ELEKTRONICKÝ ZPRAVODAJ PRO POVĚŘENCE

HLÍDACÍ PES PRO OSOBY ZODPOVĚDNÉ ZA GDPR | UKÁZKOVÉ ČÍSLO

Změna v ukládání GDPR pokut

Chystají se změny v ukládání pokut za porušení GDPR! Evropský sbor pro ochranu osobních údajů vydal nové pokyny, které mají sjednotit systém sankcí v jednotlivých členských státech EU. Končí tak období mírných pokut v Čechách?

Při pohledu na výši pokut, které se v rámci EU ukládají za porušení GDPR, není žádným tajemstvím, že Česká republika přispívá k celkové výši udělených pokut **opravdu malou měrou**. Ostatně tomuto tématu jsme se věnovali v jednom z našich předchozích **článků**.

Účelem GDPR je však sjednotit nejen právní úpravu, ale i postup při **vynucování a trestání** případného porušení této právní úpravy. Z dlouhodobého hlediska je tak neudržitelné, aby náš podíl na celkovém počtu pokut (a zejména výše průměrné pokuty) zůstal na nižších příčkách. A právě tomuto tématu se věnuje EDPB ve svém návrhu Pokynů č. 4/2022 k **výpočtu výše pokut dle GDPR**, který si můžete přečíst **zde**. Předmětné stanovisko je aktuálně ve fázi připomínkového řízení ze strany veřejnosti, které má skončit 27. června 2022. Není však od věci podívat se, jakým směrem se má toto téma ubírat a na co se můžeme připravit.

Nová pravidla

EDPB přistupuje k ukládání pokut v duchu čl. 83 GDPR, který stanovuje určitá kritéria, k nimž by měl dozorový orgán přihlížet. Kromě například povahy, závažnosti a délky porušení trvání (ovšem s přihlédnutím ke konkrétní operaci zpracování) by měl dozorový orgán zhodnotit i **zaviněnost jednání** kontrolované osoby a taktéž kroky, které osoba přijala pro **zmírnění škod**. Samotných kritérií je více, přičemž dozorový orgán by měl vzít v úvahu i jakékoliv přitěžující nebo polehčující okolnosti.

Ostatně o pokutách jsme se toho načetli už dost. S příchodem GDPR bylo největším tématem právě to, že za každé (byť sebemenší) porušení **hrozí astronomické pokuty**. Pravda však byla trochu jiná a dlužno dodat, že v rámci českého kontextu jsme se vždy mohli cítit kryti závaznou judikaturou nejvyšších soudů, které stanovují požadavky na to, aby pokuta nebyla pro pokutovanou osobu likvidační.

Vše můžeme jednoduše shrnout tak, že aby nějaká právní úprava mohla fungovat, měla by sankce za její nedodržení „bolet“, ale zároveň ne tak, aby porušitele zdecimovala. EDPB pro ulehčení sjednocení přístupu k ukládání pokut stanovil **algoritmus o pěti krocích**, kterým by měl každý dozorový orgán při ukládání pokuty za porušení GDPR projít.

První krok – zhodnocení

Prvním krokem je pochopitelně zhodnocení, co se vlastně stalo a k jakému porušení v rámci GDPR došlo. Dozorový orgán by měl pečlivě zjistit, jaké jsou **skutkové okolnosti porušení** a jaká právní norma byla ve skutečnosti porušena. Důvod je ten, že z okolností může vyplynout skutečnost, že jednáním pokutované osoby došlo k porušení více právních norem. Mohou nastat různé situace, které známe

jako **souběh přestupků**, jenž může být jednočinný či vícečinný a podobně.

Dozorový orgán tak musí zhodnotit, zda skutek lze považovat za **jedno či více pokutovatelných jednání** či zda toto jednání vede k jednomu nebo více porušením (popřípadě se jedná o kolizi porušení, která může vylučovat souběžné pokutování) nebo zda mají být sankce přičteny a podobně. Z povahy věci se jedná o startovací čáru, od níž se bude odvíjet základní rozdělení v druhém kroku.

Druhý krok – klasifikace

Druhý krok je klasifikační – dozorový orgán by měl zhodnotit, do jaké **kategorie porušení GDPR** předmětnou věc zařadí. EDPB tento krok označuje za výchozí bod pro samotný výpočet možné sankce. Dozorový orgán by tak měl zjednodušeně řečeno projít ustanovení čl. 83 (zejména odst. 4 až 6) GDPR, které obsahuje základní klasifikaci možných porušení.

V témže kroku dozorový orgán provede základní klasifikaci tak, aby bylo zřejmé, v jakém **rozsahu možného uložení pokut** se vlastně pohybuje. V tomto duchu by měl dozorový orgán zhodnotit povahu zpracování včetně všech možných aspektů, jako je:

- přeshraniční zpracování,
- účel zpracování,
- počet dotčených osob,
- výše případné škody,
- délka trvání porušení.

Všechny okolnosti totiž vykreslují, nakolik bylo dotčené porušení vlastně škodlivé. EDPB v tomto duchu navrhuje rozmezí, v němž by se pokuta měla pohybovat, přičemž pracuje s **klasifikací podle závažnosti**, kdy rozlišuje nízkou, střední a vysokou závažnost. V případě nízké závažnosti navrhuje ukládat pokuty v rozmezí 0–10 % zákonného maxima, v případě střední závažnosti v rozmezí 10–20 % zákonného maxima a v případě vysoké závažnosti pak v rozmezí 20–100 % zákonného maxima.

GDPR obsahuje vyjádření okruhů, u nichž stanovuje nižší či vyšší hranici porušení. Například správci, jenž pochybí při jmenování pověřence, hrozí pokuta maximálně 10 milionů eur (nebo 2 % celosvětového obratu). Za porušení povinností u práv subjektů údajů (popřípadě u porušení zásad zpracování) mu nicméně hrozí pokuta až 20 milionů eur (nebo 4 % celosvětového obratu).

Poněvadž uložená pokuta má sloužit několika účelům (zejména musí být dostatečně **odrazující, účinná, ale také přiměřená**), měl by se dozorový orgán zabývat majetkovými poměry pokutované osoby. Zjednodušeně řečeno – malý e-shop a nadnárodní korporace by pravděpodobně neměly dostat stejnou pokutu za téže porušení. Majetkové poměry pokutované osoby tak mohou výrazně zasáhnout do výše nastíněného rozmezí, ze kterého by dozorový orgán měl vycházet.

EDPB chce sjednotit trestání porušení GDPR ve všech státech EU

EDPB tak nabízí pro účely tohoto kroku **pravidla pro úpravu sankce dle obratu**. Rozlišuje přitom 6 kategorií, od nichž se odvíjí doporučená úprava výše pokuty (viz tabulka).

Důležité je však uvědomit si základní pravidlo, a sice že čím vyšší je obrat pokutované osoby, **tím vyšší je i výchozí částka**, kterou by dozorový orgán měl brát jako uvažovanou výši pokuty.

Pokud se vám ze všech těch čísel točí hlava, pojďme si to ukázat **na příkladu, který uvádí EDPB**: *„Startup s obratem 500 000 eur prodával citlivé osobní údaje takzvaným data brokerům. Dozorový orgán na základě představeného algoritmu došel k závěru, že se jedná o závažné porušení GDPR – pokutu tak lze udělit v rozmezí 20 % až 100 % maximální částky. Ta v tomto případě činní 20 milionů eur. Bavíme se tedy o pokutě, která se pohybuje v rozmezí od 4 do 20 milionů eur za uvedené jednání. Dozorový orgán však může zvážit (respektive by měl zvážit) otázku, která se týká obratu pokutované osoby – ten totiž činí 500 000 eur. Na základě toho tak může dozorový orgán zvážit snížení této částky na 0,2 %, a to až do výše stanovené výchozí částky odpovídající závažnosti. V tomto případě dozorový orgán došel k tomu, že pokuta ve výši 16 000 eur může být dostatečně odrazující, ale zároveň přiměřená – tato částka tak tvoří základ pro další výpočet, jehož výsledkem by měla být definitivní pokuta, která nepřesahuje hranici 20 milionů eur.“*

Proč je důležité vědět o výše uvedeném, je tak nasnadě – díky těmto informacím můžeme **relativně přesně určit rozmezí**, ve kterém se může předmětná pokuta pohybovat.

PRAVIDLA PRO ÚPRAVU SANKCE DLE OBRATU

Obrat pokutované osoby nepřesahuje:	Dozorové orgány by měly zvážit, zda jako finální sankci stanoví:
2 miliony eur	0,2 % zjištěné částky
10 milionů eur	0,4 % zjištěné částky
50 milionů eur	2 % zjištěné částky
100 milionů eur	10 % zjištěné částky
250 milionů eur	20 % zjištěné částky
Obrat je vyšší než 250 milionů eur	50 % zjištěné částky

Třetí krok – přitěžující a polehčující okolnosti

V třetím kroku (byť tak činí částečně už i v kroku druhém) by dozorový orgán měl zohlednit **přitěžující a polehčující okolnosti**, jež souvisejí s minulým či současným chováním správce či zpracovatele, a zvážit odpovídající snížení či naopak zvýšení pokuty. Dozorový orgán by však neměl přitěžující a polehčující okolnosti přičíst k výsledné pokutě dvakrát (tedy v rámci kroku dva a kroku tři). V tomto duchu se tak bude jednat spíše o okolnosti typu následného jednání pokutované osoby, které vedlo ke **snížení dopadu na subjekty údajů**, či předchozího porušení ze strany pokutované osoby.

Čtvrtý krok – určení zákonného maxima

Čtvrtým krokem by měl dozorový orgán určit **příslušná zákonná maxima** pro různé operace zpracování. Předmětné navýšení v předchozích nebo následujících krocích by pak nemělo tuto částku překročit. Ačkoliv by se zákonným maximem měl dozorový orgán zabývat už v předchozích krocích algoritmu (zejména v rámci kroku č. 2), stále nám visí ve vzduchu skutečnost, že maximální výše pokuty není stanovena pouze **fixně** (tedy 10 či 20 milionů eur), ale i dynamicky – a to v případě, že celosvětový obrat podniku přesahuje fixní hranici (a to do výše 2 %, respektive 4 % tohoto obratu). V tomto duchu tak pokyny EDPB nabízejí různá výkladová východiska, která by nám měla pomoci se zorientovat v maximální možné částce, již lze za sankci udělit. Pokud však náš **obrat nepřesahuje 10 či 20 milionů eur,** nemusíme se tím moc trápit.

Pátý krok – splnění požadavků na sankci

Otázku, zda vypočtená pokuta splňuje požadavky na její **účinnost, odrazující účinek, ale také přiměřenost** (v souladu s čl. 81 odst. 3 GDPR), by si měl dozorový orgán pokládat v rámci procházení celého algoritmu. Nicméně v pátém kroku by měl definitivně **zhodnotit naplnění účelu sankce**. Účinná pokuta je taková, která je způsobilá dosáhnout svého cíle. Cílem sankce dle GDPR totiž není jen pouhé potrestání, ale taktéž **motivace k dodržování** (respektive obnovení dodržování) pravidel. Pokuta by měla být také odrazující – měla by tedy zabránit pokutované osobě v tom, aby toto porušení v budoucnosti opakovala.

> **Výše sankce by měla odrážet majetkové poměry pokutované osoby**

Mějme tak na paměti, že výše uvedená kritéria výpočtu, jež by pro nás mohla být příznivá, **nemusí být definitivní**. Dozorový orgán vždy musí posoudit, zda je sankce účinná či dostatečně odrazující – a pokud nabyde dojmu, že není, tak ji zvýší.

V každém případě však platí, že **pokuta musí být přiměřená**. A takovou rozhodně nebude pokuta, která by byla **likvidační**. Avšak to, že společnost aktuálně nemá peníze (ačkoliv se jí dařilo a daří dobře), samo o sobě neznamená, že jí dozorový orgán udělí konkurenční výhodu v podobě nízké pokuty. V případě snížení pokuty by měl dozorový orgán zhodnotit nejen ekonomické ukazatele, ale i další kontext tak, aby pokuta byla skutečně přiměřená, ale ne nedůvodně nízká.

Definitivní podoba pokynů

Zda a jak moc se předmětné pokyny ještě změní, ukáže čas, a to relativně brzo. Samotný dokument je sice psán složitějším jazykem, nicméně obsahuje spoustu návodných příkladů a popisů různých situací spolu s uvedením dopadů jednotlivých požadavků EDPB. V budoucnu by tak tento dokument měl sloužit dozorovým orgánům k tomu, aby **sjednotily svůj postup při ukládání pokut**, ale i nám, abychom v případě problémů mohli odhadnout, kolik peněz si máme připravit, a také se mohli pokusit argumentovat ohledně výše případné sankce. Budeme tedy sledovat připomínkové řízení a vrátíme se k tomuto tématu v okamžiku, kdy budou předmětné pokyny definitivní.

▪▪▪

Mgr. Josef Bátrla,
advokát v oblasti ICT
www.josefbatrla.cz

Klikněte a stáhněte si CHECKLIST

CHECKLIST: Jaké údaje vyžadovat v rámci osobního dotazníku zaměstnance?

Identifikační údaje zaměstnance

- Jméno a příjmení
- Rodné příjmení
- Rodné číslo
- Místo narození
- Datum narození
- Státní příslušnost

Pozor, tento údaj nezaměňovat s národností. Národnost je zvláštní osobní údaj, který zaměstnavatel vyžadovat nesmí.

Údaje potřebné od zaměstnanců – cizinců

- Pracovní povolení
- Zaměstnanecká karta
- Modrá karta
- Karta vnitropodnikově převedeného zaměstnance
- Případně doklad o tom, že pracovní povolení nepotřebuje a proč (občan členského státu EU a podobně)
- Kopie dokladů prokazujících oprávněnost pobytu cizince na území ČR
- Číslo cestovního dokladu a název orgánu, který jej vydal

Bydliště

- Trvalé bydliště
- Přechodné bydliště

Údaje potřebné pro Českou správu sociálního zabezpečení a zdravotní pojišťovny

- Identifikace předešlého zaměstnavatele
- Informace, zda je zaměstnavatel poživatelem invalidního/starobního důchodu
- Zdravotní pojišťovna

Údaje potřebné k daňovému zvýhodnění zaměstnance

- Status studenta
- OSVČ
- Rodinný stav
- Počet dětí

Vzdělání a kvalifikace

- Nejvyšší dosažené vzdělání
- Akademický titul

- Dokumentace prokazující splnění předpokladů pro výkon práce
- Dokumentace prokazující splnění požadavků pro výkon práce

Platební a kontaktní údaje

- Číslo bankovního účtu, na který má být vyplácena mzda
- Telefonní číslo
- E-mailová adresa

Exekuce a insolvence

- Exekuční/Insolvenční řízení

Je možné vyžadovat je tehdy, pokud je zde věcný důvod spočívající v povaze práce (a požadavek na sdělení této informace je přiměřený) nebo pokud tak stanoví zákoník práce či zvláštní předpis.

Další možná ustanovení a souhlasy

- Potvrzení pravdivosti uvedených údajů
- Povinnost informovat o změnách

Toto ustanovení je lepší vložit do pracovní smlouvy nebo dohody.

Mimořádná pokuta pro Google: 10 milionů eur za nedodržení práva být zapomenut

Španělský dozorový úřad Agencia Española de Protección de Datos (AEPD) udělil společnosti Google pokutu 10 milionů eur (cca 247 milionů korun) za závažné porušení GDPR. Pochybení spočívalo v tom, že Google předával třetí straně se sídlem v USA bez platného právního základu informace, které by mohly být použity k identifikaci osob žádajících o vymazání svých osobních údajů podle práva EU, včetně jejich e-mailové adresy, uvedených důvodů a deklarované adresy URL. Třetí stranou, které měl Google údaje nezákonně předávat, je organizace Lumen, americký akademický projekt Harvardské univerzity, jehož cílem je studovat zákonné žádosti o odstranění online informací prostřednictvím shromažďování databáze žádostí o odstranění obsahu. Podle AEPD se tak Google dopustil dvou porušení GDPR tím, že předával osobní údaje občanů EU třetí straně bez platného právního základu a tím, že bránil právu subjektů údajů na výmaz jejich osobních údajů (tedy právu být zapomenut podle čl. 17 GDPR). Kromě pokuty tak AEPD nařídil společnosti, aby uvedla své postupy do souladu s GDPR. Organizace Lumen uvedla, že vyhověla žádosti AEPD (prostřednictvím společnosti Google) a vymazala údaje uživatelů, u nichž bylo zjištěno, že jí byly sděleny bez právního základu. Rozsudek ADPB je svým způsobem anomálií, neboť většina stížností na společnost Google obvykle končí u irského dozorového úřadu (podle zásady „one stop shop“), který je dlouhodobě kritizován za nečinnost a průtahy. Irský úřad aktuálně prošetřuje několik stížností na společnost Google, přičemž nejdelší vyšetřování se táhne od doby, kdy GDPR poprvé vstoupilo v platnost v roce 2018.

Zdroj: CPO Magazine

Nejčastější nedostatky cookies očima ÚOOÚ

Od účinnosti novely zákona o elektronických komunikacích uplynul už víc než půlrok a ÚOOÚ začíná důkladně vymáhat přísnější pravidla ukládání cookies. Jaké nedostatky se v praxi nejčastěji objevují?

Někteří provozovatelé internetových stránek stále neimplementovali správně nová pravidla, která se týkají cookies. Od Nového roku totiž **platí zpřísněný režim**, dle kterého je nutno pro uložení a používání cookies (a obdobných technologií) vyžadovat souhlas, což ne všichni provozovatelé stránek reflektují. Alespoň tak lze číst tiskovou zprávu, kterou těsně před prázdninami vydal Úřad pro ochranu osobních údajů (ÚOOÚ). V té úředníci pojmenovali **devět nejčastějších prohřešků**, na které v souvislosti s používáním cookies narazili při kontrolách v rámci prvního pololetí tohoto roku.

Povinností spojených s používáním cookies je samozřejmě více, ale pokud čtete pravidelně tento Zpravodaj, neměly by pro vás být překvapením. Ostatně, tomuto tématu jsme se věnovali ještě za předchozí právní úpravy a naše čtenáře jsme **na nová pravidla připravovali**. Těm, kteří si daná doporučení nevzali k srdci, však ÚOOÚ vyslal před začátkem prázdnin poměrně jasnou zprávu – dejte si na způsob používání cookies pozor.

Konec mírného přístupu

Sám ÚOOÚ k předmětným nedostatkům uvedl, že se jich dopouští jak **malé, tak i velké společnosti**. Předseda ÚOOÚ Jiří Kaucký k tomu uvedl následující: *„V prvním pololetí jsme dali provozovatelům prostor, aby se nové legislativě přizpůsobili. Nyní ovšem na základě vlastní iniciativy monitorujeme dodržování a oslovujeme správce, kteří porušují právní předpisy v této oblasti, aby zjednali nápravu. Pokud k ní nedojde, přistoupíme k sankcím, a to především finančního charakteru.“*

ÚOOÚ končí se shovívavým přístupem a sám zahajuje kontroly

Problematických bodů, které můžeme pokazit, je mnohem více. Využijme tedy pokud možno prázdnin a **dejme si cookies do pořádku**. Je totiž možné, že je to naše poslední šance před tím, než ÚOOÚ upustí od shovívavého přístupu.

Kontrolní činnost

Jak jsme ukázali, ÚOOÚ se nikterak netajil tím, že druhou část prvního pololetí roku 2022 zasvětí kontrole cookies. Koneckonců **kontrolu používání cookies** zařadil i do kontrolního plánu. Této oblasti se ÚOOÚ věnoval již v předchozích letech, během nichž jsme vás o závěrech těchto kontrol pravidelně informovali. Faktem však zůstává, že s příchodem **novely zákona o elektronických komunikacích** doznalo mnoho věcí zásadních změn.

Kdo si myslel, že ÚOOÚ bude při kontrolách zajímat pouze to, zda provozovatel stránek **vyžaduje souhlas**

Používání technických cookies bez souhlasu

Prvním nedostatkem je podle ÚOOÚ časté užívání cookies bez souhlasu návštěvníka. Dle zákona o elektronických komunikacích není potřeba získávat souhlas u takzvaných technických (případně nezbytných) cookies. Ne všechny cookies, u kterých se rozhodneme, že jsou pro naše stránky důležité, však spadají do této kategorie. Spolu se špatnou kategorizací a klasifikací cookies se tak velmi často setkáváme zejména s případem, kdy jsou bez souhlasu ukládána a čtena statistická cookies.

Neúměrně dlouhá doba platnosti cookies vzhledem k jejich účelu

Principiálně platí to, co známe již z GDPR – sbíráme-li nějaká data, měli bychom je uchovávat pouze po dobu, po kterou je to skutečně a objektivně nezbytné. Totéž pak platí i ve vztahu ke cookies. Poměrně často se totiž potkáváme s tím, že některá cookies jsou ukládána například na neomezenou dobu, popřípadě dobou uložení překračují svůj účel. Je tedy dobré zkontrolovat, jaké doby uložení máte v rámci svých cookies nastaveny.

uživatele, se mýlil. ÚOOÚ se totiž do mnohem větší míry soustředí na detaily a zajímá jej i to, jakým způsobem se souhlas získává, zda má návštěvník možnost udělení souhlasu odmítnout a jakým způsobem se k němu dostávají související informace. Co se týče 1. pololetí tohoto roku, ÚOOÚ sdělil, že kontroly proběhly nejen na základě kontrolního plánu, ale také **na základě stížností a podnětů**.

Pojďme se tedy podívat na jednotlivé **nejčastější prohřešky**, před kterými ÚOOÚ varuje. Pro účely tohoto článku jsme některé body (špatná kategorizace, klasifikace a účel cookies) sloučili, neboť spolu velmi úzce souvisejí.

▪▪▪

Mgr. Josef Bátrla,
advokát v oblasti ICT
josefbatrla.cz

Nedostatečná první vrstva

Jako třetí zjištění uvádí ÚOOÚ nepřítomnost volby pro vyjádření nesouhlasu s využitím netechnických cookies v 1. vrstvě cookies lišty. Stále se potkáváme s cookies lištami, které sice aktivně vyžadují souhlas a bez něj cookies neuloží ani nepoužijí, nicméně pokud svůj souhlas dát nechceme, musíme se prokliknout do 2. vrstvy. Tento postup je však v rozporu s legislativou, na což jsme upozorňovali již před nabytím účinnosti předmětné novely. Sám ÚOOÚ na tuto skutečnost poukazoval **na svých stránkách**, přesto se jedná o stále velmi častou praxi. Důvod je jednoduchý. Aby se návštěvník webu zbavil cookies lišty, je pro něj jednoduší souhlas udělit než se proklikávat přes cookies lištu někam dál. Takový souhlas však nesplňuje podmínky GDPR, a tudíž ani zákona o elektronických komunikacích, a lze jej tak považovat za nezákonně získaný.

Cookies lišta znesnadňuje či znemožňuje čtení webové stránky

O tom, že takzvané „cookie walls" jsou zakázané, víme již velmi dlouho. Postup správce, který bez odkliknutí souhlasu neumožní pokračovat ve čtení stránek, je kritizován i Soudním dvorem Evropské unie, který na tento nešvar dlouhodobě upozorňuje ve své rozhodovací praxi. Se stejným názorem se setkáme napříč prakticky všemi dozorovými orgány EU. Mnohdy však k znesnadnění četby stránek dochází téměř omylem. Ačkoliv v desktopové verzi může cookies lišta působit nerušivě, v případě návštěvy internetových stránek na mobilním zařízení nemusí být cookies lišta úplně responzivní a může zabrat významnou část obrazovky. Návštěvník stránek pak nemá možnost přečíst prakticky nic kromě dlouhého textu 1. vrstvy cookies lišty. Pokud 1. vrstva neobsahuje možnost, jak cookies lištu zavřít, jedná se o velmi zásadní problém. Doporučujeme tedy, abyste nasazenou lištu otestovali i na jiných zařízeních a zkontrolovali, že je dostatečně čitelná, ale zároveň nepůsobí rušivě.

Rozdíl ve viditelnosti tlačítek pro souhlas a nesouhlas

Jedním z takzvaných „dark patterns" je i postup, kdy se snažíme motivovat návštěvníka k tomu, aby nám souhlas udělil, ačkoliv to primárně nechce. Kromě případů, kdy čtenáři webových stránek neumožníme minimalizovat cookies lištu, pokud souhlas neudělí, je jednou ze zakázaných praktik i postup, kdy tlačítko pro neudělení souhlasu zjednodušeně řečeno zneviditelníme. Toho můžeme dosáhnout tak, že naopak zvýrazníme tlačítko pro souhlas, vedle nějž další tlačítko jednoduše zapadne. Návštěvník, který je motivován co nejrychleji schovat cookies lištu, tak spíše klikne například na zelené tlačítko „Souhlasím" než o dost menší tlačítko „Nesouhlasím", které má neutrální barvu, a je tak velmi snadno přehlédnutelné.

Absence informací o konkrétních použitých cookies

Ačkoliv lze možná z často kladených otázek ÚOOÚ vyčíst trochu benevolentnější výklad, pravdou je, že jakožto správci máme povinnost informovat uživatele o konkrétních cookies (minimálně o době jejich uložení a o jejich příjemcích). Velmi často se však můžeme setkat s cookies lištami, které sice mají (velmi zjednodušeně řečeno) všechna vyžadovaná tlačítka, nicméně návštěvník nemá šanci se seznámit s bližšími informacemi o jednotlivých cookies. To však může být z pohledu ÚOOÚ problém, a de facto tak dochází k porušení čl. 13 GDPR, který stanovuje informační povinnost.

Informace o cookies v cizím jazyce

Na trhu existuje mnoho nástrojů, které nabízejí takzvaný „cookie consent manager", tedy řešení, které nám umožňuje správně získávat souhlas. Ačkoliv mnoho z nich není v základu v souladu s GDPR, potažmo se zákonem o elektronických komunikacích, vyšší verze za příplatek tuto compliance nabízí. I přes to nelze vše vyřešit jen vložením lišty bez kontroly, zda obsahuje veškeré náležitosti. Velmi často tak na webech najdeme dobré řešení a souladný způsob sběru cookies, nicméně veškeré informace jsou uvedeny v angličtině. To je ale ve většině případů v rozporu s čl. 12 GDPR, který stanovuje požadavky na způsob poskytnutí informací.

Poradna

Obec zaměstnává účetní na hlavní pracovní poměr, to znamená, že práci vykonává na úřadě. Má aktivován „token" (k přihlašování do Czech pointu, ČNB a dalších aplikací, které eventuálně využívá ke své práci) pod hlavičkou obce. Tato zaměstnankyně vznesla na starostu požadavek, že chce do svého soukromého notebooku nainstalovat všechny přístupy do výše uvedených aplikací, včetně účetnictví, aby se mohla přihlašovat z domova. Když pominu, že notebook dle vyjádření našeho IT pracovníka nemá žádný kvalitní antivirový program, nejsem si jistá, zda je možné jí tyto přístupy zřídit. Dle mého názoru by token měl být jen na pracovišti a účetní doklady by se neměly přenášet (v účetnictví obce jsou i mzdové údaje řadových zaměstnanců). Z pozice pověřence jsem proto panu starostovi sdělila, že tak velký přístup do aplikací a dat, které využívá obec, by se neměl zavádět do soukromého notebooku a v tak velkém rozsahu odnášet z místa pracoviště. Je tento postup správný?

Zásada důvěrnosti a integrity patří mezi jednu z nejdůležitějších zásad v rámci zpracování osobních údajů. Stejně tak patří dle čl. 39 odst. 1 písm. b) GDPR mezi úkoly pověřence monitorovat soulad zpracování osobních údajů a upozorňovat na možná problematická místa. Váš postup, kdy upozorňujete na možný nesoulad, popřípadě potenciální ohrožení důvěrnosti osobních údajů, je tak správný. Tím nechci říct, že je vyloučené, aby obec svůj záměr realizovala, nebo že by byl v rozporu s GDPR. Správce by však měl takový postup posoudit a identifikovat možná rizika, a to nejen bezpečnostní, ale i právní. Pokud správce takové posouzení nevyhotovil a zároveň nezohlednil předmětná rizika v interní politice (například bezpečnostní směrnici), která by stanovovala povinnosti a omezení při práci z domova, a stejně tak neřešil otázku technických parametrů soukromých zařízení, určitě je nutné jej na to upozornit pro možný rozpor s GDPR. Je pak samozřejmě odpovědností správce, jak s tímto upozorněním naloží a jak se k dané věci postaví. ▪▪▪

JOSEF BÁTRLA ADVOKÁT

Nevíte si s něčím rady? Pošlete nám svůj dotaz a my vám zprostředkujeme odpověď! Dotazy pokládejte e-mailem na:
zpravodaj.poverenec@forum-media.cz

Elektronický zpravodaj pro pověřence | Vydavatel: Nakladatelství FORUM s.r.o. | Adresa redakce: Střelničná 1861/8a, 182 00 Praha 8 | Šéfredaktorka: Mgr. Anna Zavadilová | Zákaznický servis: Petra Pokojová, office@forum-media.cz, tel.: +420 251 115 576, fax: +420 251 512 422 | Jazyková redakce: Mgr. Jana Vašinová | Fotografie: www.bigstockphoto.com | Zlom časopisu: Renata Brtnická | Roční předplatné: 2790 Kč bez DPH | Objednávka předplatného: office@forum-media.cz, fax: +420 251 512 422, informace o předplatném: +420 251 115 576 | Ukázkové číslo | Elektronický zpravodaj vychází jako čtrnáctideník, celobarevný, 8 stran A4, ISSN 2571-1504.