EVROPSKÁ KOMISE

GENERÁLNÍ ŘEDITELSTVÍ PRO HOSPODÁŘSKOU SOUTĚŽ

Revidováno v březnu 2024

Vysvětlivky ke kontrolám Komise podle čl. 20 odst. 4 nařízení Rady (ES) č. 1/2003

Tyto vysvětlivky jsou pouze informativní a není jimi nijak dotčen formální výklad vyšetřovacích pravomocí Evropské komise.

1) Na podniky ([1]) se vztahuje právní závazek podrobit se kontrole nařízené rozhodnutím Komise podle čl. 20 odst. 4 nařízení Rady (ES) č. 1/2003. Písemná zmocnění slouží k uvedení jmen úředníků a ostatních doprovázejících osob zmocněných Komisí ke kontrole (dále jen „kontroloři“). Každý kontrolor se prokáže dokladem totožnosti.

2) Po kontrolorech nelze požadovat, aby předmět kontroly uvedený v rozhodnutí blíže vysvětlovali nebo dané rozhodnutí jakkoli odůvodňovali. Mohou však vysvětlit procesní záležitosti, například pokud jde o důvěrnost nebo osobní údaje, jakož i možné důsledky odmítnutí podřídit se kontrole.

3) Podniku bude předána ověřená kopie rozhodnutí. Zápis o oznámení rozhodnutí slouží pouze jako potvrzení doručení a jeho podpis příjemcem neznamená, že podnik souhlasí s provedením kontroly.

4) Kontroloři jsou podle čl. 20 odst. 2 nařízení (ES) č. 1/2003 zmocněni:

   a) vstupovat do všech prostor, na pozemky a do dopravních prostředků podniků;

   b) kontrolovat účetní knihy a ostatní obchodní záznamy, bez ohledu na to, v jaké formě jsou uloženy;

   c) kopírovat nebo získávat v jakékoli formě kopie nebo výpisy z těchto knih nebo záznamů;

   d) pečetit kterékoli podnikatelské prostory a účetní knihy nebo záznamy po dobu a v rozsahu, které jsou nezbytné pro kontrolu;

   e) žádat kteréhokoli zástupce nebo zaměstnance podniku o vysvětlení skutečností nebo dokumentů týkajících se předmětu kontroly a zaznamenávat odpovědi.

5) Úředníci a ostatní doprovázející osoby zmocněné nebo jmenované orgánem pro hospodářskou soutěž členského státu, na jehož území se kontrola provádí, jsou oprávněni kontrolorům při plnění jejich úkolů aktivně pomáhat. Za tímto účelem mají podle čl. 20 odst. 2 nařízení (ES) č. 1/2003 stejné pravomoci jako kontroloři (viz bod 4 výše).

([1]) Pojem „podnik“ v těchto vysvětlivkách zahrnuje podniky i sdružení podniků.

6) Podnik **se může** během kontroly **poradit s externím právním zástupcem**. Přítomnost takového právního zástupce na kontrolovaném místě však není podmínkou legality kontroly. Kontroloři mohou vstoupit do prostorů, oznámit rozhodnutí, kterým se nařizuje kontrola, a zdržovat se v kancelářích dle vlastního výběru, aniž by čekali na to, až se podnik poradí se svým právním zástupcem. Kontroloři pro účel porady s právním zástupcem v každém případě akceptují pouze krátký odklad před tím, než začnou kontrolovat účetní knihy a ostatní obchodní záznamy, pořizovat kopie nebo výpisy z těchto dokumentů a v případě potřeby pečetit podnikatelské prostory a účetní knihy nebo záznamy, nebo žádat o ústní vysvětlení. Jakýkoli takový odklad musí být omezen na nezbytné minimum.

7) Pokud některý zástupce nebo zaměstnanec podniku poskytne na místě podle čl. 4 odst. 1 nařízení Komise (ES) č. 773/2004 na žádost kontrolorů **ústní vysvětlení** ohledně skutečností nebo dokumentů týkajících se předmětu kontroly, mohou být tato vysvětlení zaznamenána jakoukoli formou. Kopie takovýchto záznamů se dotčenému podniku předá po kontrole podle čl. 4 odst. 2 nařízení (ES) č. 773/2004.

8) V případech, kdy byl o vysvětlení požádán zaměstnanec podniku, který k podání vysvětlení jménem podniku není nebo nebyl podnikem oprávněn, stanoví Komise lhůtu, v níž může podnik sdělit Komisi jakoukoli opravu či změnu vysvětlení poskytnutého tímto zaměstnancem nebo dodatek k takovému vysvětlení, které budou následně přidány k vysvětlením zaznamenaným během kontroly.

9) Kontroloři jsou oprávněni kontrolovat jakékoli účetní knihy a obchodní záznamy bez ohledu na to, v jaké formě jsou uloženy, a pořizovat nebo získávat v jakékoli formě kopie nebo výpisy z těchto knih nebo záznamů. Mohou mimo jiné provádět přezkum informací v elektronické podobě a pořizovat jejich elektronické nebo papírové kopie. Zástupci podniku jsou oprávněni sledovat opatření přijatá kontrolory, aniž by zasahovali do jejich práce.

10) Kontroloři mohou prohledávat prostředí IT (např. cloudové služby, servery, stolní počítače, notebooky, tablety a jiná mobilní zařízení) a veškerá paměťová média (např. externí úložná zařízení, zálohovací pásky, klíče USB, CD-ROMy, DVD) daného podniku. To se týká rovněž soukromých zařízení a médií používaných pro pracovní účely (systém „přines si vlastní zařízení“ (Bring Your Own Device, BYOD)), pokud jsou v daných prostorách nalezena. Za tímto účelem mohou kontroloři používat jakékoli integrované systémové funkce v informačních systémech a infrastruktuře podniku. Mohou rovněž využívat svůj vlastní specializovaný software a/nebo hardware („forenzní nástroje IT“). Tyto forenzní nástroje IT umožňují Komisi v souladu s čl. 20 odst. 2 písm. b) nařízení (ES) č. 1/2003 kontrolovat systémy a data podniku, zejména vytvářením hodnověrných duplikátů dat, včetně obnovených dat, a prohledávat takové duplikáty a současně respektovat integritu systémů a dat podniku.

11) Podnik je povinen plně a aktivně spolupracovat s kontrolory. To znamená, že od podniku může být požadováno, aby dal k dispozici zástupce nebo zaměstnance, kteří kontrolorům poskytnou účinnou pomoc. To zahrnuje nejen povinnost podat vysvětlení ohledně organizace podniku a jeho prostředí IT, ale také plnit konkrétní úkoly, jako je provádění zvláštních příkazů v systémech IT za účelem shromažďování informací, využívání integrovaných funkcí uchovávání dat pro potřeby soudního řízení (litigation hold), dočasné zablokování jednotlivých uživatelských účtů, dočasné odpojení fungujících počítačů od sítě, odstraňování a

opětovná instalace disků z počítačů a poskytování podpory v souvislosti s „přístupovými právy správce“. Pokud jsou taková opatření přijata, podnik nesmí do jejich provádění nijak zasahovat a má povinnost náležitě informovat dotčené zaměstnance. Kontroloři mohou požádat o použití hardwaru podniku (např. paměťových médií, klíčů USB, spojovacích kabelů, skenerů, tiskáren, obrazovek), ale jeho použití pro ně není povinné. Kontrolovaný podnik kontrolory na požádání informuje o tom, jak jsou jejich žádosti vyřizovány, a to tak, že poskytne soubory protokolů nebo informuje kontrolory o pokynech udělených zaměstnancům podniku, kteří jsou pověřeni vyřízením žádostí kontrolorů.

12) Paměťová média vybraná k přezkumu si mohou kontroloři ponechat až do konce kontroly v prostorách podniku. Mohou je však vrátit i dříve, např. po pořízení čitelného hodnověrného forenzního duplikátu dat, která jsou předmětem šetření. Tento forenzní hodnověrný duplikát zreplikuje (všechna nebo dílčí) data uložená na původním médiu. Přezkum hodnověrného duplikátu je rovnocenný přezkumu původního paměťového média.

13) Od okamžiku, kdy je oznámeno rozhodnutí o kontrole, podnik jedná s náležitou péčí a přijímá veškerá vhodná opatření k uchování důkazů, které má k dispozici. Je povinností podniku, aby o tom odpovídajícím způsobem informoval své zaměstnance a zástupce. Vymazání obchodních záznamů (nebo manipulace s nimi), ať už úmyslně nebo z nedbalosti, může představovat překážku při kontrole ze strany Komise. V případě, že podnik klade překážky, může mu Komise uložit pokutu až do výše 1 % jeho celkového obratu za předchozí hospodářský rok.

14) Povinnost uchovávat důkazy přesahuje samotné trvání kontroly na místě ([2]).

15) Na konci kontroly kontroloři kompletně vymažou ([3]) všechna forenzní paměťová IT média Komise, na nichž byla data společnosti uložena. Hardware poskytnutý podnikem kontroloři nevymažou a podniku ho vrátí.

16) Není-li po předpokládaném ukončení kontroly na místě v prostorách podniku výběr dokumentů relevantních pro šetření ještě dokončen, mohou existovat oprávněné důvody, aby se Komise rovněž v zájmu dotčeného podniku rozhodla, že v kontrole dat, která od podniku získala, bude pokračovat ve svých prostorách v Bruselu. V takovém případě může být získána kopie souboru dat, který je teprve třeba prohledat, společně s již prohledaným souborem dat, aby mohla kontrola pokračovat později. Tato kopie bude zabezpečena umístěním do zapečetěné obálky, která bude přemístěna do prostor Komise v Bruselu. Komise podnik vyzve, aby byl přítomen i) při otevření zapečetěné obálky a ii) během pokračování procesu kontroly v prostorách Komise. Pokud pokračování kontroly vede k tomu, že kontrolovanému podniku vzniknou dodatečné náklady pouze v důsledku uvedeného pokračování, může podnik požadovat náhradu těchto nákladů na základě řádně odůvodněné žádosti předložené za tímto účelem. Komise se může případně rozhodnout, že zapečetěnou obálku podniku vrátí, aniž by ji otevřela. Komise může také podnik požádat, aby zapečetěnou obálku uložil na bezpečném

([2]) Za tímto účelem viz rozsudek ze dne 9. dubna 2019 ve věci T-371/17, Qualcomm a Qualcomm Europe v. Komise, EU:T:2019:232, bod 136, potvrzeno v odvolání ve věci C-466/19 P, Qualcomm a Qualcomm Europe v. Komise, EU:C:2021:76, bod 114.

([3]) Technickým termínem pro tento výmaz dat je „sanitizace“ (taktéž označováno jako „bezpečné vymazání“). Cílem sanitizace je data z paměťového zařízení zcela odstranit tak, aby nemohla být žádným známým postupem zrekonstruována.

místě, což Komisi umožní pokračovat v procesu prohledávání během další ohlášené návštěvy v prostorách podniku.

17) Podniku bude poskytnuta příležitost přezkoumat soubor či soubory dat, které byly kontrolory předběžně vybrány a které mají být přidány do spisu, aby se určilo, zda chce vznést nároky týkající se například dat, jež jsou potenciálně chráněna povinností mlčenlivosti, nebo zvláštních kategorií osobních údajů ([4]). Pokud se podnik domnívá, že jakákoli data, která kontroloři vybrali a která mají být doplněna do spisu, nesouvisejí s předmětem rozhodnutí o kontrole, může to v této fázi rovněž oznámit. Pokud jde o konečný soubor dat vybraný kontrolory během kontroly na místě (nebo v rámci pokračující kontroly), který je přidán do spisu Komise, obdrží podnik datový nosič (např. klíč USB), na němž jsou všechna tato data uložena. Podnik bude požádán, aby podepsal seznam (seznamy) konečného exportu vybraných dat. Kontroloři si odnesou dvě identické kopie těchto souborů dat uložených na zašifrovaných datových nosičích.

18) Důkazy vybrané během kontroly mohou být shromážděny jako technický celek (pokud je např. vybrána jen jedna příloha e-mailu, bude konečný export sestávat z průvodního e-mailu a všech příloh, které k dané zprávě patří). Při konečném zpracování do spisu může být každý důkaz rozložen na jednotlivé komponenty (např. průvodní e-mail, přílohy a/nebo další vložená data), které mohou být poté zaevidovány samostatně a jimž jsou následně přidělena samostatná referenční čísla.

19) V případě, že podnik na žádost kontrolorů poskytne materiál ke kopírování, Komise na žádost podniku náklady na materiál, jenž byl použit na pořízení kopií pro Komisi, uhradí.

20) Na dokumenty zkopírované během kontroly se vztahují ustanovení článku 28 nařízení (ES) č. 1/2003 o profesním tajemství. Pokud bude v pozdější fázi řízení nutné zpřístupnit uvedené dokumenty dalším stranám, např. za účelem udělení přístupu ke spisu, bude podnik vyzván, aby označil jakékoli obchodní tajemství nebo jiné důvěrné informace obsažené v těchto dokumentech, odůvodnil svoje žádosti a poskytl verze, které nejsou důvěrné.

21) Pokud se kontroloři rozhodnou zapečetit podnikatelské prostory, účetní knihy nebo záznamy, sepíše se zápis. Je povinností podniku zajistit, že umístěné pečeti zůstanou neporušeny do doby, než je kontroloři opět odstraní. Při odstraňování pečetí bude vypracován samostatný zápis, v němž bude zaznamenán stav pečetí v daném okamžiku.

22) Na osobní údaje shromážděné Komisí během antimonopolních šetření se vztahuje nařízení (EU) 2018/1725. Jelikož se antimonopolní pravidla EU vztahují pouze na podniky, nejsou osobní údaje fyzických osob jako takové předmětem antimonopolních šetření a kontrol prováděných Komisí. Osobní údaje jednotlivých zaměstnanců podniků (např. jejich jména, telefonní čísla, e-mailové adresy) však mohou být obsaženy v obchodních dokumentech týkajících se těchto šetření, a

([4]) Viz čl. 10 odst. 1 nařízení (EU) 2018/1725, v němž se zvláštními kategoriemi osobních údajů myslí osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické nebo biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci. Viz čl. 9 odst. 1 nařízení (EU) 2016/679.

proto mohou být během kontroly zkopírovány nebo získány a mohou být zařazeny do spisu Komise.

23) Veškeré osobní údaje v antimonopolních spisech Komise lze použít pouze pro účely, k nimž byly shromážděny (prosazování článků 101 a/nebo 102 Smlouvy o fungování EU), a budou zpracovávány v souladu s nařízením (EU) 2018/1725, jak je dále upřesněno v prohlášení GŘ pro hospodářskou soutěž o ochraně osobních údajů([5]).

24) Pokud soubor (soubory) dat zpřístupněný (zpřístupněné) kontrolorům zahrnuje (zahrnují) zvláštní kategorie osobních údajů,([6]) měl by podnik kontrolory upozornit na přítomnost těchto citlivých osobních údajů a identifikovat konkrétní dotčené soubory nebo data. Kontroloři se budou snažit tyto záznamy přezkoumat v souladu se samostatným postupem s ohledem na jejich citlivost.

([5]) Viz https://competition-policy.ec.europa.eu/system/files/2021-05/privacy_statement_antitrust_cs.pdf

([6]) Viz poznámka pod čarou 4 výše.