

Otázky:

- 1) název osoby, které byla pokuta uložena (případně alespoň sektorové vymezení této osoby, pokud tuto informaci o názvu nelze poskytnout),
- 2) datum udělení sankce;
- 3) výši pokuty; a
- 4) povaha porušení, za které byla pokuta uložena.

1) Výše pokuty 351 000 000,- Kč; rozhodnutí o rozkladu vydáno dne: 10. dubna 2024**Výrok:**

Společnost vyvíjející antivirový software (dále též jen „obviněná“)

- I. je vinna, že jako správce osobních údajů podle čl. 4 bodu 7) nařízení (EU) 2016/679 předávala osobní údaje uživatelů antivirového programu [REDACTED] a jeho rozšíření internetových prohlížečů společnosti [REDACTED], [REDACTED], (dále jen „společnost [REDACTED]“, za účelem tvorby statistické analýzy trendů, přestože k tomuto zpracování jí nesvědčil právní titul ve smyslu čl. 6 odst. 1 nařízení (EU) 2016/679, a to nejméně od nezjištěného dne v dubnu 2019 do nezjištěného dne v červenci 2019, tedy nejméně po dobu celých dvou kalendářních měsíců, čímž porušila základní zásadu pro zpracování osobních údajů podle čl. 6 odst. 1 nařízení (EU) 2016/679, tedy zásadu, dle které je zpracování osobních údajů zákonné pouze pokud je splněna nejméně jedna z podmínek uvedených v tomto ustanovení, a tím spáchala přestupek podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb.,
- II. je vinna, že v souvislosti s předáváním osobních údajů společnosti [REDACTED] jako správce osobních údajů podle čl. 4 bodu 7) nařízení (EU) 2016/679 v okamžiku získání osobních údajů nedostatečně informovala subjekty údajů (uživatelé antivirového programu [REDACTED] a jeho rozšíření internetových prohlížečů) o účelech zpracování, pro které jsou osobní údaje určeny, a právním základem pro zpracování, a to nejméně od nezjištěného dne v dubnu 2019 do nezjištěného dne v červenci 2019, tedy nejméně po dobu celých dvou kalendářních měsíců, čímž porušila povinnost podle čl. 13 odst. 1 písm. c) nařízení (EU) 2016/679, tedy povinnost poskytnout subjektu údajů v okamžiku získání osobních údajů informace uvedené v tomto ustanovení, a tím spáchala přestupek podle § 62 odst. 1 písm. c) zákona č. 110/2019 Sb.,
- III. za což se jí v souladu s čl. 83 odst. 5 nařízení (EU) 2016/679 ukládá

pokuta ve výši 351.000.000 Kč Kč


(slovy tři sta padesát jeden milion korun českých)

- IV. a dále podle § 95 odst. 1 zákona č. 250/2016 Sb. povinnost nahradit náklady řízení ve výši 1.000 Kč,
- V. obojí splatné do 30 dnů ode dne nabytí právní moci tohoto rozhodnutí bezhotovostním převodem na účet Úřadu vedený u ČNB, č. ú. 19-5825001/0710, variabilní symbol IČO obviněné, konstantní symbol 1148.

2) Výše pokuty 898 000,-Kč; příkaz vydán den 23. června 2023


Výrok:

I. Mobilní operátor (dále jen „obviněná“)

1. je vinna, že jako správce osobních údajů osob navštěvujících webové stránky  (dále též jako „subjekty údajů“) podle čl. 4 bodu 7 nařízení (EU) 2016/679 zpracovávala nejméně ke dni 25. dubna 2023 osobní údaje subjektů údajů prostřednictvím datových informací s názvem „_uetsid“, „_uetsid_exp“, „_uetvid“, „_uetvid_exp“ a „MUID“ ukládaných do koncových zařízení subjektů údajů nebo sloužících k následnému přístupu k údajům uloženým v koncových zařízeních subjektů údajů bez jejich předchozího souhlasu ve smyslu § 89 odst. 3 zákona č. 127/2005 Sb., zákona o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, (dále jen „zákon č. 127/2005 Sb.“), přičemž tyto datové informace nesloužily výhradně pro technické ukládání nebo přístup pro potřeby přenosu zprávy prostřednictvím sítě elektronických komunikací, ani nebyly nezbytné pro potřeby poskytování služby informační společnosti, výslovně subjekty údajů vyžádané ve smyslu § 89 odst. 3 věty druhé zákona č. 127/2005 Sb.,


čímž porušila základní zásadu zpracování osobních údajů stanovenou v čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679, tedy zásadu, že osobní údaje ve vztahu k subjektu údajů musí být zpracovávány zákonným způsobem („zákonost“),

a tím spáchala přestupek podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb.,

2. je vinna, že jako správce osobních údajů osob navštěvujících webové stránky  (dále též jako „subjekty údajů“) podle čl. 4 bodu 7 nařízení (EU) 2016/679 zpracovávala nejméně ke dni 25. dubna 2023 osobní údaje subjektů údajů prostřednictvím datových informací s názvem „personalization_id“, „uuid2“, „uid“, „sid“, „guest_id_marketing“, „muc_ads“, „guest_id_ads“ a „anj“ ukládaných do koncových zařízení subjektů údajů nebo sloužících k následnému přístupu k údajům uloženým v koncových zařízeních subjektů údajů na základě souhlasu, který nesplňoval podmínku informovanosti podle čl. 4 odst. 11 nařízení (EU) 2016/679, tedy bez platného předchozího souhlasu ve smyslu § 89 odst. 3 zákona č. 127/2005 Sb., přičemž tyto datové informace nesloužily výhradně pro technické ukládání nebo přístup pro potřeby přenosu zprávy prostřednictvím sítě elektronických komunikací, ani nebyly nezbytné pro potřeby poskytování služby informační společnosti, výslovně subjekty údajů vyžádané ve smyslu § 89 odst. 3 věty druhé zákona č. 127/2005 Sb.,

čímž porušila povinnost stanovenou v čl. 6 odst. 1 nařízení (EU) 2016/679, tedy povinnost zpracovávat osobní údaje pouze na základě některého právního důvodu upraveného v písm. a) až f) tohoto ustanovení,

a tím spáchala přestupek podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb.,

3. je vinna, že jako správce osobních údajů osob navštěvujících webové stránky , podle čl. 4 bodu 7 nařízení (EU) 2016/679, nejméně ke dni 25. dubna 2023 neuvedla účel, právní základ a dobu zpracování osobních údajů prováděného prostřednictvím datových informací s názvem „_uetsid“, „_uetsid_exp“, „_uetvid“, „_uetvid_exp“ a „MUID“ ukládaných do koncových zařízení subjektů údajů nebo sloužících k následnému přístupu k údajům uloženým v koncových zařízeních subjektů údajů bez jejich předchozího souhlasu ve smyslu § 89 odst. 3 zákona č. 127/2005 Sb., přičemž tyto datové informace nesloužily výhradně pro technické ukládání nebo přístup pro potřeby přenosu zprávy prostřednictvím sítě elektronických komunikací, ani nebyly nezbytné pro potřeby poskytování služby informační společnosti, výslovně subjekty údajů vyžádané ve smyslu § 89 odst. 3 věty druhé zákona č. 127/2005 Sb.,

čímž porušila čl. 13 odst. 1 písm. c) a odst. 2 písm. a) nařízení (EU) 2016/679, tedy právo subjektu údajů, aby mu správce v okamžiku získání osobních údajů subjektu údajů poskytl informaci o účelech zpracování, pro které jsou osobní údaje určeny, o právním základu pro zpracování a o době, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, o kritériích použitých pro stanovení této doby,


a tím spáchala přestupek podle § 62 odst. 1 písm. c) zákona č. 110/2019 Sb.,


4. za což se jí podle § 41 zákona č. 250/2016 Sb. a v souladu s čl. 83 odst. 5 písm. a) a b) nařízení (EU) 2016/679 ukládá



pokuta ve výši 898.000 Kč

(slovy osm set devadesát osm tisíc korun českých)

splatná do 30 dnů ode dne nabytí právní moci tohoto příkazu bezhotovostním převodem na účet vedený u ČNB, č.ú. 19-5825001/0710, variabilní symbol IČO obviněné, konstantní symbol 1148.

- II. Obviněné se podle čl. 58 odst. 2 písm. d) nařízení (EU) 2016/679 nařizuje, aby operace zpracování osobních údajů, prováděné v souvislosti s provozem webových stránek , prostřednictvím datových informací ukládaných do koncových zařízení subjektů údajů nebo sloužících k následnému přístupu k údajům uloženým v koncových zařízeních subjektů údajů bez jejich předchozího souhlasu ve smyslu § 89 odst. 3 zákona č. 127/2005 Sb., (dále jen „soubory cookie“) které neslouží výhradně pro technické ukládání nebo přístup pro potřeby přenosu zprávy prostřednictvím sítě elektronických komunikací, ani nebyly nezbytné pro potřeby poskytování služby informační společnosti, výslovně subjekty údajů vyžádané ve smyslu § 89 odst. 3 věty druhé zákona č. 127/2005 Sb., (dále jen „netechnické soubory cookie“), uvedla do souladu s nařízením (EU) 2016/679 tak, že:


1. ukončí zpracování osobních údajů prováděné prostřednictvím těch netechnických souborů cookie, které byly do koncových zařízení užívaných subjekty údajů instalovány v souvislosti s prohlížením webové stránky  bez prokazatelného předem získaného souhlasu subjektů údajů k jejich uložení a přístupu k nim,

2. poskytne osobám navštěvujícím webové stránky  veškeré informace o zpracování osobních údajů prostřednictvím souborů cookie, které je správce povinen poskytnout subjektům údajů podle čl. 13 odst. 1 a 2 nařízení (EU) 2016/679, zejména informace o účelu a právním základu zpracování a o době zpracování osobních údajů prováděného prostřednictvím souborů cookie,
3. poskytne osobám navštěvujícím webové stránky  veškeré informace o zpracování osobních údajů prostřednictvím souborů cookies, které je správce povinen poskytnout subjektům údajů podle čl. 13 odst. 1 a 2 nařízení (EU) 2016/679 tak, aby bylo subjektům údajů umožněno udělit souhlas se zpracováním jejich osobních údajů, který bude platný,


a to ve lhůtě 30 dnů od právní moci tohoto příkazu,
4. Úřadu pro ochranu osobních údajů podá zprávu o splnění uložených opatření uvedených ve výroku II.1. a II.2. tohoto příkazu, a to ve lhůtě 14 dnů od splnění.

3) Výše pokuty 602 000,- Kč; příkaz vydán den 18. července 2023

Výrok:

- I. Společnost provozující lékárenskou síť (dále jen „obviněná“)
 1. je vinna, že jako správce osobních údajů osob navštěvujících webové stránky  (dále též jako „subjekty údajů“) podle čl. 4 bodu 7 nařízení (EU) 2016/679 zpracovávala nejméně ke dni 14. června 2023 osobní údaje subjektů údajů prostřednictvím souborů cookie s názvem „lux_uid“ bez předchozího souhlasu subjektů údajů k uložení těchto souborů cookie do jimi užívaných koncových zařízení a k následnému přístupu k němu ve smyslu § 89 odst. 3 zákona č. 127/2005 Sb., zákona o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, (dále jen „zákon č. 127/2005 Sb.“)


čímž porušila základní zásadu zpracování osobních údajů stanovenou v čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679, tedy zásadu, že osobní údaje ve vztahu k subjektu údajů musí být zpracovávány zákonným způsobem („zákonost“),

a tím spáchala přestupek podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb.,
 2. je vinna, že jako správce osobních údajů osob navštěvujících webové stránky , podle čl. 4 bodu 7 nařízení (EU) 2016/679, neuvedla účel zpracování osobních údajů prováděného prostřednictvím datových informací s názvem „_ga_QCVLHVXRSN,G-BX1XHL8Y5P“ (x2), „13WakrfVbNJBaAmhQtEeDv-config“, „13WakrfVbNJBaAmhQtEeDv-query“, „deviceCache“, „feedbotConversationId“, „glide_language“, „meiro_checkout_data“, „sentryReplaySession“ a „nWC1Uzs7EI“ ukládaných do koncových zařízení subjektů údajů nebo sloužících k následnému přístupu k údajům uloženým v koncových zařízeních subjektů, přičemž tyto datové informace nesloužily výhradně pro technické ukládání nebo přístup pro potřeby přenosu zprávy prostřednictvím sítě elektronických komunikací, ani nebyly nezbytné pro potřeby

poskytování služby informační společnosti, výslovně subjekty údajů vyžádané ve smyslu § 89 odst. 3 věty druhé zákona č. 127/2005 Sb.,

čímž porušila čl. 13 odst. 1 písm. c) nařízení (EU) 2016/679, tedy právo subjektu údajů, aby mu správce v okamžiku získání osobních údajů subjektu údajů poskytl informaci o účelech zpracování, pro které jsou osobní údaje určeny,

a tím spáchala přestupek podle § 62 odst. 1 písm. c) zákona č. 110/2019 Sb.,

3. je vinna, že jako správce osobních údajů osob navštěvujících webové stránky , podle čl. 4 bodu 7 nařízení (EU) 2016/679, nejméně ke dni 14. června 2023 neuvedla v českém jazyce účel zpracování osobních údajů prováděného prostřednictvím souborů cookie s názvem „AWSALBCORS“, „rc::a“, „rc::c“, „bounce“, „FPID“, „FPLC“, „td“, „_uetid“, „anj“, „MR“, „tv_UICR“ a „tvid“,


čímž porušila čl. 12 odst. 1 nařízení (EU) 2016/679, tedy právo subjektu údajů, aby správce přijal vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v člancích 13 a 14 a učinil veškerá sdělení podle článků 15 až 22 a 34 o zpracování, informace poskytne písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě,



a tím spáchala přestupek podle § 62 odst. 1 písm. c) zákona č. 110/2019 Sb.,


4. za což se jí podle § 41 zákona č. 250/2016 Sb. a v souladu s čl. 83 odst. 5 písm. a) a b) nařízení (EU) 2016/679 ukládá

pokuta ve výši 602.000 Kč
(slovy šest set dva tisíce korun českých)

splatná do 30 dnů ode dne nabytí právní moci tohoto příkazu bezhotovostním převodem na účet vedený u ČNB, č.ú. 19-5825001/0710, variabilní symbol IČ obviněné, konstantní symbol 1148.

- II. Obviněné se podle čl. 58 odst. 2 písm. d) nařízení (EU) 2016/679 nařizuje, aby operace zpracování osobních údajů, prováděné v souvislosti s provozem webových stránek , uvedla do souladu s nařízením (EU) 2016/679 tak, že:

1. ukončí zpracování osobních údajů prováděné prostřednictvím těch souborů cookie, které byly do koncových zařízení užívaných subjekty údajů instalovány v souvislosti s prohlížením webové stránky  bez prokazatelného předem získaného souhlasu subjektů údajů k jejich uložení a přístupu k nim a nesplňují podmínky § 89 odst. 3 věty druhé zákona č. 127/2005 Sb.,
2. poskytne osobám navštěvujícím webové stránky  veškeré informace o zpracování osobních údajů prostřednictvím souborů cookie, které je správce povinen poskytnout subjektům údajů podle čl. 13 odst. 1 a 2 nařízení (EU) 2016/679,

3. veškeré informace o zpracování osobních údajů prostřednictvím souborů cookie, které je správce povinen poskytnout subjektům údajů podle čl. 13 odst. 1 nařízení (EU) 2016/679, včetně informace o účelu ve vztahu k používaným souborům cookie na webových stránkách  zveřejní v českém jazyce,

a to ve lhůtě 30 dnů od právní moci tohoto příkazu,

4. Úřadu pro ochranu osobních údajů podá zprávu o splnění uložených opatření uvedených ve výroku II.1., 2. a 3. tohoto příkazu, a to ve lhůtě 14 dnů od splnění.

4) Výše pokuty 309 000,- Kč; rozhodnutí o rozkladu vydáno dne 7. srpna 2023

Výrok:

Společnost provozující specializovaná zdravotnická zařízení (dále jen „obviněná“), jako správce osobních údajů přibližného počtu 58 zaměstnanců a 247.000 pacientů podle čl. 4 bodu 7 nařízení (EU) 2016/679 (dále jen „subjekty údajů“),

I. je vinna, že od spáchání kybernetického útoku dne 14. března 2021 do zahájení tohoto řízení nedoložila, že by ve smyslu čl. 34 nařízení (EU) 2016/679, jež promítá zásadu transparentnosti dle čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679, oznámila porušení zabezpečení osobních údajů následkem kybernetického útoku na servery, na kterých měla uložené databáze s osobními údaji subjektů údajů v rozsahu identifikační, kontaktní, ekonomické a finanční údaje, data o poloze a údaje o zdravotním stavu ze dne 14. března 2021 subjektům údajů,

čímž porušila povinnost stanovenou v čl. 5 odst. 2 nařízení (EU) 2016/679, tedy povinnost správce doložit dodržení souladu se základními zásadami uvedenými v odst. 1 daného článku,

a tím spáchala přestupek podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb.,

II. je vinna, že bez zbytečného odkladu po spáchání kybernetického útoku dne 14. března 2021 na servery, na kterých měla uložené databáze s osobními údaji subjektů údajů v rozsahu identifikační, kontaktní, ekonomické a finanční údaje, data o poloze a údaje o zdravotním stavu, až do dne 23. listopadu 2021 neohlásila tento útok Úřadu pro ochranu osobních údajů,

čímž porušila povinnost stanovenou v čl. 33 odst. 1 nařízení (EU) 2016/679, tedy povinnost správce ohlásit dozorovému úřadu jakékoli porušení zabezpečení osobních údajů bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl,

a tím spáchala přestupek podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb.,

III. je vinna, že dokumentace zaznamenávající porušení zabezpečení způsobené kybernetickým útokem dne 14. března 2021 neobsahovala účinky daného porušení, jakožto povinný údaj dle čl. 33 odst. 5 nařízení (EU) 2016/679,

čímž porušila povinnost stanovenou v čl. 33 odst. 5 nařízení (EU) 2016/679, tedy povinnost správce dokumentovat veškeré případy porušení zabezpečení osobních údajů, včetně uvedení skutečností, které se daného porušení týkají, jeho účinky a přijatá nápravná opatření,

a tím spáchala přešupek podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb.,

- IV. za což se jí podle § 41 zákona č. 250/2016 Sb. a v souladu s čl. 83 odst. 4 písm. a) a čl. 83 odst. 5 písm. a) nařízení (EU) 2016/679 ukládá

pokuta ve výši 309.000 Kč
(slovy tři sta devět tisíc korun českých)

- V. a dále podle § 95 odst. 1 zákona č. 250/2016 Sb. a vyhlášky 520/2005 Sb., o rozsahu hotových výdajů a ušlého výdělku, které správní orgán hradí jiným osobám, a o výši paušální částky nákladů řízení, ve znění vyhlášky č. 112/2017 Sb., povinnost nahradit **náklady řízení ve výši 1.000 Kč,**

obojí splatné do 30 dnů ode dne nabytí právní moci tohoto rozhodnutí bezhotovostním převodem na účet vedený u ČNB, č. ú. 19-5825001/0710, variabilní symbol IČO obviněné, konstantní symbol 1148.

5) Výše pokuty 140 000,- Kč; rozhodnutí o rozkladu vydáno dne 3. května 2023
Výrok:

Společnost provozující internetový obchod (dále jen „obviněná“):

I. v období ode dne 31. prosince 2014 nejméně do dne 27. srpna 2017 jako správce osobních údajů svých zákazníků používala k hashování nejméně 735 956 hesel k zákaznickým účtům nedostatečně odolné hashovací algoritmy, a to algoritmus MD5 a algoritmus SHA-1 s kryptografickou solí, přičemž opatření spočívající v resetování stávajících hesel k zákaznickým účtům hashovaných výše uvedenými hashovacími algoritmy a hashování nově vygenerovaných hesel dostatečně odolným hashovacím algoritmem bcrypt provedla až ke dni 27. srpna 2017, poté, co se dozvěděla, že po úniku databáze jejích zákazníků byla hesla zákazníků hashovaná hashovacími algoritmy MD5 a SHA-1 s kryptografickou solí v plně čitelné podobě spolu s dalšími kategoriemi osobních údajů jejích zákazníků nejméně v rozsahu jméno, příjmení a e-mailová adresa zveřejněna neznámou osobou na internetových stránkách www.ulozto.cz,

čímž porušila § 13 odst. 1 zákona č. 101/2000 Sb., podle něhož jsou správce a zpracovatel povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů,

a tím spáchala přešupek podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., podle něhož se právnická nebo podnikající fyzická osoba jako správce nebo zpracovatel dopustí přešupku

tím, že při zpracování osobních údajů nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů (§ 13),

II. za což se jí podle § 35 písm. b) zákona č. 250/2016 Sb. a v souladu s § 45 odst. 3 zákona č. 101/2000 Sb. ukládá

pokuta ve výši 140 000 Kč
(slovy jedno sto čtyřicet tisíc korun českých),

III. a dále podle § 95 odst. 1 zákona č. 250/2016 Sb. povinnost nahradit **náklady řízení ve výši 1 000 Kč**,

obojí splatné do 30 dnů ode dne nabytí právní moci tohoto rozhodnutí bezhotovostním převodem na účet vedený u ČNB, č. ú. 19-5825001/0710, variabilní symbol IČO obviněné, konstantní symbol 1148.