141

VYHLÁŠKA

ze dne 26. června 2018

o hlášení závažných bezpečnostních a provozních incidentů osobami oprávněnými poskytovat platební služby

(znění účinné od 1. ledna 2022)

Změna: vyhláška č. 485/2021 Sb.

Česká národní banka stanoví podle § 263 zákona č. 370/2017 Sb., o platebním styku, k provedení § 221 odst. 5:

§ 1

Předmět úpravy

Tato vyhláška stanoví podrobnosti náležitostí oznámení závažného bezpečnostního nebo provozního incidentu v oblasti platebního styku (dále jen "oznámení"), jeho formáty a další technické náležitosti při hlášení závažných bezpečnostních a provozních incidentů v oblasti platebního styku osobami oprávněnými poskytovat platební služby.

§ 2

Oznámení

Osoba oprávněná poskytovat platební služby předkládá České národní bance oznámení zahrnující v části

a) A úvodní oznámení,

b) B průběžné oznámení a

c) C závěrečné oznámení.

§ 3

Podrobnosti náležitostí oznámení

Osoba oprávněná poskytovat platební služby podává oznámení na formuláři, jehož vzor je uveden v příloze č. 1 k této vyhlášce, a postupně do něj doplňuje údaje do jednotlivých částí podle § 2.

§ 4

Formát a další technické náležitosti oznámení

(1) Oznámení se podává ve formátu xls/xlsx.

(2) Oznámení jsou České národní bance předávána prostřednictvím internetového rozhraní České národní banky pro sběr informačních povinností a výkazů.

(3) Oznámení lze učinit také v anglickém jazyce. Vzor formuláře v anglickém jazyce je uveden v příloze č. 2 k této vyhlášce

§ 5

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. srpna 2018.

Guvernér:

Ing. Rusnok v. r.

Příloha č. 1 k vyhlášce č. 141/2018 Sb.

Hlášení závažných bezpečnostních a provozních incidentů v oblasti platebního styku

(česká verze)

Oznámení o závažném incidentu

Úvodní oznámení

Resetovat výběry v rozbalovacích nabídkách

Datum oznámení *(DD/MM/RRRR)*		Čas *(HH:MM)*	
Referenční kód incidentu			

A - Úvodní oznámení

A 1 - OBECNÉ ÚDAJE

Druh oznámení						
Druh oznámení						
Dotčená osoba oprávněná poskytovat platební služby (OOPPS)						
Název OOPPS						
Vnitrostátní identifikační číslo OOPPS						
Vedoucí skupiny, připadá-li v úvahu						
Země dotčená / dotčené incidentem	☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ	☐ DE ☐ DK ☐ EE ☐ ES ☐ FI	☐ FR ☐ GR ☐ HR ☐ HU ☐ IE	☐ IS ☐ IT ☐ LI ☐ LT ☐ LU	☐ LV ☐ MT ☐ NL ☐ NO ☐ PL	☐ PT ☐ RO ☐ SE ☐ SI ☐ SK
Hlavní kontaktní osoba		E-mail		Telefon		
Další kontaktní osoba		E-mail		Telefon		
Oznamující subjekt (tento oddíl se vyplní v případě delegovaného oznamování, jestliže oznamujícím subjektem není dotčená osoba oprávněná poskytovat platební služby)						
Název oznamujícího subjektu						
Vnitrostátní identifikační číslo						
Hlavní kontaktní osoba		E-mail		Telefon		
Další kontaktní osoba		E-mail		Telefon		

A 2 - ZJIŠTĚNÍ INCIDENTU a PRVOTNÍ KLASIFIKACE

Datum a čas zjištění incidentu *(DD/MM/RRRR HH:MM)*			
Datum a čas klasifikace incidentu *(DD/MM/RRRR HH:MM)*			
Kdo incident zjistil		Je-li zvoleno „Jinak", upřesněte:	
Druh incidentu			
Kritéria vedoucí k oznámení o závažném incidentu	☐ Dotčené transakce ☐ Dotčení uživatelé platebních služeb ☐ Výpadek služby ☐ Narušení zabezpečení sítě nebo informačních systémů ☐ Ekonomický dopad ☐ Vysoká úroveň interní eskalace ☐ Ostatní potenciálně dotčené OOPPS nebo příslušné infrastruktury ☐ Reputační dopad		
Stručný a obecný popis incidentu			
Případný dopad v jiných členských státech EU			
Oznamování jiným orgánům		Je-li zvoleno „Ano", upřesněte:	
Důvody pro pozdní předložení úvodního oznámení			

Oznámení o závažném incidentu

Průběžné oznámení

Resetovat výběry v rozbalovacích nabídkách

Datum oznámení (DD/MM/RRRR)
Referenční kód incidentu
Čas *(HH:MM)*

B – Průběžné oznámení

B 1 – OBECNÉ ÚDAJE

Podrobnější popis incidentu:

V čem je konkrétně problém?			
Jak incident začal?			
Jak se vyvíjel?			
Jaké má důsledky (zejména pro uživatele platebních služeb)?			
Byli o incidentu informováni uživatelé platebních služeb?		Je-li zvoleno „Ano", upřesněte:	
Souvisí incident s předchozími incidenty?		Je-li zvoleno „Ano", upřesněte:	
Byli dotčeni nebo zapojeni další poskytovatelé služeb či třetí strany?		Je-li zvoleno „Ano", upřesněte:	
Bylo zahájeno krizové řízení (interní a/nebo externí)?		Je-li zvoleno „Ano", upřesněte:	
Datum a čas vzniku incidentu (je-li znám) *(DD/MM/RRRR HH:MM)*			
Datum a čas, kdy u incidentu došlo nebo podle očekávání dojde k návratu do původního stavu *(DD/MM/RRRR HH:MM)*			
Dotčené funkční oblasti	☐ Ověření/autorizace ☐ Přímé vypořádání ☐ Komunikace ☐ Nepřímé vypořádání ☐ Zúčtování ☐ Jiné	Je-li zvoleno „Jiné", upřesněte:	
Změny oproti předchozím oznámením			

B 2 – KLASIFIKACE INCIDENTU / INFORMACE O INCIDENTU

Dotčené transakce	Úroveň dopadu		
	Počet dotčených transakcí		Odhad
	Jako % z běžného počtu transakcí		
	Hodnota dotčených transakcí v eurech		
	Doba trvání incidentu (pouze pro provozní incidenty)		
	Poznámky:		
Dotčení uživatelé platebních služeb	Úroveň dopadu		
	Počet dotčených uživatelů platebních služeb		
	Jako % z celkového počtu uživatelů platebních služeb		
Narušení zabezpečení sítě nebo informačních systémů		Popište, jak byla dotčena síť nebo informační systémy	
Délka výpadku služby	Celková délka výpadku služby:	Dny: / Hodiny: / Minuty:	
Ekonomický dopad	Úroveň dopadu		
	Přímé náklady v eurech		
	Nepřímé náklady v eurech		
Vysoká úroveň interní eskalace	Ano	Popište úroveň interní eskalace incidentu a uveďte, zda incident vedl nebo pravděpodobně povede k vyhlášení krizového (nebo podobného) režimu, a pokud ano, popište jej	
Ostatní potenciálně dotčené OOPPS nebo příslušné infrastruktury		Popište, jak by se incident mohl dotknout jiných OOPPS a/nebo infrastruktur	
Reputační dopad		Popište, jak by incident mohl ovlivnit dobrou pověst OOPPS (např. mediální pokrytí, zveřejnění právních kroků nebo porušení právních předpisů…)	

B 3 – POPIS INCIDENTU

Druh incidentu		
Příčina incidentu	☐ Probíhá šetření ☐ Škodlivá činnost ☐ Selhání procesu ☐ Selhání systému ☐ Lidská chyba ☐ Externí události ☐ Jiné	Je-li zvoleno „Jiné", upřesněte:
Dotkl se vás incident přímo nebo prostřednictvím poskytovatele služeb?		Pokud „nepřímo", uveďte název poskytovatele služeb:

B 4 – DOPAD INCIDENTU

Celkový dopad	☐ Integrita ☐ Dostupnost	☐ Důvěrnost ☐ Autentičita	
Dotčené obchodní kanály	☐ Pobočky ☐ Elektronické bankovnictví ☐ Elektronické obchodování	☐ Telefonní bankovnictví ☐ Mobilní bankovnictví ☐ Bankomaty	☐ Místo prodeje ☐ Jiné
	Je-li zvoleno „Jiné", upřesněte:		
Dotčené platební služby	☐ Vložení hotovosti na platební účet ☐ Výběry hotovosti z platebního účtu ☐ Operace nutné k vedení platebního účtu ☐ Akceptace platebních prostředků	☐ Úhrady ☐ Inkaso ☐ Platby kartou ☐ Vydávání platebních prostředků	☐ Poukazování peněz ☐ Služby nepřímého dání platebního příkazu ☐ Služby informování o platebním účtu

B 5 – ZMÍRNĚNÍ INCIDENTU

Jaká opatření byla doposud přijata nebo jsou plánována s cílem dosáhnout obnovy po incidentu?	
Došlo k aktivaci plánu kontinuity činnosti a/nebo plánu obnovy provozu po havárii?	
Pokud ano, kdy? *(DD/MM/RRRR, HH:MM)*	
Pokud ano, popište je	

Oznámení o závažném incidentu

Zvolte druh oznámení:

Popište:
(pro incidenty, jejichž klasifikace byla změněna na „nezávažný")

Resetovat výběry v rozbalovacích nabídkách

Datum oznámení (DD/MM/RRRR)

Čas *(HH:MM)*

Referenční kód incidentu

C – Závěrečné oznámení

Nebylo-li žádné průběžné oznámení zasláno, vyplňte rovněž oddíl B.

C 1 – OBECNÉ ÚDAJE

Aktualizace informací z úvodního oznámení a průběžných oznámení	
Změny oproti předchozím oznámením	
Jakékoli další relevantní informace	
Jsou zavedena všechna původní opatření?	
Je-li zvoleno „Ne", uveďte, o které kontroly jde a jaký čas je zapotřebí k jejich obnovení	

C 2 – ANALÝZA HLAVNÍCH PŘÍČIN A NÁSLEDNÁ OPATŘENÍ

Co bylo hlavní příčinou (je-li již známa)?

☐ Škodlivá činnost ☐ Selhání procesu ☐ Selhání systému ☐ Lidská chyba ☐ Externí událost ☐ Jiné

Upřesněte:

Škodlivá činnost	Selhání procesu	Selhání systému	Lidská chyba	Externí událost
Škodlivý kód	Nedostatečné monitorování a kontrola	Selhání hardwaru	Neúmyslná činnost	Selhání dodavatele / poskytovatele technických služeb
Shromažďování informací	Problémy s komunikací	Selhání sítě	Nečinnost	Vyšší moc
Průniky	Nesprávné operace	Problémy s databází	Nedostatečné zdroje	Jiné
Útok (distribuovaným) odmítnutím služby (D/DoS)	Nedostatečné řízení změn	Selhání softwaru/aplikace	Jiné	
Úmyslná interní činnost	Nedostatečnost interních postupů a dokumentace	Fyzické poškození		
Úmyslné externí fyzické poškození	Problémy s obnovou	Jiné		
Zabezpečení informačního obsahu	Jiné			
Podvodná jednání				
Jiné				

Je-li zvoleno „Jiné", upřesněte:

Další relevantní informace o hlavní příčině	
Hlavní nápravná opatření přijatá nebo plánovaná s cílem zabránit opakování incidentu v budoucnu, pokud jsou již tato opatření známa	

C 3 – DOPLŇUJÍCÍ INFORMACE

Byly o incidentu informovány další OOPPS?	Je-li zvoleno „Ano", uveďte podrobnosti:
Byly proti oznamující osobě učiněny nějaké právní kroky?	Je-li zvoleno „Ano", uveďte podrobnosti:
Posouzení účinnosti přijatých opatření	Uveďte podrobnosti:

Příloha č. 2 k vyhlášce č. 141/2018 Sb.

Reporting template on major incidents

(anglická verze)

Major Incident Report					
Initial report				Reset dropdown selections	
Report date *(DD/MM/YYYY)*		Time *(HH:MM)*			
Incident reference code					

A - Initial report					
A 1 - GENERAL DETAILS					
Type of report					
Type of report					
Affected payment service provider (PSP)					
PSP name					
PSP national identification number					
Head of group, if applicable					
Country / countries affected by the incident	☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ	☐ DE ☐ DK ☐ EE ☐ ES ☐ FI	☐ FR ☐ GR ☐ HR ☐ HU ☐ IE	☐ IS ☐ IT ☐ LI ☐ LT ☐ LU	☐ LV ☐ MT ☐ NL ☐ NO ☐ PL	☐ PT ☐ RO ☐ SE ☐ SI ☐ SK
Primary contact person		E-mail		Telephone	
Secondary contact person		E-mail		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					
National identification number					
Primary contact person		E-mail		Telephone	
Secondary contact person		E-mail		Telephone	
A 2 - INCIDENT DETECTION and CLASSIFICATION					
Date and time of detection of the incident *(DD/MM/YYYY HH:MM)*					
Date and time of classification of the incident *(DD/MM/YYYY HH:MM)*					
The incident was detected by		If 'Other', please specify:			
Type of Incident					
Criteria triggering the major incident report	☐ Transactions affected ☐ Payment service users affected ☐ Service downtime ☐ Breach of security of network or information systems ☐ Economic impact ☐ High level of internal escalation ☐ Other PSPs or relevant infrastructures potentially affected ☐ Reputational impact				
A short and general description of the incident					
Impact in other EU Member States, if applicable					
Reporting to other authorities		If 'Yes', please specify:			
Reasons for late submission of the initial report					

Major Incident Report

Intermediate report

Reset dropdown selections

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

Incident reference code:

B - Intermediate report

B 1 - GENERAL DETAILS

More detailed description of the incident:

What is the specific issue?	
How did the incident start?	
How did it evolve?	
What are the consequences (in particular for payment service users)?	
Was the incident communicated to payment service users?	If 'Yes', please specify:
Was it related to a previous incident/s?	If 'Yes', please specify:
Were other service providers/third parties affected or involved?	If 'Yes', please specify:
Was crisis management started (internal and/or external)?	If 'Yes', please specify:
Date and time of beginning of the incident (if already identified) *(DD/MM/YYYY HH:MM)*	
Date and time when the incident was restored or is expected to be restored *(DD/MM/YYYY HH:MM)*	
Functional areas affected	☐ Authentication/Authorisation ☐ Direct settlement ☐ Communication ☐ Indirect settlement ☐ Clearing ☐ Other — If 'Other', please specify:
Changes made to previous reports	

B 2 - INCIDENT CLASSIFICATION / INFORMATION ON THE INCIDENT

Transactions affected [2]	Impact level; Number of transactions affected; As a % of regular number of transactions; Value of transactions affected in EUR; Duration of the incident (only applicable to operational incidents); Comments:
Payment service users affected [3]	Impact level; Number of payment service users affected; As a % of total payment service users
Breach of security of network or information systems	Describe how the network or information systems have been affected
Service downtime	Total service downtime: Days: Hours: Minutes:
Economic impact	Impact level; Direct costs in EUR; Indirect costs in EUR
High level of internal escalation	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	Describe how this incident could affect other PSPs and/or infrastructures
Reputational impact	Describe how the incident could affect the reputation of the PSP (e.g. media coverage, publication of legal actions or infringements of law...)

B 3 - INCIDENT DESCRIPTION

Type of Incident	
Cause of incident	☐ Under investigation ☐ Malicious action ☐ Process failure ☐ System failure ☐ Human errors ☐ External events ☐ Other — If 'Other', please specify:
Was the incident affecting you directly, or indirectly through a service provider?	If 'Indirectly', please provide the service provider's name:

B 4 - INCIDENT IMPACT

Overall impact	☐ Integrity ☐ Availability ☐ Confidentiality ☐ Authenticity
Commercial channels affected	☐ Branches ☐ E-banking ☐ E-commerce ☐ Telephone banking ☐ Mobile banking ☐ ATMs ☐ Point of sale ☐ Other; If 'Other', please specify:
Payment services affected	☐ Cash placement on a payment account ☐ Cash withdrawal from a payment account ☐ Operations required for operating a payment account ☐ Acquiring of payment instruments ☐ Credit transfers ☐ Direct debits ☐ Card payments ☐ Issuing of payment instruments ☐ Money remittance ☐ Payment initiation ☐ Account information services

B 5 - INCIDENT MITIGATION

Which actions/measures have been taken so far or are planned to recover from the incident?	
Have the Business Continuity Plan and/or Disaster Recovery Plan been activated?	
If so, when? *(DD/MM/YYYY HH:MM)*	
If so, please describe	

Major Incident Report

Please select the type of report:

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

Reset dropdown selections

Report date *(DD/MM/YYYY)*
Incident reference code

Time *(HH:MM)*

C - Final report

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

C 1 - GENERAL DETAILS

Update of the information from the initial report and the intermediate report(s)

Changes made to previous reports	
Any other relevant information	
Are all original controls in place?	
If "No", specify which controls and the additional period required for their restoration	

C 2 - ROOT CAUSE ANALYSIS AND FOLLOW UP

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

C 3 - ADDITIONAL INFORMATON

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