Sbírka soudních rozhodnutí

ROZSUDEK SOUDNÍHO DVORA (třetího senátu)

14. prosince 2023 *

„Řízení o předběžné otázce – Ochrana fyzických osob v souvislosti se zpracováním osobních údajů – Nařízení (EU) 2016/679 – Článek 5 – Zásady tohoto zpracování – Článek 24 – Odpovědnost správce – Článek 32 – Opatření prováděná k zajištění zabezpečení zpracování – Posouzení vhodnosti takových opatření – Rozsah soudního přezkumu – Provádění důkazů – Článek 82 – Právo na náhradu újmy a odpovědnost – Případné zproštění odpovědnosti správce v případě porušení, kterého se dopustily třetí strany – Návrh na náhradu nehmotné újmy na základě obavy z možného zneužití osobních údajů“

Ve věci C-340/21,

jejímž předmětem je žádost o rozhodnutí o předběžné otázce podaná na základě článku 267 SFEU rozhodnutím Nejvyššího správního soudu (Varchoven administrativen sad, Bulharsko) ze dne 14. května 2021, došlým Soudnímu dvoru dne 2. června 2021, v řízení

VB

proti

Nacionalna agencia za prichodite,

SOUDNÍ DVŮR (třetí senát),

ve složení: K. Jürimäe, předsedkyně senátu, N. Piçarra, M. Safjan, N. Jääskinen (zpravodaj) a M. Gavalec, soudci,

generální advokát: G. Pitruzzella,

za soudní kancelář: A. Calot Escobar, vedoucí,

s přihlédnutím k písemné části řízení,

s ohledem na vyjádření, která předložili:

– za Nacionalna agencia za prichodite: R. Specov,

– za bulharskou vládu: M. Georgieva a L. Zacharieva, jako zmocněnkyně,

– za českou vládu: O. Serdula, M. Smolek a J. Vláčil, jako zmocněnci,

* Jednací jazyk: bulharština.

– za Irsko: M. Browne, Chef State Solicitor, A. Joyce, J. Quaney a M. Tierney, jako zmocněnci, ve spolupráci s: D. Fennelly, BL,

– za italskou vládu: G. Palmieri, jako zmocněnkyně, ve spolupráci s: E. De Bonis, avvocato dello Stato,

– za portugalskou vládu: P. Barros da Costa, A. Pimenta, J. Ramos a C. Vieira Guerra, jako zmocněnkyně,

– za Evropskou komisi: A. Bouchagiar, H. Kranenborg a N. Nikolova, jako zmocněnci,

po vyslechnutí stanoviska generálního advokáta na jednání konaném dne 27. dubna 2023,

vydává tento

Rozsudek

1 Žádost o rozhodnutí o předběžné otázce se týká výkladu čl. 5 odst. 2, článků 24 a 32, jakož i čl. 82 odst. 1 až 3 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. 2016, L 119, s. 1, dále jen „GDPR“).

2 Tato žádost byla předložena v rámci sporu mezi VB, fyzickou osobou, a Národní agenturou pro veřejné příjmy (Nacionalna agencia za prichodite, Bulharsko) (dále jen „NAP“) ve věci náhrady nehmotné újmy, která měla této osobě vzniknout v důsledku údajného nesplnění zákonných povinností ze strany tohoto orgánu veřejné moci jakožto správce osobních údajů.

Právní rámec

3 Body 4, 10, 11, 74, 76, 83, 85 a 146 odůvodnění GDPR znějí následovně:

„(4) […] Toto nařízení ctí všechna základní práva a dodržuje svobody a zásady uznávané [Listinou základních práv Evropské unie], jak jsou zakotveny ve Smlouvách, zejména respektování soukromého a rodinného života, obydlí a komunikace, ochranu osobních údajů, […] právo na účinnou právní ochranu a spravedlivý proces […]

[…]

(10) S cílem zajistit soudržnou a vysokou úroveň ochrany fyzických osob a odstranit překážky bránící pohybu osobních údajů v rámci [Evropské] [u]nie by měla být úroveň ochrany práv a svobod fyzických osob v souvislosti se zpracováním těchto údajů rovnocenná ve všech členských státech. V celé Unii je třeba zajistit soudržné a jednotné uplatňování pravidel ochrany základních práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů. […]

(11) Účinná ochrana osobních údajů v celé Unii vyžaduje […] posílení a podrobné vymezení práv subjektů údajů a povinností těch, kdo osobní údaje zpracovávají a o jejich zpracování rozhodují, […]

[…]

(74) Měla by být stanovena odpovědnost správce za jakékoliv zpracování osobních údajů prováděné správcem nebo pro něj. Správce by měl být zejména povinen zavést vhodná a účinná opatření a být schopen doložit, že činnosti zpracování jsou v souladu s tímto nařízením, včetně účinnosti opatření. Tato opatření by měla zohledňovat povahu, rozsah, kontext a účely zpracování a riziko pro práva a svobody fyzických osob.

[…]

(76) Pravděpodobnost a závažnost rizika pro práva a svobody subjektu údajů by měly být určeny na základě povahy, rozsahu, kontextu a účelům zpracování. Riziko by mělo být hodnoceno na základě objektivního posouzení, které stanoví, zda operace zpracování představují riziko či vysoké riziko.

[…]

(83) V zájmu zachování bezpečnosti a zabránění zpracování, které by bylo v rozporu s tímto nařízením, by měl správce nebo zpracovatel posoudit rizika spojená se zpracováním a přijmout opatření ke zmírnění těchto rizik, například šifrování. Tato opatření by měla zajistit náležitou úroveň bezpečnosti, včetně důvěrnosti, s ohledem na stav techniky, náklady na provedení v souvislosti s rizikem a povahu osobních údajů, které mají být chráněny. Při posuzování rizik pro zabezpečení osobních údajů by se měla vzít v úvahu rizika, která zpracování představuje, jako jsou náhodné nebo protiprávní zničení, ztráta, pozměnění, neoprávněné zpřístupnění nebo zpřístupnění předaných, uložených nebo jiným způsobem zpracovaných osobních údajů, které by mohly zejména vést k fyzické, hmotné nebo nehmotné újmě.

[…]

(85) Není-li porušení zabezpečení osobních údajů řešeno náležitě a včas, může to fyzickým osobám způsobit fyzickou, hmotnou či nehmotnou újmu, jako je ztráta kontroly nad jejich osobními údaji nebo omezení jejich práv, diskriminace, krádež nebo zneužití identity, finanční ztráta, neoprávněné zrušení pseudonymizace, poškození pověsti, ztráta důvěrnosti osobních údajů chráněných služebním tajemstvím nebo jakékoliv jiné významné hospodářské či společenské znevýhodnění dotčených fyzických osob. Jakmile se tedy správce o porušení zabezpečení osobních údajů dozví, měl by je bez zbytečného odkladu […] ohlásit příslušnému dozorovému úřadu […]

[…]

(146) Veškerou újmu, která může osobám vzniknout v důsledku zpracování, které porušuje toto nařízení, by měl nahradit správce nebo zpracovatel. Správce nebo zpracovatel by však měl být odpovědnosti zproštěn, pokud prokáže, že za újmu nenese žádným způsobem odpovědnost. Výklad pojmu ‚újma' by měl být široký a opírat se o judikaturu Soudního dvora při plném zohlednění cílů tohoto nařízení. Tím nejsou dotčeny jakékoliv nároky uplatňované v případě újmy způsobené porušením jiných pravidel práva Unie nebo členského státu. Zpracování, které porušuje toto nařízení, zahrnuje rovněž zpracování,

které porušuje akty v přenesené pravomoci a prováděcí akty přijaté v souladu s tímto nařízením a právními předpisy členského státu upřesňující pravidla tohoto nařízení. Subjekty údajů by měly obdržet plnou a účinnou náhradu újmy, kterou utrpěly. […]“

4 Článek 4 tohoto nařízení, nadepsaný „Definice“, stanoví:

„Pro účely tohoto nařízení se rozumí:

1) ‚osobními údaji‘ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen ‚subjekt údajů‘); […]

2) ‚zpracováním‘ jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů […]

[…]

7) ‚správcem‘ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; […]

[…]

10) ‚třetí stranou‘ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů;

[…]

12) ‚porušením zabezpečení osobních údajů‘ porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;

[…]“

5 Článek 5 uvedeného nařízení, nadepsaný „Zásady zpracování osobních údajů“, stanoví:

„1. Osobní údaje musí být:

a) ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem (‚zákonnost, korektnost a transparentnost‘);

[…]

f) zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením (‚integrita a důvěrnost‘).

2. Správce odpovídá za dodržení odstavce 1 a musí být schopen toto dodržení souladu doložit (‚odpovědnost‘).“

6 Článek 24 téhož nařízení, nadepsaný „Odpovědnost správce“, stanoví:

„1. S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována.

2. Pokud je to s ohledem na činnosti zpracování přiměřené, zahrnují opatření uvedená v odstavci 1 uplatňování vhodných koncepcí v oblasti ochrany údajů správcem.

3. K doložení plnění povinností správce lze použít i dodržování schválených kodexů chování uvedených v článku 40 nebo schválených mechanismů pro vydávání osvědčení uvedených v článku 42.“

7 Článek 32 GDPR, nadepsaný „Zabezpečení zpracování“, stanoví:

„1. S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

a) pseudonymizace a šifrování osobních údajů;

b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;

c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění zabezpečení zpracování.

2. Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

3. K doložení plnění požadavků stanovených v odstavci 1 tohoto článku lze použít i dodržování schváleného kodexu chování uvedeného v článku 40 nebo schváleného mechanismu pro vydávání osvědčení uvedeného v článku 42.

[…]“

8 Článek 79 tohoto nařízení, nadepsaný „Právo na účinnou soudní ochranu vůči správci nebo zpracovateli“, v odstavci 1 stanoví:

„Aniž je dotčena jakákoli dostupná správní či mimosoudní ochrana, včetně práva na podání stížnosti u dozorového úřadu podle článku 77, má každý subjekt údajů právo na účinnou soudní ochranu, pokud má za to, že jeho práva podle tohoto nařízení byla porušena v důsledku zpracování jeho osobních údajů v rozporu s tímto nařízením.“

9 Článek 82 uvedeného nařízení, nadepsaný „Právo na náhradu újmy a odpovědnost“, v odstavcích 1 až 3 stanoví:

„1. Kdokoli, kdo v důsledku porušení tohoto nařízení utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy.

2. Správce zapojený do zpracování je odpovědný za újmu, kterou způsobí zpracováním, jež porušuje toto nařízení. […]

3. Správce nebo zpracovatel jsou odpovědnosti podle odstavce 2 zproštěni, pokud prokáží, že nenesou žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.“

Spor v původním řízení a předběžné otázky

10 NAP je orgánem, který je podřízen bulharskému ministrovi financí. V rámci svých úkolů spočívajících mimo jiné v identifikaci, zajištění a vymáhání veřejných pohledávek je správcem osobních údajů ve smyslu čl. 4 bodu 7 GDPR.

11 Dne 15. července 2019 odhalily sdělovací prostředky, že došlo k neoprávněnému přístupu do informačního systému NAP, a že v důsledku tohoto kybernetického útoku byly na internetu zveřejněny osobní údaje obsažené v uvedeném systému.

12 Těmito událostmi bylo dotčeno více než šest milionů fyzických osob bulharské nebo cizí státní příslušnosti. Několik stovek z nich, včetně žalobkyně v původním řízení, podalo proti NAP žaloby na náhradu nehmotné újmy, která jim údajně vznikla v důsledku zveřejnění jejich osobních údajů.

13 V tomto kontextu podala žalobkyně v původním řízení žalobu ke Správnímu soudu města Sofie (Administrativen sad Sofia-grad, Bulharsko), kterou se domáhala, aby jí NAP zaplatila částku 1 000 bulharských leva (BGN) (přibližně 510 eur) z titulu náhrady újmy na základě článku 82 GDPR a ustanovení bulharského práva. Na podporu této žádosti tvrdila, že utrpěla nehmotnou újmu v důsledku porušení zabezpečení osobních údajů ve smyslu čl. 4 bodu 12 GDPR, konkrétně porušení zabezpečení, které mělo být způsobeno tím, že NAP nesplnila povinnosti, které pro ni vyplývají zejména z čl. 5 odst. 1 písm. f), jakož i z článků 24 a 32 tohoto nařízení. Její nehmotná újma spočívala v obavě, že její osobní údaje, které byly zveřejněny bez jejího souhlasu, budou v budoucnu zneužity nebo že bude sama vystavena vydírání, útoku, nebo dokonce únosu.

14 NAP na svou obranu nejprve uvedla, že žalobkyně v původním řízení ji nepožádala o informace týkající se přesných údajů, které byly zveřejněny. NAP dále předložila dokumenty, které měly prokázat, že přijala veškerá nezbytná opatření, aby zabránila porušení zabezpečení osobních údajů obsažených v jejím informačním systému, jakož i následně aby omezila účinky tohoto porušení a ubezpečila občany. Kromě toho podle NAP neexistovala příčinná souvislost mezi tvrzenou nehmotnou újmou a uvedeným porušením. Nakonec uvedla, že vzhledem k tomu, že sama byla poškozena nepřátelským zásahem ze strany osob, které nebyly jejími zaměstnanci, nemůže být činěna odpovědnou za škodlivé následky tohoto zásahu.

15 Rozhodnutím ze dne 27. listopadu 2020 zamítl Správní soud města Sofie (Administrativen sad Sofia-grad) žalobu žalobkyně v původním řízení. Tento soud měl za to, že neoprávněný přístup k databázi NAP byl výsledkem informačního pirátství spáchaného třetími stranami a žalobkyně v původním řízení neprokázala nečinnost NAP, pokud jde o přijetí bezpečnostních opatření. Dále měl za to, že této žalobkyni nevznikla nehmotná újma zakládající nárok na náhradu.

16 Žalobkyně v původním řízení podala proti uvedenému rozhodnutí kasační opravný prostředek k Nejvyššímu správnímu soudu (Varchoven administrativen sad, Bulharsko), který je předkládajícím soudem v projednávané věci. Na podporu svého kasačního opravného prostředku tvrdí, že se soud prvního stupně dopustil nesprávného právního posouzení při rozložení důkazního břemene týkajícího se bezpečnostních opatření přijatých NAP a že tento orgán v tomto ohledu neprokázal neexistenci nečinnosti. Kromě toho žalobkyně v původním řízení tvrdí, že obava z možného zneužití jejích osobních údajů v budoucnu představuje skutečnou, a nikoli hypotetickou nehmotnou újmu. NAP na svou obranu každý z těchto argumentů zpochybňuje.

17 Předkládající soud nejprve zvažuje možnost, že zjištění, že došlo k porušení zabezpečení osobních údajů, samo o sobě umožňuje učinit závěr, že opatření provedená správcem těchto údajů nebyla „vhodná“ ve smyslu článků 24 a 32 GDPR.

18 Nicméně v případě, že by toto zjištění nepostačovalo k učinění takového závěru, klade si předkládající soud otázku týkající se rozsahu přezkumu, který musí vnitrostátní soudy provést k posouzení vhodnosti dotyčných opatření, a dále pravidel týkajících se provádění důkazů, která musí být v tomto rámci uplatněna, a to v otázce jak důkazního břemene, tak důkazních prostředků, zejména je-li těmto soudům předložena žaloba na náhradu újmy na základě článku 82 tohoto nařízení.

19 Dále se tento soud táže, zda s ohledem na čl. 82 odst. 3 uvedeného nařízení skutečnost, že k porušení zabezpečení osobních údajů došlo v důsledku jednání třetích stran, v projednávané věci kybernetického útoku, představuje faktor, který systematicky zprošťuje správce těchto údajů odpovědnosti za újmu způsobenou subjektu údajů.

20 Nakonec si uvedený soud klade otázku, zda obava osoby, že její osobní údaje mohou být v budoucnu zneužity, v projednávaném případě v důsledku neoprávněného přístupu k těmto údajům a jejich zveřejnění pachateli kybernetické kriminality, může sama o sobě představovat „nehmotnou újmu“ ve smyslu čl. 82 odst. 1 GDPR. V případě kladné odpovědi by tato osoba byla zproštěna povinnosti prokázat, že před jejím návrhem na náhradu újmy došlo k takovému protiprávnímu užití údajů třetími stranami, jako je například zneužití její totožnosti.

21 Za těchto podmínek se Varchoven administrativen sad (Nejvyšší správní soud) rozhodl přerušit řízení a položit Soudnímu dvoru následující předběžné otázky:

„1) Musí být články 24 a 32 [GDPR] vykládány v tom smyslu, že postačuje, aby došlo k neoprávněnému poskytnutí nebo zpřístupnění osobních údajů ve smyslu čl. 4 bodu 12 [GDPR] ze strany osob, které nejsou zaměstnanci administrativy správce osobních údajů a nepodléhají jeho kontrole, aby bylo možno mít za to, že přijatá technická a organizační opatření nejsou vhodná?

2) V případě záporné odpovědi na první otázku, jaký předmět a rozsah by měl mít soudní přezkum legality prováděný při posuzování otázky, zda jsou technická a organizační opatření podle článku 32 [GDPR], která přijal správce osobních údajů, vhodná?

3) V případě záporné odpovědi na první otázku musí být zásada odpovědnosti podle čl. 5 odst. 2 a článek 24 ve spojení s bodem 74 odůvodnění [GDPR] vykládány v tom smyslu, že v řízení o žalobě podle čl. 82 odst. 1 tohoto nařízení nese správce osobních údajů důkazní břemeno ohledně toho, že přijatá technická a organizační opatření podle článku 32 [téhož] nařízení jsou vhodná?

   Lze opatření znaleckého posudku považovat za nezbytný a dostatečný důkazní prostředek pro zjištění, zda byla technická a organizační opatření přijatá správcem v takovém případě, jako je tento, vhodná, pokud je neoprávněný přístup k osobním údajům nebo jejich neoprávněné zpřístupnění důsledkem ‚hackerského útoku'?

4) Musí být čl. 82 odst. 3 [GDPR] vykládán v tom smyslu, že neoprávněné poskytnutí nebo zpřístupnění osobních údajů ve smyslu čl. 4 bodu 12 [GDPR], k němuž jako v projednávané věci došlo prostřednictvím ‚hackerského útoku' osob, které nejsou zaměstnanci administrativy správce osobních údajů a nepodléhají jeho kontrole, představuje událost, za kterou správce osobních údajů žádným způsobem nenese odpovědnost a která opravňuje ke zproštění odpovědnosti?

5) Musí být čl. 82 odst. 1 a 2 ve spojení s body 85 a 146 odůvodnění [GDPR] vykládány v tom smyslu, že v takovém případě porušení zabezpečení osobních údajů, o jaký se jedná v projednávané věci, který se projevuje neoprávněným zpřístupněním a šířením osobních údajů prostřednictvím ‚hackerského útoku', pod pojem ‚nehmotné újmy', který je třeba vykládat široce, spadají pouhé znepokojení, obavy a úzkost z možného budoucího zneužití osobních údajů, které zakusil subjekt údajů, a opravňují k náhradě újmy, pokud nebylo zjištěno, že k takovému zneužití došlo, nebo subjektu údajů nevznikla žádná další újma?"

K předběžným otázkám

K první otázce

22 Podstatou první otázky předkládajícího soudu je, zda články 24 a 32 GDPR musí být vykládány v tom smyslu, že postačuje samotná skutečnost, že došlo k neoprávněnému poskytnutí nebo zpřístupnění osobních údajů „třetími stranami" ve smyslu čl. 4 bodu 10 tohoto nařízení, aby bylo možno mít za to, že technická a organizační opatření zavedená dotčeným správcem nejsou „vhodná" ve smyslu těchto článků 24 a 32.

23 Úvodem je třeba připomenout, že podle ustálené judikatury musí být znění ustanovení unijního práva, které stejně jako články 24 a 32 GDPR výslovně neodkazuje na právo členských států za účelem vymezení svého smyslu a dosahu, zpravidla vykládáno autonomním a jednotným způsobem v celé Unii, přičemž tento výklad je třeba nalézt zejména s přihlédnutím ke znění dotčeného ustanovení, cílům sledovaným tímto ustanovením a kontextu, do něhož toto ustanovení spadá [v tomto smyslu viz rozsudky ze dne 18. ledna 1984, Ekro, 327/82, EU:C:1984:11, bod 11; ze dne 1. října 2019, Planet49, C-673/17, EU:C:2019:801, body 47 a 48, jakož i ze dne 4. května 2023, Österreichische Post (Nehmotná újma související se zpracováním osobních údajů), C-300/21, EU:C:2023:370, bod 29].

24 Zaprvé, pokud jde o znění relevantních ustanovení, je třeba uvést, že článek 24 GDPR stanoví obecnou povinnost správce osobních údajů zavést vhodná technická a organizační opatření, aby zajistil, že uvedené zpracování bude prováděno v souladu s tímto nařízením, a mohl to doložit.

25 Za tímto účelem tento článek 24 v odstavci 1 vyjmenovává určitá kritéria, která je třeba zohlednit při posuzování vhodnosti takových opatření, a sice povahu, rozsah, kontext a účely zpracování, jakož i různě pravděpodobná a různě závažná rizika pro práva a svobody fyzických osob. Toto ustanovení dodává, že uvedená opatření musí být podle potřeby revidována a aktualizována.

26 Z tohoto hlediska článek 32 GDPR upřesňuje povinnosti správce a případného zpracovatele, pokud jde o zabezpečení tohoto zpracování. Odstavec 1 tohoto článku tak stanoví, že posledně zmínění musí provést vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající rizikům uvedeným v předchozím bodě tohoto rozsudku, a to s přihlédnutím ke stavu techniky, nákladům na provedení, jakož i k povaze, rozsahu, kontextu a účelům dotyčného zpracování.

27 Stejně tak odstavec 2 uvedeného článku stanoví, že při posuzování vhodné úrovně zabezpečení se musí zohlednit zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění osobních údajů, nebo neoprávněný přístup k nim.

28 Kromě toho jak čl. 24 odst. 3 tohoto nařízení, tak jeho čl. 32 odst. 3 uvádějí, že správce nebo zpracovatel může doložit, že splnil požadavky odstavců 1 těchto článků na základě toho, že dodržuje schválený kodex chování nebo schválený mechanismus pro vydávání osvědčení, jak jsou uvedeny v článcích 40 a 42 uvedeného nařízení.

29 Odkaz v čl. 32 odst. 1 a 2 GDPR na „úroveň zabezpečení odpovídající danému riziku“ a na „vhodnou úroveň zabezpečení“ svědčí o tom, že toto nařízení zavádí režim řízení rizik a nijak neusiluje o odstranění rizik porušování zabezpečení osobních údajů.

30 Ze znění článků 24 a 32 GDPR tak vyplývá, že tato ustanovení pouze ukládají správci povinnost zavést technická a organizační opatření, jejichž cílem je v co největším možném rozsahu zabránit jakémukoliv porušení zabezpečení osobních údajů. Vhodnost takových opatření musí být posouzena konkrétně, přičemž se prověří, zda tato opatření byla tímto správcem zavedena s přihlédnutím k jednotlivým kritériím stanoveným v uvedených článcích a potřebám ochrany údajů dotyčného zpracování, jakož i rizikům plynoucím z tohoto zpracování.

31 Články 24 a 32 GDPR tudíž nelze chápat v tom smyslu, že neoprávněné poskytnutí nebo zpřístupnění osobních údajů třetí stranou postačují k učinění závěru, že opatření přijatá dotyčným správcem nejsou vhodná ve smyslu těchto ustanovení, aniž tomuto správci umožňují prokázat opak.

32 Takový výklad je jediný možný tím spíše, že článek 24 GDPR výslovně stanoví, že správce musí být schopen doložit soulad opatření, která zavedl, s tímto nařízením, což je možnost, o kterou by v případě připuštění nevyvratitelné domněnky přišel.

33 Zadruhé tento výklad článků 24 a 32 GDPR potvrzují kontextuální a teleologické faktory.

34 Pokud jde o kontext těchto dvou článků, je třeba uvést, že z čl. 5 odst. 2 GDPR vyplývá, že správce musí být schopen doložit, že dodržel zásady zpracování osobních údajů stanovené v odstavci 1 uvedeného článku. Tato povinnost je převzata a upřesněna v čl. 24 odst. 1 a 3, jakož i v čl. 32 odst. 3 tohoto nařízení, co se týče povinnosti zavést technická a organizační opatření k ochraně takových údajů při zpracování prováděném tímto správcem. Taková povinnost doložit vhodnost těchto opatření by přitom neměla smysl, pokud by byl správce povinen zabránit jakémukoliv zásahu do uvedených údajů.

35 Kromě toho bod 74 odůvodnění GDPR zdůrazňuje, že je důležité, aby měl správce povinnost zavést vhodná a účinná opatření a být schopen doložit, že činnosti zpracování jsou v souladu s tímto nařízením, včetně účinnosti opatření, která by měla zohledňovat kritéria související s charakteristikami dotyčného zpracování a s jím představovaným rizikem, která jsou rovněž uvedena v jeho článcích 24 a 32.

36 Stejně tak podle bodu 76 odůvodnění tohoto nařízení závisí pravděpodobnost a závažnost rizika na specifických rysech dotčeného zpracování a toto riziko by mělo být hodnoceno na základě objektivního posouzení.

37 Kromě toho z čl. 82 odst. 2 a 3 GDPR vyplývá, že i když je správce odpovědný za újmu, kterou způsobí zpracováním, jež porušuje toto nařízení, je nicméně zproštěn odpovědnosti, pokud prokáže, že nenese žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.

38 Výklad uvedený v bodě 31 tohoto rozsudku je rovněž potvrzen bodem 83 odůvodnění GDPR, který ve své první větě uvádí, že „[v] zájmu zachování bezpečnosti a zabránění zpracování, které by bylo v rozporu s tímto nařízením, by měl správce nebo zpracovatel posoudit rizika spojená se zpracováním a přijmout opatření ke zmírnění těchto rizik“. Unijní normotvůrce tak vyjádřil svůj záměr „zmírnit“ rizika porušení zabezpečení osobních údajů, aniž tvrdil, že by bylo možné je odstranit.

39 S ohledem na výše uvedené důvody je třeba na první otázku odpovědět tak, že články 24 a 32 GDPR musí být vykládány v tom smyslu, že samotná skutečnost, že došlo k neoprávněnému poskytnutí nebo zpřístupnění osobních údajů „třetími stranami“ ve smyslu čl. 4 bodu 10 tohoto nařízení nepostačuje k tomu, aby bylo možné mít za to, že technická a organizační opatření zavedená dotčeným správcem nejsou „vhodná“ ve smyslu těchto článků 24 a 32.

K druhé otázce

40 Podstatou druhé otázky předkládajícího soudu je, zda musí být článek 32 GDPR vykládán v tom smyslu, že vhodnost technických a organizačních opatření zavedených správcem na základě tohoto článku musí být vnitrostátními soudy posuzována konkrétně, zejména s přihlédnutím k rizikům spojeným s dotyčným zpracováním.

41 V tomto ohledu je třeba připomenout, jak bylo zdůrazněno v rámci odpovědi na první otázku, že článek 32 GDPR vyžaduje, aby s přihlédnutím ke kritériím pro posouzení stanoveným v odstavci 1 provedli správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající riziku. Kromě toho odstavec 2 tohoto článku obsahuje demonstrativní výčet určitých faktorů, které jsou relevantní při posuzování vhodné úrovně zabezpečení s ohledem na rizika dotyčného zpracování.

42 Z uvedeného čl. 32 odst. 1 a 2 vyplývá, že vhodnost takových technických a organizačních opatření je třeba posoudit ve dvou fázích. V první fázi je třeba zjistit rizika porušení zabezpečení osobních údajů vyvolané dotyčným zpracováním a jejich případné důsledky pro práva a svobody fyzických osob. Toto posouzení musí být prováděno konkrétně s přihlédnutím ke stupni pravděpodobnosti zjištěných rizik a stupni jejich závažnosti. V druhé fázi je třeba ověřit, zda opatření zavedená správcem odpovídají těmto rizikům, a to s přihlédnutím ke stavu techniky, nákladům na provedení, jakož i k povaze, rozsahu, kontextu a účelům tohoto zpracování.

43 Je sice pravda, že správce má určitý prostor pro uvážení při stanovení vhodných technických a organizačních opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, jak vyžaduje čl. 32 odst. 1 GDPR. Nic to však nemění na tom, že vnitrostátní soud musí mít možnost přezkoumat komplexní posouzení, které provedl správce, a ujistit se tak, že jím přijatá opatření mohou zajistit takovou úroveň zabezpečení.

44 Takový výklad může ostatně zajistit jednak účinnost ochrany osobních údajů, kterou zdůrazňují body 11 a 74 odůvodnění tohoto nařízení, a jednak právo na účinnou soudní ochranu vůči správci, které je zakotveno v čl. 79 odst. 1 uvedeného nařízení ve spojení s bodem 4 odůvodnění téhož nařízení.

45 Za účelem přezkumu vhodnosti technických a organizačních opatření zavedených na základě článku 32 GDPR se tudíž vnitrostátní soud nesmí omezit na zjištění, jakým způsobem měl dotyčný správce v úmyslu splnit povinnosti, které pro něj vyplývají z tohoto článku, ale musí provést meritorní přezkum těchto opatření s ohledem na všechna kritéria uvedená v tomto článku, jakož i k okolnostem projednávané věci a důkazům, které má v tomto ohledu tento soud k dispozici.

46 Takový přezkum vyžaduje provedení konkrétní analýzy povahy a obsahu opatření zavedených správcem, způsobu, jakým byla tato opatření uplatňována, a jejich praktických účinků na úroveň zabezpečení, kterou byl tento správce povinen zajistit s přihlédnutím k rizikům tohoto zpracování.

47 V důsledku toho je třeba na druhou otázku odpovědět tak, že článek 32 GDPR musí být vykládán v tom smyslu, že vhodnost technických a organizačních opatření zavedených správcem na základě tohoto článku musí být vnitrostátními soudy posuzována konkrétně se zohledněním rizik spojených s dotyčným zpracováním, přičemž posoudí, zda povaha, obsah a provádění těchto opatření odpovídají těmto rizikům.

K třetí otázce

K první části třetí otázky

48 Podstatou první části třetí otázky předkládajícího soudu je, zda zásada odpovědnosti správce, která je uvedena v čl. 5 odst. 2 GDPR a konkretizována v jeho článku 24, musí být vykládána v tom smyslu, že v rámci žaloby na náhradu újmy na základě článku 82 tohoto nařízení nese dotčený správce důkazní břemeno ohledně vhodnosti bezpečnostních opatření, která provedl podle článku 32 uvedeného nařízení.

49 V tomto ohledu je třeba zaprvé připomenout, že čl. 5 odst. 2 GDPR stanoví zásadu odpovědnosti, podle níž správce odpovídá za dodržení zásad zpracování osobních údajů uvedených v odstavci 1 tohoto článku a stanoví, že uvedený správce musí být schopen doložit, že jsou tyto zásady dodrženy.

50 Správce musí zejména v souladu se zásadou integrity a důvěrnosti osobních údajů, která je uvedena v čl. 5 odst. 1 písm. f) tohoto nařízení, zajistit, aby takové údaje byly zpracovávány způsobem, který zajistí jejich náležité zabezpečení, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením, a musí být schopen doložit, že je tato zásada dodržována.

51 Je třeba rovněž uvést, že jak čl. 24 odst. 1 GDPR ve spojení s bodem 74 odůvodnění tohoto nařízení, tak čl. 32 odst. 1 tohoto nařízení ukládají správci, aby v souvislosti s jakýmkoliv zpracováním osobních údajů prováděným tímto správcem nebo pro něj, zavedl vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s uvedeným nařízením.

52 Ze znění čl. 5 odst. 2, čl. 24 odst. 1 a čl. 32 odst. 1 GDPR jednoznačně vyplývá, že důkazní břemeno ohledně toho, že osobní údaje jsou zpracovávány způsobem, který zajistí jejich náležité zabezpečení ve smyslu čl. 5 odst. 1 písm. f) a článku 32 tohoto nařízení, nese dotyčný správce [obdobně viz rozsudky ze dne 4. května 2023, Bundesrepublik Deutschland (Elektronická soudní schránka), C-60/22, EU:C:2023:373, body 52 a 53, jakož i ze dne 4. července 2023, Meta Platforms a další (Všeobecné podmínky používání sociální sítě), C-252/21, EU:C:2023:537, bod 95].

53 Tyto tři články tak stanoví obecně použitelné pravidlo, které je třeba použít, není-li v GDPR stanoveno jinak, rovněž v rámci žaloby na náhradu újmy na základě článku 82 tohoto nařízení.

54 Zadruhé je třeba konstatovat, že předchozí doslovný výklad je podpořen zohledněním cílů sledovaných GDPR.

55 Na jedné straně, jelikož úroveň ochrany podle GDPR závisí na bezpečnostních opatřeních přijatých správci osobních údajů, musí být tito správci na základě toho, že nesou důkazní břemeno ohledně vhodnosti těchto opatření, motivováni k tomu, aby učinili vše, co je v jejich silách, aby zabránili provádění operací zpracování, které nejsou v souladu s tímto nařízením.

56 Na druhé straně, pokud by bylo třeba mít za to, že důkazní břemeno ohledně vhodnosti uvedených opatření nesou subjekty údajů, které jsou definovány v čl. 4 bodě 1 GDPR, vyplývalo by z toho, že právo na náhradu újmy stanovené v čl. 82 odst. 1 tohoto nařízení by bylo zbaveno podstatné části svého užitečného účinku, přestože unijní normotvůrce zamýšlel posílit jak práva těchto subjektů, tak povinnosti správců ve srovnání s ustanoveními předcházejícími tomuto nařízení, jak uvádí bod 11 odůvodnění tohoto nařízení.

57 Na první část třetí otázky je tedy třeba odpovědět tak, že zásada odpovědnosti správce, která je uvedena v čl. 5 odst. 2 GDPR a konkretizována v jeho článku 24, musí být vykládána v tom smyslu, že v rámci žaloby na náhradu újmy na základě článku 82 tohoto nařízení nese dotčený správce důkazní břemeno ohledně vhodnosti bezpečnostních opatření, která provedl podle článku 32 uvedeného nařízení.

K druhé části třetí otázky

58 Podstatou druhé části třetí otázky předkládajícího soudu je, zda článek 32 GDPR a zásada efektivity unijního práva musí být vykládány v tom smyslu, že za účelem posouzení vhodnosti bezpečnostních opatření, která správce provedl na základě tohoto článku, představuje znalecký posudek nezbytný a dostatečný důkazní prostředek.

59 V tomto ohledu je nutno připomenout, že podle ustálené judikatury je při neexistenci unijních pravidel v dané oblasti na vnitrostátním právním řádu každého členského státu, aby na základě zásady procesní autonomie upravil procesní podmínky soudních řízení určených k zajištění ochrany práv jednotlivců, avšak za podmínky, že tyto podmínky nejsou v situacích, na které se uplatní unijní právo, méně příznivé než v podobných situacích podléhajících vnitrostátnímu právu (zásada rovnocennosti) a v praxi neznemožňují nebo nadměrně neztěžují výkon práv přiznaných unijním právem (zásada efektivity) [rozsudek ze dne 4. května 2023, Österreichische Post (Nehmotná újma související se zpracováním osobních údajů), C-300/21, EU:C:2023:370, bod 53 a citovaná judikatura].

60 V projednávaném případě je třeba uvést, že GDPR nestanoví pravidla týkající se přípustnosti a důkazní hodnoty takového důkazního prostředku, jako je znalecký posudek, která musí být uplatňována vnitrostátními soudy, jež rozhodují o žalobě na náhradu újmy na základě článku 82 tohoto nařízení a jejichž úkolem je s ohledem na článek 32 tohoto nařízení posoudit vhodnost bezpečnostních opatření, která dotyčný správce provedl. V souladu s tím, co bylo připomenuto v předchozím bodě tohoto rozsudku, a při neexistenci pravidel unijního práva v dané oblasti, je tudíž na vnitrostátním právním řádu každého členského státu, aby stanovil podmínky žalob určených k zajištění ochrany práv, která jednotlivcům vyplývají z tohoto článku 82, a zejména pravidla týkající se důkazních prostředků, které umožňují posoudit vhodnost takových opatření v tomto kontextu, s výhradou dodržení uvedených zásad rovnocennosti a efektivity [obdobně viz rozsudky ze dne 21. června 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, bod 297, jakož i ze dne 4. května 2023, Österreichische Post (Nehmotná újma související se zpracováním osobních údajů), C-300/21, EU:C:2023:370, bod 54].

61 V tomto řízení nemá Soudní dvůr k dispozici žádné poznatky, které by mohly vyvolat pochybnosti o dodržení zásady rovnocennosti. Jinak je tomu, pokud jde o soulad se zásadou efektivity, jelikož samotné znění druhé části třetí otázky uvádí použití znaleckého posudku jako „nezbytného a dostatečného důkazního prostředku“.

62 Konkrétně vnitrostátní procesní pravidlo, podle kterého by bylo systematicky „nezbytné“, aby vnitrostátní soudy nařizovaly pořízení znaleckého posudku, může být v rozporu se zásadou efektivity. Systematické využívání takového posudku se totiž může jevit jako nadbytečné s ohledem na ostatní důkazy, které má soud, jemuž byla věc předložena, k dispozici, zejména – jak uvedla bulharská vláda ve svém písemném vyjádření – s ohledem na výsledky kontroly dodržování opatření na ochranu osobních údajů, kterou provedl nezávislý orgán zřízený zákonem, za předpokladu, že tato kontrola proběhla nedávno, neboť v souladu s čl. 24 odst. 1 GDPR musí být uvedená opatření podle potřeby revidována a aktualizována.

63 Kromě toho, jak uvedla Evropská komise ve svém písemném vyjádření, zásada efektivity by mohla být porušena v případě, že by výraz „dostatečný“ měl být chápán tak, že znamená, že vnitrostátní soud musí výhradně nebo automaticky vyvodit ze znaleckého posudku, že bezpečnostní opatření provedená dotčeným správcem jsou „vhodná“ ve smyslu článku 32 GDPR. Ochrana práv přiznaných tímto nařízením, k níž směřuje uvedená zásada efektivity, a zejména právo na

účinnou soudní ochranu vůči správci, které je zaručeno v čl. 79 odst. 1 tohoto nařízení, přitom vyžadují, aby nestranný soud provedl objektivní posouzení vhodnosti dotyčných opatření, namísto toho, aby se omezil na takovou dedukci (v tomto smyslu viz rozsudek ze dne 12. ledna 2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, EU:C:2023:2, bod 50).

64 S ohledem na výše uvedené důvody je třeba na druhou část třetí otázky odpovědět tak, že článek 32 GDPR a zásada efektivity unijního práva musí být vykládány v tom smyslu, že za účelem posouzení vhodnosti bezpečnostních opatření, která správce provedl na základě tohoto článku, nemůže znalecký posudek představovat systematicky nezbytný a dostatečný důkazní prostředek.

Ke čtvrté otázce

65 Podstatou čtvrté otázky předkládajícího soudu je, zda čl. 82 odst. 3 GDPR musí být vykládán v tom smyslu, že je správce zproštěn své povinnosti nahradit újmu způsobenou osobě na základě čl. 82 odst. 1 a 2 tohoto nařízení pouze na základě skutečnosti, že tato újma byla způsobena neoprávněným poskytnutím nebo zpřístupněním osobních údajů „třetími stranami“ ve smyslu čl. 4 bodu 10 uvedeného nařízení.

66 Úvodem je třeba upřesnit, že z čl. 4 bodu 10 GDPR vyplývá, že postavení „třetí strany“ mají mimo jiné osoby jiné než ty přímo podléhající správci nebo zpracovateli, jež jsou oprávněny ke zpracování osobních údajů. Tato definice se vztahuje na osoby, které nejsou zaměstnanci správce a nejsou pod jeho kontrolou, jako jsou osoby uvedené v položené otázce.

67 Dále je třeba v první řadě připomenout, že čl. 82 odst. 2 GDPR stanoví, že „správce zapojený do zpracování je odpovědný za újmu, kterou způsobí zpracováním, jež porušuje toto nařízení“, a že odstavec 3 tohoto článku stanoví, že správce nebo zpracovatel jsou této odpovědnosti zproštěni, „pokud prokáží, že nenesou žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla“.

68 Kromě toho bod 146 odůvodnění GDPR, který se týká konkrétně článku 82 tohoto nařízení, ve své první a druhé větě uvádí, že „[v]eškerou újmu, která může osobám vzniknout v důsledku zpracování, které porušuje toto nařízení, by měl nahradit správce nebo zpracovatel“, avšak tento správce nebo zpracovatel by „měl být odpovědnosti zproštěn, pokud prokáže, že za újmu nenese žádným způsobem odpovědnost“.

69 Z těchto ustanovení vyplývá, že dotčený správce musí v zásadě nahradit újmu způsobenou porušením tohoto nařízení souvisejícím s tímto zpracováním a kromě toho může být odpovědnosti zproštěn pouze, pokud prokáže, že nenese žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.

70 Jak tedy vyplývá z výslovného doplnění příslovečného určení „žádným způsobem“ v průběhu legislativního procesu, okolnosti, za kterých se správce může domáhat zproštění občanskoprávní odpovědnosti, kterou má na základě článku 82 GDPR, musí být striktně omezeny na okolnosti, kdy je tento správce schopen prokázat, že mu nelze přičíst odpovědnost za újmu.

71 Pokud stejně jako v projednávané věci bylo porušení zabezpečení osobních údajů ve smyslu čl. 4 bodu 12 GDPR spácháno pachateli kybernetické kriminality, a tedy „třetími stranami“ ve smyslu čl. 4 bodu 10 tohoto nařízení, nelze toto porušení přičítat správci, ledaže tento správce umožnil uvedené porušení tím, že porušil povinnost stanovenou GDPR, zejména povinnost ochrany údajů, kterou má na základě čl. 5 odst. 1 písm. f) a článků 24 a 32 téhož nařízení.

72 V případě porušení zabezpečení osobních údajů třetí stranou se tak správce může zprostit odpovědnosti na základě čl. 82 odst. 3 GDPR tím, že prokáže, že neexistuje žádná příčinná souvislost mezi jeho případným porušením povinnosti ochrany údajů a újmou způsobenou fyzické osobě.

73 V druhé řadě výše uvedený výklad tohoto čl. 82 odst. 3 je rovněž v souladu s cílem GDPR, který spočívá v zajištění vysoké úrovně ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů, který je uveden v bodech 10 a 11 odůvodnění tohoto nařízení.

74 S ohledem na všechny tyto úvahy je třeba na čtvrtou otázku odpovědět tak, že čl. 82 odst. 3 GDPR musí být vykládán v tom smyslu, že správce nemůže být zproštěn své povinnosti nahradit újmu způsobenou osobě na základě čl. 82 odst. 1 a 2 tohoto nařízení pouze na základě skutečnosti, že tato újma byla způsobena neoprávněným poskytnutím nebo zpřístupněním osobních údajů „třetími stranami“ ve smyslu čl. 4 bodu 10 uvedeného nařízení, přičemž uvedený správce musí prokázat, že nenese žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.

K páté otázce

75 Podstatou páté otázky předkládajícího soudu je, zda čl. 82 odst. 1 GDPR musí být vykládán v tom smyslu, že obava z možného zneužití osobních údajů třetími stranami, kterou má subjekt údajů v důsledku porušení tohoto nařízení, může sama o sobě představovat „nehmotnou újmu“ ve smyslu tohoto ustanovení.

76 Pokud jde zaprvé o znění čl. 82 odst. 1 GDPR, je třeba poznamenat, že toto ustanovení stanoví, že „[k]dokoli, kdo v důsledku porušení tohoto nařízení utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy“.

77 V tomto ohledu Soudní dvůr uvedl, že ze znění čl. 82 odst. 1 GDPR jasně vyplývá, že existence „utrpěné“ „újmy“ je jednou z podmínek práva na náhradu újmy stanoveného v uvedeném ustanovení, stejně jako existence porušení GDPR a příčinné souvislosti mezi touto újmou a tímto porušením, přičemž tyto tři podmínky jsou kumulativní [rozsudek ze dne 4. května 2023, Österreichische Post (Nehmotná újma související se zpracováním osobních údajů), C-300/21, EU:C:2023:370, bod 32].

78 Kromě toho Soudní dvůr na základě doslovného, systematického i teleologického hlediska vyložil čl. 82 odst. 1 GDPR v tom smyslu, že brání vnitrostátnímu pravidlu nebo praxi, které náhradu „nehmotné újmy“ ve smyslu tohoto ustanovení podmiňují tím, že újma, kterou utrpěl subjektu údajů, dosáhla určité míry závažnosti [rozsudek ze dne 4. května 2023, Österreichische Post (Nehmotná újma související se zpracováním osobních údajů), C-300/21, EU:C:2023:370, bod 51].

79 Po tomto připomenutí je třeba v projednávané věci zdůraznit, že čl. 82 odst. 1 GDPR nerozlišuje mezi případy, kdy v důsledku prokázaného porušení ustanovení tohoto nařízení je „nehmotná újma“ tvrzená subjektem údajů spojena se zneužitím jeho osobních údajů třetími stranami, ke kterému již došlo ke dni podání návrhu na náhradu újmy, nebo je spojena s obavou tohoto subjektu, že k takovému zneužití může v budoucnu dojít.

80 Znění čl. 82 odst. 1 GDPR tedy nevylučuje, aby pojem „nehmotná újma“ uvedený v tomto ustanovení zahrnoval takovou situaci, jako je situace uvedená předkládajícím soudem, kdy subjekt údajů za účelem získání náhrady újmy na základě tohoto ustanovení argumentuje svojí obavou, že jeho osobní údaje budou v budoucnu zneužity třetími stranami v důsledku porušení tohoto nařízení, k němuž došlo.

81 Tento doslovný výklad je zadruhé podpořen bodem 146 odůvodnění GDPR, který se týká konkrétně práva na náhradu újmy stanoveného v čl. 82 odst. 1 tohoto nařízení a ve třetí větě uvádí, že „výklad pojmu ‚újma‘ by měl být široký a opírat se o judikaturu Soudního dvora při plném zohlednění cílů tohoto nařízení“. Výklad pojmu „nehmotná újma“ ve smyslu tohoto čl. 82 odst. 1, který by nezahrnoval situace, kdy se subjekt údajů dotčený porušením uvedeného nařízení dovolává obavy, že jeho osobní údaje budou v budoucnu zneužity, by přitom neodpovídal širokému pojetí tohoto pojmu, jak jej zamýšlel unijní normotvůrce [obdobně viz rozsudek ze dne 4. května 2023, Österreichische Post (Nehmotná újma související se zpracováním osobních údajů), C-300/21, EU:C:2023:370, body 37 a 46].

82 Kromě toho první věta bodu 85 odůvodnění GDPR uvádí, že „[n]ení-li porušení zabezpečení osobních údajů řešeno náležitě a včas, může to fyzickým osobám způsobit fyzickou, hmotnou či nehmotnou újmu, jako je ztráta kontroly nad jejich osobními údaji nebo omezení jejich práv, diskriminace, krádež nebo zneužití identity, finanční ztráta, […] nebo jakékoliv jiné významné hospodářské či společenské znevýhodnění dotčených fyzických osob“. Z tohoto demonstrativního výčtu „škod“ nebo „újem“, které mohou subjektům údajů vzniknout, vyplývá, že unijní normotvůrce zamýšlel pod tyto pojmy zahrnout zejména pouhou „ztrátu kontroly“ nad jejich vlastními údaji v důsledku porušení tohoto nařízení, a to i v případě, že nedošlo ke skutečnému zneužití dotčených údajů na úkor uvedených osob.

83 Zatřetí a nakonec výklad uvedený v bodě 80 tohoto rozsudku je podpořen cíli GDPR, které je třeba plně zohlednit při definování pojmu „újma“, jak uvádí bod 146 třetí věta odůvodnění tohoto nařízení. Výklad čl. 82 odst. 1 GDPR, podle kterého by pojem „nehmotná újma“ ve smyslu tohoto ustanovení nezahrnoval situace, kdy se subjekt údajů argumentuje pouze svoji obavou, že jeho údaje budou v budoucnu zneužity třetími stranami, by přitom nebyl v souladu se zárukou vysoké úrovně ochrany fyzických osob v souvislosti se zpracováním osobních údajů v rámci Unie, na kterou se tento nástroj vztahuje.

84 Je však třeba zdůraznit, že subjekt dotčený porušením GDPR, které mělo pro něj negativní důsledky, je povinen prokázat, že tyto důsledky představují nehmotnou újmu ve smyslu článku 82 tohoto nařízení [v tomto smyslu viz rozsudek ze dne 4. května 2023, Österreichische Post (Nehmotná újma související se zpracováním osobních údajů), C-300/21, EU:C:2023:370, bod 50].

85 Konkrétně pokud subjekt údajů domáhající se na tomto základě náhrady újmy argumentuje obavou, že v budoucnu dojde ke zneužití jeho osobních údajů v důsledku takového porušení, musí vnitrostátní soud, jemuž byla věc předložena, ověřit, že tato obava může být za konkrétních okolností a ve vztahu k subjektu údajů považována za opodstatněnou.

86 S ohledem na výše uvedené důvody je třeba na pátou otázku odpovědět tak, že čl. 82 odst. 1 GDPR musí být vykládán v tom smyslu, že obava z možného zneužití osobních údajů třetími stranami, kterou má subjekt údajů v důsledku porušení tohoto nařízení, může sama o sobě představovat „nehmotnou újmu“ ve smyslu tohoto ustanovení.

K nákladům řízení

87 Vzhledem k tomu, že řízení má, pokud jde o účastníky původního řízení, povahu incidenčního řízení ve vztahu ke sporu probíhajícímu před předkládajícím soudem, je k rozhodnutí o nákladech řízení příslušný uvedený soud. Výdaje vzniklé předložením jiných vyjádření Soudnímu dvoru než vyjádření uvedených účastníků řízení se nenahrazují.

Z těchto důvodů Soudní dvůr (třetí senát) rozhodl takto:

1) **Články 24 a 32 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)**

   musí být vykládány v tom smyslu, že

   samotná skutečnost, že došlo k neoprávněnému poskytnutí nebo zpřístupnění osobních údajů „třetími stranami“ ve smyslu čl. 4 bodu 10 tohoto nařízení nepostačuje k tomu, aby bylo možné mít za to, že technická a organizační opatření zavedená dotčeným správcem nejsou „vhodná“ ve smyslu těchto článků 24 a 32.

2) **Článek 32 nařízení 2016/679**

   musí být vykládán v tom smyslu, že

   vhodnost technických a organizačních opatření zavedených správcem na základě tohoto článku musí být vnitrostátními soudy posuzována konkrétně se zohledněním rizik spojených s dotyčným zpracováním, přičemž posoudí, zda povaha, obsah a provádění těchto opatření odpovídají těmto rizikům.

3) **Zásada odpovědnosti správce, která je uvedena v čl. 5 odst. 2 nařízení 2016/679 a konkretizována v jeho článku 24,**

   musí být vykládána v tom smyslu, že

   v rámci žaloby na náhradu újmy na základě článku 82 GDPR nese dotčený správce důkazní břemeno ohledně vhodnosti opatření, která provedl podle článku 32 uvedeného nařízení.

4) **Článek 32 nařízení 2016/679 a zásada efektivity unijního práva**

   musí být vykládány v tom smyslu, že

   za účelem posouzení vhodnosti bezpečnostních opatření, která správce provedl na základě tohoto článku, nemůže znalecký posudek představovat systematicky nezbytný a dostatečný důkazní prostředek.

5) **Článek 82 odst. 3 nařízení 2016/679**

   musí být vykládán v tom smyslu, že

správce nemůže být zproštěn své povinnosti nahradit újmu způsobenou osobě na základě čl. 82 odst. 1 a 2 tohoto nařízení pouze na základě skutečnosti, že tato újma byla způsobena neoprávněným poskytnutím nebo zpřístupněním osobních údajů „třetími stranami“ ve smyslu čl. 4 bodu 10 uvedeného nařízení, přičemž uvedený správce musí prokázat, že nenese žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.

6) **Článek 82 odst. 1 nařízení 2016/679**

musí být vykládán v tom smyslu, že

obava z možného zneužití osobních údajů třetími stranami, kterou má subjekt údajů v důsledku porušení tohoto nařízení, může sama o sobě představovat „nehmotnou újmu“ ve smyslu tohoto ustanovení.

Podpisy