, чрез който могат да бъдат отправени всякакви 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, ако е приложимо.

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

Национален идентификационен номер: уникалният национален идентификационен номер, използван в държавата, в която се намира третата страна, за да се идентифицира недвусмислено субектът, който докладва инцидента. Ако докладващата трета страна е ДПУ, националният идентификационен номер следва да бъде уникалният национален идентификационен номер на ДПУ, използван от компетентния орган на държавата членка по произход в неговия национален регистър.

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, чрез който могат да бъдат отправяни 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, чрез 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 класификация

Дата и час на откриване на инцидента: датата и часът, в които инцидентът е установен за първи път.

Дата и час на класифициране на инцидента: датата и часът, в които инцидентът, свързан със сигурността, или операционният инцидент, е бил класифициран като значим.

Инцидент, 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 друго външно лице (напр. доставчик на услуги). Ако не е нито един от горепосочените, дайте обяснение в съответното поле.

Вид на инцидента: посочете дали, доколкото ви е известно и доколкото е налична информацията, дали 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 и/или непрекъснатостта на услуги, свързани с плащания.

Свързан със сигурността: нерегламентиран достъп, използване, разкриване, прекъсване, изменение или унищожаване на активите на доставчика на платежни услуги, което оказва влияние върху целостта, достъпността, поверителността и/или автентичността на услуги, свързани с плащания. Това може да се случи, наред с другото, когато ДПУ претърпи нарушение на сигурността на мрежите или информационните системи.

Критерии за задействане на докладването на значим инцидент: посочете кой от критериите е задействал докладването на значимия инцидент. Може да бъдат избрани няколко критерия: засегнати операции, засегнати ползватели на платежни услуги, прекъсване на услугата, нарушаване на сигурността на мрежите или информационните системи, икономическо въздействие, високо ниво на вътрешно ескалиране, други ДПУ или свързани инфраструктури, които са потенциално засегнати, и/или влияние върху репутацията.

Кратко и общо описание на инцидента: обяснете накратко най-важните елементи на инцидента, като обхванете възможните причини, непосредствените въздействия и др.

Въздействие в други държави членки на ЕС, ако е приложимо: обяснете накратко въздействието на инцидента в друга държава членка на ЕС (напр. върху ползвателите на платежни услуги, ДПУ и/или платежните инфраструктури). Ако е осъществимо в рамките на приложимите срокове за докладване, моля да предоставите превод на английски език.

Докладване пред други органи: посочете дали инцидентът е бил/ще бъде докладван на други органи съгласно отделна рамка за докладване на инциденти, ако са известни към момента на докладването. Ако отговорът е „да“, посочете съответните органи.

Причини за късното подаване на първоначалния доклад: обяснете причините, поради които са ви необходими повече от 24 часа, за да класифицирате инцидента.

Б Междинен доклад

Б 1 – Обща информация

По-подробно описание на инцидента: опишете основните характеристики на инцидента, като включите най-малко информацията за конкретния проблем и свързаната с него информация, описанието на начина, по който инцидентът е започнал и се е развил, както и последиците, особено за ползвателите на платежни услуги и др. Моля да предоставите също така информация относно комуникацията с ползвателите на платежни услуги, ако е приложимо.

Свързан ли е с предходен(ни) инцидент(и)?: посочете дали инцидентът е свързан с предходни инциденти, ако тази информация е налична. Ако инцидентът е свързан с предходни инциденти, посочете кои.

Засегнати или участвали ли са други доставчици на услуги/трети страни?: посочете дали инцидентът е засегнал или включвал други доставчици на услуги/трети страни, ако тази информация е налична. Ако инцидентът е засегнал или е включвал други доставчици на услуги/трети страни, избройте ги и предоставете повече информация.

Започнало ли е управлението на кризи (вътрешно и/или външно)?: посочете дали е започнало управлението на кризи (вътрешно и/или външно). Ако управлението на кризи е започнало, дайте повече информация.

Дата и час на започване на инцидента: датата и часът, в които инцидентът е започнал, ако са известни.

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.

Засегнати функционални области: посочете стъпката или стъпките от платежния процес, които са били засегнати от инцидента, например идентифициране/оправомощаване, комуникация, клиринг, директен сетълмент, индиректен сетълмент и други.

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

Комуникации: обмен на информация с цел идентифициране, оправомощаване, уведомяване и изпращане на информация между доставчиците на платежни услуги, които обслужват 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.

Промени, направени в предходни доклади: посочете промените, направени в информацията, предоставена с предходни доклади, свързани със същия инцидент (напр. първоначалния или,

когато е приложимо, междинния доклад).

Б 2 – Класифициране на инцидента/Информация за инцидента

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 действителни или прогнозни. 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 инициирани или обработени, операции, при които съдържанието на платежното нареждане 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“. В случаите, когато платежните операции във валути, различни от евро, са засегнати от инцидента, при изчисляването на праговете и отчитането на стойността на засегнатите трансакции ДПУ следва да конвертират в евро сумата на операциите във валута, различна от евро, като използват референтния обменен курс на ЕЦБ за деня, предхождащ предоставянето на доклада за инцидента.

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 свързаните 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. 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 ДПУ, 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 прогнози, 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 своите 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 собствените 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, последната налична цифра) и имат достъп до засегнатата платежна услуга, независимо от техния размер или независимо дали са считани за активни или пасивни

ползватели на платежни услуги.

Нарушаване на сигурността на мрежите или информационните системи: Доставчиците на платежни услуги следва да определят дали злонамереното действие е застрашило наличността, автентичността, целостта или поверителността на мрежовите или информационните системи (вкл. данни), свързани с предоставянето 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. 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 прекъснати и, следователно, възпрепятстват i) иницииране и/или изпълнението на платежна услуга и/или ii) достъпа до платежна сметка. Доставчиците на платежни услуги следва да отмерват 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 те следва да отмерват прекъсването на услугата от момента на откриването му.

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. 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 незаконно присвоените средства или активи, разходите за подмяна на хардуер или софтуер, другите разходи за съдебно-техническа експертиза или отстраняване, таксите, дължащи се за 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. В случаите, когато разходите са във валути, различни от евро, при изчисляването на прага и отчитането на стойността на икономическото въздействие ДПУ следва да конвертират в евро сумата на разходите във валута, различна от евро, като използват референтния обменен курс на ЕЦБ за деня, предхождащ представянето на доклада за инцидента.

> **Преки разходи:** разходи (в евро), нанесени пряко от инцидента, включително разходи за коригиране на инцидента (напр. отчуждени средства или активи, разходи за подмяна на хардуер и софтуер, такси поради неспазване на договорни задължения).
>
> **Непреки разходи:** разходи (в евро), причинени непряко от инцидента (напр. разходи за правна защита/компенсация на клиентите, потенциални съдебни разходи).

Високо ниво на вътрешно ескалиране: Доставчиците на платежни услуги следва да преценят дали, в резултат на въздействието върху услугите, свързани с плащания, ръководният орган, определен в Насоките на ЕБО относно управлението на риска в областта на ИКТ и сигурността, е уведомен или вероятно ще бъде уведомен за инцидента, съгласно насока 60, буква г) от Насоките на ЕБО относно управлението на риска в областта на ИКТ и сигурността, 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 услуги, свързани с плащанията, е задействан или е вероятно да бъде задействан кризисен режим.

Други ДПУ или свързани инфраструктури, които са потенциално засегнати: ДПУ следва да оценят въздействието на инцидента върху финансовия пазар, който представлява инфраструктурите на финансовите пазари и/или платежните схеми, които го подпомагат, както и другите ДПУ. По-специално ДПУ следва да оценят дали инцидентът е възникнал или е вероятно да възникне при други ДПУ, независимо дали е засегнал или вероятно ще засегне гладкото функциониране на инфраструктурите на финансовите пазари и дали е изложил на риск или вероятно ще застраши надеждността 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 ДПУ 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 видимост, която, доколкото им е известно, инцидентът има или вероятно ще има на пазара. По-конкретно ДПУ 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 вземат предвид дали: i) ползвателите на платежни услуги и/или други ДПУ са се оплакали от неблагоприятното въздействие на инцидента, ii) инцидентът е засегнал видим процес, свързан с платежни услуги, и следователно има вероятност да получи или вече е получил медийно отразяване (като се имат предвид не само традиционните медии, като например вестници, но и блогове, социални мрежи и др.; медийното отразяване в този контекст обаче означава не само няколко негативни коментара от последователи, следва да е налице валиден доклад или значителен брой негативни коментари/сигнали), iii) пропуснати са или вероятно ще бъдат пропуснати договорни задължения, което е довело до публикуването на правни действия срещу доставчика на платежна услуга, iv) не са спазени договорни задължения, което е довело до налагане на надзорни мерки или санкции, които са или е вероятно да бъдат оповестени, или v) преди е възниквал подобен тип инцидент.

Б 3 – Описание на инцидента

Тип инцидент: операционен или свързан със сигурността. Допълнителни обяснения са дадени в съответното поле в първоначалния доклад.

Причина за инцидента: посочете причината за инцидента и, ако все още не е известна, тази, която е най-вероятна. Можете да изберете няколко отговора.

Предмет на разследване: поставете отметка в квадратчето, когато причината понастоящем не е известна.

Злонамерени действия: действия, насочени умишлено към доставчика на платежни услуги. Те включват зловреден код, събиране на информация, намеса, разпределена атака тип „отказ на услуга“/отказ на услуга (D/DoS), умишлени вътрешни действия, умишлени външни материални щети, сигурност на информационното съдържание, измамни действия и други. За повече подробности вж. раздел Б 2 от настоящия образец.

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

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

Човешки грешки: инцидентът е причинен от непреднамерена грешка на дадено лице, било то 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).

Външни събития: причината е свързана със събития, които като цяло са извън прекия контрол на организацията (напр. природни бедствия, повреда при доставчик на техническа услуга).

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

Инцидентът засегна ли Ви пряко или косвено чрез доставчик на услуги?: посочете дали инцидентът е бил насочен пряко към доставчика на платежни услуги, или го засяга косвено чрез трета страна, ако тази информация е налична. В случай на непряко въздействие, посочете името на доставчика(ците) на услуги.

Б 4 – Въздействие на инцидента

Цялостно въздействие: посочете кои измерения са засегнати от инцидента, свързан с функционирането или сигурността. Можете да изберете няколко отговора.

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

Достъпност: характеристиката на свързаните с плащанията услуги да бъде напълно достъпна и използваема от ползвателите на платежни услуги в съответствие с приемливи предварително определени равнища.

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

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

Засегнати търговски канали: посочете канала или каналите за взаимодействие с ползватели на платежни услуги, които са били засегнати от инцидента. Можете да отметнете няколко квадратчета.

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 адрес на 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.

Електронна търговия: платежната операция се инициира на виртуален пункт за продажба (напр. за плащания, инициирани по интернет чрез кредитни преводи, платежни карти, прехвърляне на електронни пари между сметки за електронни пари).

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. Можете да отметнете няколко квадратчета.

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).

Приемане на плащания с платежни инструменти: платежна услуга, при която доставчик на платежни услуги се договоря с получател да приема 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 от 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 платежните услуги при друг доставчик на платежни услуги, или при повече от един доставчик на платежни услуги.

Б 5 – Смекчаване на инцидента

Какви действия/мерки са предприети до момента или се планират за възстановяване след инцидента?: представете подробности за действията, които са били предприети или се планира да бъдат предприети за временно справяне с 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 това е така, посочете най-важните подробности за това, което се е случило (т.е. кога е задействан и в какво се е състоял).

В – Окончателен доклад

В 1 – Обща информация

Актуализиране на информацията от първоначалния доклад и междинния(ите) доклад(и) (резюме): представете допълнителна информация за инцидента, включително конкретните промени, направени в информацията, предоставена с междинния доклад. Включете и всякаква друга свързана информация.

Въведени ли са всички първоначални мерки за контрол?: посочете дали доставчикът на платежни услуги е трябвало да отмени или да отслаби някои проверки в какъвто и да е момент по време на инцидента. Ако отговорът е „да“, посочете дали всички мерки за контрол са възстановени и, ако това не е така, обяснете в полето за свободен текст кои проверки не са въведени отново и какъв допълнителен срок е необходим за тяхното възстановяване.

В 2 – Анализ на първопричината и последващи действия

Каква е първопричината, ако вече е известна?: посочете каква е първопричината за инцидента или, ако все още не е известна, коя е най-вероятната. Можете да изберете няколко отговора. (Имайте предвид, че първопричината следва да бъде разграничена от въздействието на инцидента.)

Злонамерени действия: външни или вътрешни действия, насочени умишлено към доставчика на платежни услуги. Те са разделени в следните категории:

Зловреден код: напр. вирус, червеи, троянски кон, шпионски софтуер.

Събиране на информация: напр. сканиране, подслушване, социално инженерство.

Намеси: напр. компрометиране на привилегировани сметки, компрометиране на непривилегировани сметки, компрометиране на приложения, бот.

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

Умишлени вътрешни действия: напр. саботаж, кражба.

Умишлени външни материални щети: напр. саботаж, физическо нападение на помещенията/центровете за данни.

Сигурност на информационното съдържание: неразрешен достъп до информация, неразрешено изменение на информация).

Измамни действия: неразрешено използване на ресурси, авторски права, маскиране, фишинг.

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

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, изпитване, конфигурация, капацитет, мониторинг). Те са разделени в следните категории:

Пропуски в наблюдението и контрола: напр. във връзка с текущите операции, датите на изтичане на срока на валидност на сертификата, датите на изтичане на валидността на лицензите, датите на изтичане на корекциите, определените максимални насрещни стойности, нивата на попълване на базата данни, управлението на правата на потребителите, принципа на двоен контрол.

Въпроси, свързани с комуникацията: напр. между пазарни участници или в рамките на организацията.

Неправилни операции: например липса на обмен на сертификати, кеш паметта е пълна.

Неподходящо управление на промените: напр. неидентифицирани грешки в конфигурацията, разгръщане, включително актуализации, проблеми с

поддръжката, неочаквани грешки.

Неподходящи вътрешни процедури и документация: например липса на прозрачност по отношение на функционалностите, процесите и случаите на неправилно функциониране, липса на документация.

Въпроси, свързани с възстановяването: напр. управление на извънредни ситуации, неподходящи съкращения.

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

Неизправност на системата: причината за инцидента е свързана с неподходящото проектиране, изпълнение, компоненти, спецификации, интеграция или сложност на системите, мрежите, инфраструктурите и базите данни, които спомагат за извършването на платежната дейност. Те са разделени в следните категории:

Неизправност на хардуера: повреда на материално технологично оборудване, което управлява процесите и/или съхранява данните, необходими на доставчиците на платежни услуги, за да извършват дейността си, свързана с плащанията (напр. повреда на твърди дискове, центрове за данни, друга инфраструктура).

Повреда на мрежата: отказ на далекосъобщителни мрежи, публични или частни, които позволяват обмен на данни и информация (напр. чрез интернет) по време на процеса на плащане.

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

Неизправност на софтуера/приложенията: неизправности на програми, операционни системи и др., които поддържат предоставянето на платежни услуги от доставчика на платежни услуги (напр. неизправности, неизвестни функции).

Материални щети: напр. неумишлени щети, причинени от неподходящи условия, строителни работи.

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

Човешка грешка: инцидентът е причинен от непреднамерена грешка на дадено лице, било то 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). Те са разделени в следните категории:

Непредвидени: напр. грешки, пропуски, липса на опит и знания.

Бездействие: напр. поради липса на умения, знания, опит, осведоменост.

Недостатъчни ресурси: напр. липса на човешки ресурси, наличност на персонал.

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

Външно събитие: причината е свързана със събития, които обикновено са извън контрола на организацията. Те са разделени в следните категории:

Неизправност на доставчик/доставчик на техническа услуга: напр. прекъсване на електрозахранването, прекъсване на интернет, правни въпроси, бизнес въпроси, зависимости от услуги.

Непреодолима сила: напр. прекъсване на електрозахранването, пожари, природни явления като земетресения, наводнения, силни валежи, силен вятър.

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

Друго: причината за инцидента не е нито една от горепосочените. В полето за свободен

текст следва да се предостави допълнителна информация.

Друга информация от значение за първопричината: посочете допълнителни подробности относно първопричината, включително предварителните заключения, направени от анализа на първопричините.

Основни коригиращи 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 доставчика на платежни услуги?: 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, той е загубил лиценза си) в резултат на инцидента.

Оценка на ефективността на предприетите действия: включете, когато е възможно, самооценка на ефективността на действията, предприети по време на инцидента, включително всички поуки, извлечени от инцидента.