

NÁVRH VYHLÁŠKA

ze dne 2021,

kteřou se mění vyhláška č. 141/2018 Sb., o hlášení závažných bezpečnostních a provozních incidentů osobami oprávněnými poskytovat platební služby

Česká národní banka stanoví podle § 263 zákona č. 370/2017 Sb., o platebním styku, ve znění zákona č. 298/2021 Sb., (dále jen „zákon“) k provedení § 221 odst. 5 zákona:

Čl. I

Vyhláška č. 141/2018 Sb., o hlášení závažných bezpečnostních a provozních incidentů osobami oprávněnými poskytovat platební služby se mění takto:

1. Příloha č. 1 zní:

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

Hlášení závažných bezpečnostních a provozních incidentů v oblasti platebního styku

(česká verze uvedeného dokumentu)

Oznámení o závažném incidentu						
Úvodní oznámení		do 4 hodin od klasifikace incidentu jako závažného			Resetovat výběry v rozbalovacích nabídkách	
Datum oznámení (DDMMRRRR)		Referenční kód incidentu			Čas (HHMM)	
A - Úvodní oznámení						
A 1 - OBECNÉ ÚDAJE						
Druh oznámení						
Dotčená osoba oprávněná poskytovat platební služby (OOPPS)						
Název OOPPS						
Vnitrostátní identifikační číslo OOPPS						
Vedoucí skupiny, případně v úvahu						
Země dotčená / dotčené incidentem						
<input type="checkbox"/> AT <input type="checkbox"/> DE <input type="checkbox"/> FR <input type="checkbox"/> IS <input type="checkbox"/> LV <input type="checkbox"/> PT <input type="checkbox"/> BE <input type="checkbox"/> DK <input type="checkbox"/> GR <input type="checkbox"/> IT <input type="checkbox"/> MT <input type="checkbox"/> RO <input type="checkbox"/> BG <input type="checkbox"/> EE <input type="checkbox"/> HR <input type="checkbox"/> LI <input type="checkbox"/> NL <input type="checkbox"/> SE <input type="checkbox"/> CY <input type="checkbox"/> ES <input type="checkbox"/> HU <input type="checkbox"/> LT <input type="checkbox"/> NO <input type="checkbox"/> SI <input type="checkbox"/> CZ <input type="checkbox"/> FI <input type="checkbox"/> IE <input type="checkbox"/> LU <input type="checkbox"/> PL <input type="checkbox"/> SK						
Hlavní kontaktní osoba		Email		Telefon		
Další kontaktní osoba		Email		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		Email		Telefon		
Další kontaktní osoba		Email		Telefon		
A 2 - ZJIŠTĚNÍ INCIDENTU A PRVOTNÍ KLASIFIKACE						
Datum a čas zjištění incidentu (DDMMRRRR HH:MM)						
Datum a čas klasifikace incidentu (DDMMRRRR HH:MM)						
Kdo incident zjistil						
Druh incidentu						
Kritéria vedoucí k oznámení o závažném incidentu						
<input type="checkbox"/> Dotčená transakce <input type="checkbox"/> Dotčení uživatelů platebních služeb <input type="checkbox"/> Výpadek služby <input type="checkbox"/> Narušení zabezpečení síťového nebo informačního systému <input type="checkbox"/> Ekonomický dopad <input type="checkbox"/> Výsoká úroveň intenzity eskalace <input type="checkbox"/> Ostatní potenciálně dotčené OOPPS nebo příslušné infrastruktury <input type="checkbox"/> 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

maximálně 3 pracovní dny od předložení úvodního 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) (DDMMRRRR HH:MM)

Datum a čas, kdy u incidentu došlo nebo podle očekávání dojde k návratu do původního stavu (DDMMRRRR 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 ⁽²⁾

Úroveň dopadu:
 Počet dotčených transakcí:
 Jako % z běžného počtu transakcí:
 Hodnota dotčených transakcí v eurech:
 Doba trvání incidentu (pouze pro provozní incidenty):
 Poznámky:

Dotčení uživatelé platebních služeb ⁽³⁾

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

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
 Lidské chyby
 Externí události
 Jiné

Je-li zvoleno „Jiné“, upřesněte:

Dotkl se váš incident přímo nebo prostřednictvím poskytovatele služeb?

Pokud „nepřímě“, uveďte název poskytovatele služeb:

B 4 – DOPAD INCIDENTU

Celkový dopad

- Integrita Důvěrnost
 Dostupnost Autentikita

Dotčené obchodní kanály

- Pobočky Telefonní bankovnídvi
 Elektronické bankovnídvi Mobilní bankovnídvi
 Elektronické obchodování Bankomaty
 Místo prodeje
 Jiné

Je-li zvoleno „Jiné“, upřesněte:

Dotčené platební služby

- Vložení hotovosti na platební účet Úhrady Poukazování peněz
 Výběry hotovosti z platebního účtu Inkaso Služby nepřímého dání platebního příkazu
 Operace nutné k vedení platebního účtu Platby kartou Služby informování o platebním účtu
 Akceptace platebních prostředků Vydávání platebních prostředků

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? (DDMMRRRR, HH:MM)

Pokud ano, popište je

Oznámení o závažném incidentu	
Zvolte druh oznámení: <input type="text"/>	maximálně devět pracovních dnů od předložení průběžného oznámení
(pro incidenty, jejichž klasifikace byla změněna na „nezávažný“)	Popište: <input type="text"/>
Resetovat výběry v rozbalovacích nabídkách	
Datum oznámení (DD/MM/RRRR) <input type="text"/>	Čas (HH:MM) <input type="text"/>
Referenční kód incidentu <input type="text"/>	

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?	<input type="text"/>
Je-li zvoleno „Ne“, uveďte, o která opatření jde a jaký čas je zapotřebí k jejich obnově	
C 2 – ANALÝZA HLAVNÍCH PŘÍČIN A NÁSLEDNÁ OPATŘENÍ	
Co bylo hlavní příčinou (je-li již známa)?	<input type="checkbox"/> Škodlivá činnost <input type="checkbox"/> Selhání procesu <input type="checkbox"/> Selhání systému <input type="checkbox"/> Lidská chyba <input type="checkbox"/> Externí událost <input type="checkbox"/> Jiné
Upřesněte:	<div style="display: flex; flex-wrap: wrap;"> <div style="width: 33%;"> <input type="checkbox"/> Škodlivý kód <input type="checkbox"/> Shromáždění informací <input type="checkbox"/> Průniky <input type="checkbox"/> Útok (distribuoivaní) odmítnutím služby (D/Dos) <input type="checkbox"/> Úmyslná interní činnost <input type="checkbox"/> Úmyslné externí fyzické poškození <input type="checkbox"/> Zabezpečení informačního obsahu <input type="checkbox"/> Podvodná jednání <input type="checkbox"/> Jiné Je-li zvoleno „jiné“, upřesněte: </div> <div style="width: 33%;"> <input type="checkbox"/> Nedostatečné monitorování a kontrola <input type="checkbox"/> Problémy s komunikací <input type="checkbox"/> Nesprávné operace <input type="checkbox"/> Nedostatečné řízení změn <input type="checkbox"/> Nedostatečnost interních postupů a dokumentace <input type="checkbox"/> Problémy s obnovou <input type="checkbox"/> Jiné </div> <div style="width: 33%;"> <input type="checkbox"/> Selhání hardwaru <input type="checkbox"/> Selhání sítě <input type="checkbox"/> Problémy s databází <input type="checkbox"/> Selhání softwaru/aplikace <input type="checkbox"/> Fyzické poškození <input type="checkbox"/> Jiné </div> <div style="width: 33%;"> <input type="checkbox"/> Neúmyslná činnost <input type="checkbox"/> Nečinnost <input type="checkbox"/> Nedostatečné zdroje <input type="checkbox"/> Jiné </div> <div style="width: 33%;"> <input type="checkbox"/> Selhání dodavatele / poskytovatele technických služeb <input type="checkbox"/> Vyšší moc <input type="checkbox"/> Jiné </div> </div>
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?	<input type="text"/>
Je-li zvoleno „Ano“, uveďte podrobnosti:	
Byly proti oznamující osobě učiněny nějaké právní kroky?	<input type="text"/>
Je-li zvoleno „Ano“, uveďte podrobnosti:	
Posouzení účinnosti přijatých opatření	<input type="text"/>
Uveďte podrobnosti:	

2. Příloha č. 2 zní:

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

Reporting template on major incidents

(anglická verze uvedeného dokumentu)

Major Incident Report	
Initial report	within 4 hours after classification of the incident as major
Report date (DDMMYYYY) <input type="text"/>	Time (HH:MM) <input type="text"/>
Incident reference code <input type="text"/>	
Reset dropdown selections	
A - Initial report	
A 1 - GENERAL DETAILS	
Type of report	<input type="text"/>
Affected payment service provider (PSP)	
PSP name	
PSP national identification number	
Head of group, if applicable	
Country / countries affected by the incident	<input type="checkbox"/> AT <input type="checkbox"/> DE <input type="checkbox"/> FR <input type="checkbox"/> IS <input type="checkbox"/> LV <input type="checkbox"/> PT <input type="checkbox"/> BE <input type="checkbox"/> DK <input type="checkbox"/> GR <input type="checkbox"/> IT <input type="checkbox"/> MT <input type="checkbox"/> RO <input type="checkbox"/> BG <input type="checkbox"/> ES <input type="checkbox"/> HR <input type="checkbox"/> LI <input type="checkbox"/> NL <input type="checkbox"/> SE <input type="checkbox"/> CY <input type="checkbox"/> IE <input type="checkbox"/> HU <input type="checkbox"/> LT <input type="checkbox"/> NO <input type="checkbox"/> SI <input type="checkbox"/> CZ <input type="checkbox"/> FI <input type="checkbox"/> IE <input type="checkbox"/> LU <input type="checkbox"/> PL <input type="checkbox"/> SK
Primary contact person	Email <input type="text"/>
Secondary contact person	Email <input type="text"/>
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	Email <input type="text"/>
Secondary contact person	Email <input type="text"/>
A 2 - INCIDENT DETECTION and CLASSIFICATION	
Date and time of detection of the incident (DDMMYYYYHH:MM)	
Date and time of classification of the incident (DDMMYYYYHH:MM)	
The incident was detected by	<input type="text"/> If 'Other', please specify: <input type="text"/>
Type of incident	<input type="text"/>
Criteria triggering the major incident report	<input type="checkbox"/> Transactions affected <input type="checkbox"/> Payment service users affected <input type="checkbox"/> Service downtime <input type="checkbox"/> Breach of security of network or information systems <input type="checkbox"/> Economic impact <input type="checkbox"/> High level of internal escalation <input type="checkbox"/> Other PSPs or relevant infrastructures potentially affected <input type="checkbox"/> Reputational impact
A short and general description of the incident	
Impact in other EU Member States, if applicable	
Reporting to other authorities	<input type="text"/> If 'Yes', please specify: <input type="text"/>
Reasons for late submission of the initial report	

Major Incident Report

Intermediate report	maximum of 3 working days from the submission of the initial report	Reset dropdown selections
Report date (DDMMYYYY)	Incident reference code	Time (HHMM)

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?	<input type="checkbox"/> Yes <input type="checkbox"/> No If 'Yes', please specify:
Was it related to a previous incident/s?	<input type="checkbox"/> Yes <input type="checkbox"/> No If 'Yes', please specify:
Were other service providers/third parties affected or involved?	<input type="checkbox"/> Yes <input type="checkbox"/> No If 'Yes', please specify:
Was crisis management started (internal and/or external)?	<input type="checkbox"/> Yes <input type="checkbox"/> No If 'Yes', please specify:
Date and time of beginning of the incident (if already identified) (DDMMYYYY HH:MM)	
Date and time when the incident was restored or is expected to be restored (DDMMYYYY HH:MM)	
Functional areas affected	<input type="checkbox"/> Authentication/authorisation <input type="checkbox"/> Direct settlement <input type="checkbox"/> Communication <input type="checkbox"/> Indirect settlement <input type="checkbox"/> Clearing <input type="checkbox"/> 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
Breach of security of network or information systems	As a % of total payment service users
	Describe how the network or information systems have been affected
Service downtime	Total service downtime: Days: <input type="text"/> Hours: <input type="text"/> Minutes: <input type="text"/>
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	<input type="checkbox"/> Under investigation
Cause of incident	<input type="checkbox"/> Malicious action
	<input type="checkbox"/> Process failure
	<input type="checkbox"/> System failure
	<input type="checkbox"/> Human errors
	<input type="checkbox"/> External events
	<input type="checkbox"/> Other If 'Other', please specify:
Was the incident affecting you directly, or indirectly through a service provider?	<input type="checkbox"/> Directly <input type="checkbox"/> Indirectly If 'Indirectly', please provide the service provider's name:
B 4 - INCIDENT IMPACT	
Overall impact	<input type="checkbox"/> Integrity <input type="checkbox"/> Confidentiality <input type="checkbox"/> Availability <input type="checkbox"/> Authenticity
Commercial channels affected	<input type="checkbox"/> Branches <input type="checkbox"/> Telephone banking <input type="checkbox"/> Point of sale <input type="checkbox"/> E-banking <input type="checkbox"/> Mobile banking <input type="checkbox"/> Other <input type="checkbox"/> E-commerce <input type="checkbox"/> ATMs
	If 'Other', please specify:
	<input type="checkbox"/> Cash placement on a payment account <input type="checkbox"/> Credit transfers <input type="checkbox"/> Money remittance <input type="checkbox"/> Cash withdrawal from a payment account <input type="checkbox"/> Direct debits <input type="checkbox"/> Payment initiation <input type="checkbox"/> Operations required for operating a payment account <input type="checkbox"/> Card payments <input type="checkbox"/> Account information services <input type="checkbox"/> Acquiring of payment instruments <input type="checkbox"/> Issuing of payment instruments
B 5 - INCIDENT MITIGATION	
Which actions/measurements 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?	<input type="checkbox"/> Yes <input type="checkbox"/> No
If so, when? (DDMMYYYY HH:MM)	
If so, please describe	

Major Incident Report

Please select the type of report: <input style="width: 100%;" type="text"/> within 20 working days after the submission of the intermediate report Please describe: <input style="width: 100%;" type="text"/> (applicable for incidents reclassified as non-major)	<div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 0 auto;"> Reset dropdown selections </div>
Report date (DDMMYYYY) <input style="width: 150px;" type="text"/> Time (HH:MM) <input style="width: 100px;" type="text"/>	Incident reference code <input style="width: 150px;" type="text"/>

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	<input style="width: 100%;" type="text"/>
Any other relevant information	<input style="width: 100%;" type="text"/>
Are all original controls in place?	<input style="width: 100%;" type="text"/>
If "No", specify which controls and the additional period required for their restoration	<input style="width: 100%;" type="text"/>
C 2 - ROOT CAUSE ANALYSIS AND FOLLOW UP	
What was the root cause (if already known)?	<input type="checkbox"/> Malicious action <input type="checkbox"/> Process failure <input type="checkbox"/> System failure <input type="checkbox"/> Human error <input type="checkbox"/> External event <input type="checkbox"/> Other
Please specify:	<div style="display: flex; flex-wrap: wrap; padding: 5px;"> <div style="width: 25%;"><input type="checkbox"/> Malicious code</div> <div style="width: 25%;"><input type="checkbox"/> Deficient monitoring and control</div> <div style="width: 25%;"><input type="checkbox"/> Hardware failure</div> <div style="width: 25%;"><input type="checkbox"/> Unintended</div> <div style="width: 25%;"><input type="checkbox"/> Failure of a supplier/technical service provider</div> <div style="width: 25%;"><input type="checkbox"/> Information gathering</div> <div style="width: 25%;"><input type="checkbox"/> Communication issues</div> <div style="width: 25%;"><input type="checkbox"/> Network failure</div> <div style="width: 25%;"><input type="checkbox"/> Inaction</div> <div style="width: 25%;"><input type="checkbox"/> Insufficient resources</div> <div style="width: 25%;"><input type="checkbox"/> Force majeure</div> <div style="width: 25%;"><input type="checkbox"/> Intrusions</div> <div style="width: 25%;"><input type="checkbox"/> Improper operations</div> <div style="width: 25%;"><input type="checkbox"/> Database issues</div> <div style="width: 25%;"><input type="checkbox"/> Other</div> <div style="width: 25%;"><input type="checkbox"/> Distributed/Denial of service attack (D/DoS)</div> <div style="width: 25%;"><input type="checkbox"/> Inadequate Change management</div> <div style="width: 25%;"><input type="checkbox"/> Software/application failure</div> <div style="width: 25%;"><input type="checkbox"/> Physical damage</div> <div style="width: 25%;"><input type="checkbox"/> Other</div> <div style="width: 25%;"><input type="checkbox"/> Deliberate internal actions</div> <div style="width: 25%;"><input type="checkbox"/> Inadequacy of internal procedures and documentation</div> <div style="width: 25%;"><input type="checkbox"/> Recovery issues</div> <div style="width: 25%;"><input type="checkbox"/> Other</div> <div style="width: 25%;"><input type="checkbox"/> Deliberate external physical damage</div> <div style="width: 25%;"><input type="checkbox"/> Fraudulent actions</div> <div style="width: 25%;"><input type="checkbox"/> Other</div> </div>
Other relevant information on the root cause	<input style="width: 100%;" type="text"/>
Main corrective actions/measure taken or planned to prevent the incident from happening again in the future, if already known	<input style="width: 100%;" type="text"/>
C 3 - ADDITIONAL INFORMATION	
Has the incident been shared with other PSPs for information purposes?	<input style="width: 100%;" type="text"/>
Has any legal action been taken against the PSP?	<input style="width: 100%;" type="text"/>
Assessment of the effectiveness of the action taken	<input style="width: 100%;" type="text"/>

Čl. II

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. ledna 2022.

Guvernér: