

DATUM: 14. 12. 2020

Dohledové sdělení č. 1/2020

K povinnosti poskytovatelů platebních služeb promítnout požadavky na silné ověření uživatele do informací poskytovaných klientům a smluvní dokumentace

V souvislosti s implementací požadavků právních předpisů na silné ověření uživatele (viz § 223 a násl. zákona č. 370/2017 Sb., o platebním styku, ve znění pozdějších předpisů (dále jen „ZoPS“)) je třeba zabývat se otázkou, **zda a případně jakým způsobem by poskytovatelé platebních služeb měli v předmluvních informacích a smluvní dokumentaci uzavírané s uživateli zohlednit skutečnost, že je používáno silné ověření uživatele.**

Česká národní banka uvádí, že poskytovatel platebních služeb má povinnost zajistit, aby před uzavřením rámcové smlouvy o platebních službách byly uživateli poskytnuty v souladu s § 135 písm. c) ZoPS **informace o formě a postupu při udělení souhlasu s provedením platební transakce.**¹ S ohledem na nutnost prokázat splnění této povinnosti poskytovatelem platebních služeb, měla by být dohoda o formě a postupu při udělení souhlasu s platební transakcí součástí smluvních ujednání s klienty. Součástí informace/ujednání by měla být i dohoda o autorizaci platebního příkazu prostřednictvím osobních bezpečnostních prvků či přepisem jednorázových kódů, jsou-li k autorizaci použity.

Ustanovení § 139 písm. a) bodu 1 ZoPS stanoví, že uživateli musí být v případě, že byl uživateli vydán platební prostředek, v souladu s § 133 odst. 1 poskytnut **popis opatření, která musí uživatel přijmout na ochranu jeho osobních bezpečnostních prvků, a informace o způsobu, jímž má uživatel oznámit ztrátu, odcizení, zneužití nebo neoprávněné použití platebního prostředku.**

Česká národní banka níže specifikuje **minimum** informací, které by poskytovatelé platebních služeb měli zohlednit s uživateli při on-line autorizaci platebních příkazů.

A. Za účelem dosažení souladu s § 135 písm. c) ZoPS je třeba zohlednit následující skutečnosti:

¹ Obdobně se postupuje i v případě smlouvy o jednorázové platební transakci (viz § 132 odst. 2 písm. e) ZoPS).

1. bezpečnostní prvky uživatele: ujednání o tom, co tvoří osobní bezpečnostní prvky uživatele, kterými uživatel dává souhlas s platební transakcí a s pomocí kterých poskytovatel platebních služeb uživatele ověřuje;
2. dvoufaktorové (nebo vícefaktorové) ověření: ujednání o tom, že v rámci ověření uživatele poskytovatel platebních služeb zpravidla ověřuje uživatele prostřednictvím (kombinace) dvou prvků z různých kategorií (pokud nejsou splněny podmínky pro některou z výjimek předpokládaných právními předpisy);
3. postup uživatele při udělení souhlasu s transakcí: ujednání o postupu uživatele při udělení souhlasu s platební transakcí tak, aby byla transakce považována za autorizovanou (např. udělení souhlasu zadáním jednorázového kódu a/či PINU/ otiskem prstu, apod.).

B. Za účelem dosažení souladu s § 139 písm. a) bodu 1 ZoPS je třeba zohlednit následující skutečnosti:

4. opatření přijatá uživatelem na ochranu bezpečnostních prvků: ujednání o opatřeních, která musí uživatel přijmout na ochranu svých osobních bezpečnostních prvků;
5. možnosti, jak oznámit ztrátu, odcizení, zneužití či neoprávněné použití platebního prostředku sloužícího k silnému ověření uživatele: ujednání o tom, kam, v jakých lhůtách a jakým způsobem má uživatel postupovat v případě ztráty, odcizení, zneužití či neoprávněného použití platebního prostředku (např. mobilního telefonu s uloženou platební kartou či nainstalovanou platební aplikací).

V případě, že uvedené skutečnosti nebudou uživateli poskytnuty a nebudou s nimi dohodnuty, **nebudou poskytovatelem platebních služeb řádně splněny povinnosti** dle § 135 písm. c) a § 139 písm. a) bodu 1 ZoPS. Absence smluvního ujednání ohledně náležitostí formy a postupu při udělení souhlasu dle § 135 písm. c) ZoPS může mít rovněž dopad na posouzení, zda byla platební transakce řádně autorizována. Absence smluvního ujednání ohledně opatření na ochranu osobních bezpečnostních prvků a způsobu oznámení ztráty, odcizení, zneužití nebo neoprávněného použití platebního prostředku dle § 139 písm. a) bodu 1 ZoPS může mít rovněž dopad na odpovědnost poskytovatele za neautorizovanou platební transakci tak, že se poskytovatel nebude moci dovolávat odpovědnosti plátce dle § 182 odst. 1 písm. b) ZPS.

Obdobně lze doporučit, aby si poskytovatelé platebních služeb upravili ve smluvní dokumentaci **své právo transakci neprovést** (resp. odmítnout v souladu s § 159 ZoPS) v případě, že do jejich dispozice přijde pokyn k provedení platebního příkazu, u kterého předchozí subjekty podílející se na zpracování transakce neumožnily provedení silného ověření uživatele. Typicky půjde o platební příkaz, kdy bude poskytovatel platebních služeb vystupovat v roli vydavatele karty u karetní

platební transakce a platební příkaz nebyl ověřen předchozími subjekty účastnicími se na této transakci, ačkoliv být ověřen měl/mohl.

Ačkoliv oblast ochrany osobních údajů nespadá do působnosti České národní banky, ta přesto doporučuje poskytovatelům platebních služeb, aby zajistili při nakládání s osobními údaji uživatelů při autorizaci platebních transakcí s využitím jejich osobních bezpečnostních prvků soulad s právními předpisy na ochranu osobních údajů. Uživatelé by měli být minimálně poučeni o rozsahu zpracovávaných dat, účelu jejich zpracování a době, po kterou budou tyto údaje zpracovány a v případě, že pro zpracování údajů je nutný souhlas klienta, je nutné rovněž tento souhlas získat.