HAVEN

ADVOKÁTNÍ KANCELÁŘ

PŘEHLED K PROBLEMATICE OCHRANY OSOBNÍCH ÚDAJŮ

HAVEN
ADVOKÁTNÍ KANCELÁŘ

V následujícím přehledu si Vás dovolujeme seznámit s nedávnými rozhodnutími Úřadu pro ochranu osobních údajů (ÚOOÚ), závěry jím provedených kontrol a s dalšími novinkami v oblasti ochrany osobních údajů. O dalších informacích z oblasti právní ochrany osobních údajů Vás budeme informovat v dalším vydání tohoto přehledu nebo v přehledu právních aktualit.

Z kontrolní činnosti ÚOOÚ

+ Kontrola zpracování osobních údajů prostřednictvím kamerového systému v prostorách nemocnice

Na základě podnětu byla zahájena kontrola dodržování povinností stanovených obecným nařízením o ochraně osobních údajů (dále jen „**GDPR**“) v souvislosti se zpracováním osobních údajů prostřednictvím kamerového systému v prostorách kliniky nemocnice. Zavedení kamerového systému zdůvodňovala kontrolovaná osoba potřebou detekování vzniku nežádoucích stavů pacientů a jako nezbytnou součást celkové léčby pacienta. Zpracování zvláštních kategorií osobních údajů pacientů (jako je například údaj o rasovém či etnickém původu, náboženském vyznání, zdravotním stavu, sexuální orientaci osoby a další) pak zdůvodnila výjimkou dle čl. 9 odst. 2 písm. i) GDPR, kdy je zpracování nezbytné z důvodu veřejného zdraví a slouží k zajištění přísných norem kvality a bezpečnosti zdravotní péče, léčivých přípravků nebo zdravotnických přípravků.

ÚOOÚ (dále jen „**Úřad**“) však poukázal na to, že z právního základu, ze kterého kontrolovaná osoba vychází, nevyplývá povinnost sledovat stav pacientů pomocí videokamer. V průběhu kontroly vyšlo dále najevo, že v posledních 10 letech nebylo do kamerových záznamů nahlíženo. Úřad proto konstatoval, že kontrolované osobě pro použití kamerového systému ve vnitřních prostorách kliniky výše zmíněný právní titul nesvědčí.

Závěrem Úřad doplňuje, že kamerový systém by ve vnitřních prostorách mohl být provozován v souladu s čl. 6 odst. 1 písm. f) GDPR (tj. pokud je zpracování údajů nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany), správce osobních údajů by však musel prokázat, že pro konkrétní účely má jeho oprávněný zájem přednost před zájmy nebo základními právy a svobodami subjektů údajů (tedy provést test proporcionality – balanční test).

+ Kontrola zpracování osobních údajů na sociálních sítích

Úřad se touto kontrolou zabýval zejména zveřejněním adres poslanců na sociální síti Facebook a Telemetr.io. Osobní údaje ve formě adres měly být také rozesílány prostřednictvím e-mailu. Úřad zjistil, že kontrolovaná osoba nezpracovávala osobní údaje v souladu s GDPR, tedy nedisponovala legitimním právním titulem podle čl. 6 odst. 1 GDPR (mezi které patří (1) udělení souhlasu se zpracováním osobních údajů, (2) zpracování je nezbytné pro splnění smlouvy, (3) pro splnění právní povinnosti, (4) pro ochranu životně důležitých zájmů subjektu údajů, (5) pro splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci a (6) pro účely oprávněného zájmu správce údajů).

Dalším pochybením kontrolované osoby bylo neplnění informační povinnosti vůči subjektům údajů – na webových stránkách neuvedla žádnou informaci o ochraně osobních údajů ani informaci o způsobu zpracování těchto údajů. V návaznosti na tato pochybení bylo zahájeno správní řízení.

+ Kontrola zasílání obchodních sdělení

V několika případech zahájil Úřad na základě stížností kontrolu týkající se dodržování povinností souvisejících s rozesíláním obchodních sdělení (elektronickými prostředky) a zpracování osobních údajů v návaznosti s přímým marketingem.

Přímý marketing jako určitá forma reklamy cílící na konkrétní osoby a jako nástroj k podpoře podnikatelské činnosti společnosti, musí při šíření obchodních sdělení dodržovat přesně stanovené podmínky (upravené v GDPR i speciální úpravě v zákoně č. 480/2004 Sb., o některých službách informační společnosti). Ke zpracování osobních údajů pro účely přímého marketingu Úřad uvádí, že jde o zpracování z důvodu oprávněného zájmu dle GDPR, a tudíž zákazník při nákupu výrobku či služby může důvodně očekávat, že mu obchodník zašle obdobnou nabídku.

Obchodník, jako správce osobních údajů, však musí splnit informační povinnost – tj. informovat subjekt údajů a jeho právu vznést námitku proti zpracování osobních údajů pro účely přímého marketingu a informovat ho o způsobech, jak tak lze učinit (např. uvést kontakt, kterým lze zasílání zrušit). Pokud tak subjekt údajů učiní, nesmějí být jeho osobní údaje pro tento účel již dále zpracovávány. Tyto informace lze zveřejnit na webových stránkách a současně také přímo při uzavírání zákaznického vztahu, ať už elektronicky, prostřednictvím zákaznické linky nebo osobně na prodejně.

Kontrolovaná osoba (obchodník) musí dále prokázat, že předmětná obchodní sdělení šířila buď na základě zákaznického vztahu nebo na základě uděleného souhlasu adresátů. Úřad opětovně upozorňuje na to, že za šíření obchodních sdělení je odpovědný jak samotný faktický odesílatel, tak i subjekt, v jehož prospěch byla obchodní sdělení zasílána, a to na základě objektivní odpovědnosti, tedy odpovědnosti za následek. Totožnost odesílatele v obchodním sdělení nesmí být skrytá ani utajovaná, proto pouhý odkaz na webové stránky, kde lze např. nabízené zboží zakoupit, je nedostatečné.

Mezi nejčastější pochybení, která Úřad v rámci těchto kontrol zjistil, patří jednak zpracování osobních údajů v nadbytečném rozsahu (např. údaje fakturační a platební) a jednak zpracování údajů po dobu delší, než je nezbytná ke stanovenému účelu (například až 3 roky po ukončení zákaznického vztahu). Kontaktování zákazníka po ukončení zákaznického vztahu je dle Úřadu akceptovatelné a odpovídá běžné praxi, doba kontaktování však musí být přiměřená a vždy s možností odmítnutí ze strany subjektu údajů.

V návaznosti na některá porušení bylo zahájeno správní řízení, za některá porušení došlo také k uložení sankce ve výši 10 000 Kč.

Z důvodu množících se dotazů a stížností na zasílání obchodních sdělení prostřednictvím SMS zpráv uvádí Úřad souhrn podmínek, za nichž lze tato obchodní sdělení zasílat:

- ve zprávě musí být jasně a zřetelně označeno, že se jedná o obchodní sdělení, např. zkratkou „OS“.
- obchodní sdělení musí obsahovat název toho, jehož jménem se komunikace uskutečňuje

(odesílatele). Pokud se odesílatel liší od toho, v čí prospěch je zpráva odeslána, je potřeba uvést oba názvy.

- v obchodním sdělení musí být dána možnost odmítnout zasílání zpráv – např. uvedením telefonního čísla, na které lze zdarma zavolat nebo zaslat zprávu s odmítnutím. Uvedení odkazu, jehož prokliknutím dojde k odhlášení, není v případě zasílání obchodních sdělení SMS/MMS zprávou dostačující, neboť ne každý adresát disponuje s chytrým telefonem a připojením k internetové síti.

Další aktuality

+ Cookie lišty a udělování souhlasu

Úřad aktualizoval doporučení, informace a základní pravidla pro nastavení a uživatelský přístup prostřednictvím cookie souborů. V následujícím článku si dovolujeme uvést základní otázky a odpovědi v této problematice.

Co je u cookies potřeba na webových stránkách dodržovat?

Používání souborů cookie na webových stránkách představuje zpracování osobních údajů, proto je nezbytné jasně vymezit jejich účel a správně určit právní důvod zpracování. To je důležité pro rozlišení, zda se jedná o technické cookies (nezbytná pro vlastní provoz webových stránek), či jde o netechnické cookies (určené k sledování návštěvnosti, analýze preferencí návštěvníků apod.), které je možno ukládat a znovu k nim přistupovat pouze na základě souhlasu uživatele.

Na webové stránky, které využívají pouze technické coookies, není třeba zavádět tzv. cookie lištu (aplikace, která obsahuje informace o cookies a umožňuje udělit souhlas či odmítnutí souhlasu se zpracováním údajů). Vůči subjektům údajů je však nutné splnit informační povinnost, která se umístí na viditelné místo na webové stránce (informace obsahuje zejména vymezení správce, účel a právní důvod použití cookies, příjemce osobních údajů, předávání údajů do třetích zemí, kontaktní údaje pověřence, dobu uložení údajů (nesmí být delší, něž jaká je nezbytná pro účely zpracování), informace o právech subjektů údajů a další). Tato informace musí být všem přístupná a srozumitelná (tj. uživatel by se k ní neměl proklikávat skrze více stránek).

Pokud se jedná o netechnické cookies, je třeba na cookie liště umístit tlačítko pro nesouhlas s těmito soubory tak, aby mohl návštěvník případný souhlas udělit bez nátlaku a nebyl při své volbě ovlivňován. Příkladem správného provedení je umístění tlačítek pro udělení souhlasu a pro nesouhlas s netechnickými cookies do stejné (první) vrstvy cookie lišty, ve stejné rovině a srovnatelném vizuálním provedení. Cookie lišta nesmí bránit v interakci s webovou stránkou a narušit využívání služby, a to ani v případě, kdy návštěvník ještě nezvolil žádnou z uvedených možností ohledně souhlasu. Netechnické cookies se mohou aktivovat až po udělení souhlasu (jako souhlas se nepovažuje zavření lišty bez výběru možnosti souhlasu nebo nesouhlasu ani nečinnost uživatele, tj. pokud na cookie lištu nereagoval).

Jaký je rozdíl mezi souhlasem podle zákona o elektronických komunikacích a podle GDPR?

Souhlas dle zákona o elektronických komunikacích je nutné získat pro využití netechnických souborů cookies (ukládání a

čtení) a podobných technologií. Získaný souhlas však neřeší zpracování osobních údajů, ke kterému prostřednictvím cookies dochází (analýza, profilování). Souhlas pouze umožňuje správci ukládání cookies do zařízení koncového uživatele.

Souhlas dle GDPR je jeden ze šesti právních titulů, na základě kterých je možné osobní údaje zpracovávat. Zpracování souborů cookies nemusí být nezbytně založeno na právním titulu souhlasu. Pokud ano, souhlas musí být vždy svobodný, konkrétní, informovaný a jednoznačný. Subjekt údajů musí mít také jednoduchou možnost souhlas neudělit. V případě cookies může být právním titulem zpracování i oprávněný zájem nebo zpracování nezbytné pro splnění smlouvy.

Je možné udělit souhlas prostřednictvím nastavení prohlížeče?

Ne, to možné není. Správce musí být schopen prokázat, že mu uživatel souhlas ke zpracování udělil. Udělení souhlasu je aktivní činnost uživatele (tj. např. kliknutí na tlačítko souhlasu), předem nastavený souhlas v prohlížeči tuto podmínku nesplňuje.

Musím umožnit uživateli udělený souhlas odvolat?

Ano, subjekt údajů může souhlas kdykoli odvolat. Odvolání souhlasu by mělo být stejně snadné, jako jeho udělení (např. snadno dostupné tlačítko nebo odkaz pro možnost souhlas odvolat).

Může mít tlačítko „Přijmout vše“ jinou barvu než tlačítko „Odmítnout vše“?

Subjekt údajů musí mít možnost svobodně se rozhodnout, zda souhlas udělí či nikoli. Tlačítko *souhlasím* by tak nemělo být např. výrazněji větší nebo barevnější, než tlačítko *odmítám*. Pokud by tlačítko *odmítám* bylo hůře viditelné a subjekt údajů ho přehlédl, nejednalo by se o svobodně udělený souhlas.

Je možné mít předem zaškrtnuté ANO u analytických a marketingových cookies?

Předem zaškrtnutá políčka nelze považovat za souhlas v souladu s GDPR.

Jak dlouho lze uchovávat souhlas s ukládáním cookies?

Obecně se za přiměřenou dobu, na kterou byl udělen souhlas s využíváním cookies, považuje doba 12 měsíců. V případě odmítnutí udělení souhlasu by jeho udělení nemělo být znovu vyžadováno alespoň 6 měsíců od posledního zobrazení cookie lišty. Přičemž platí, že opětovné zobrazování cookie lišty by nemělo narušovat činnost uživatele při používání webové stránky.

+ Pokuta pro Instagram a Facebook ve výši 390 miliónů EUR za behaviorální reklamu

Dne 12. 1. 2023 přijal irský úřad pro ochranu údajů (dále jen „**IE DPA**“) v souladu se závaznými rozhodnutími EDPB (Evropský sbor pro ochranu osobních údajů) svá rozhodnutí týkající se společnosti Facebook a Instagram (které provozuje společnost Meta Platforms Ireland Limited, dále jen „**Meta**“). Z celkové výše pokuty 390 miliónů EUR náleží 210 miliónů EUR Facebooku a zbylých 180 miliónů EUR Instagramu, a to za netransparentnost zpracování osobních údajů klientů pro tzv. behaviorální reklamu (jinak také zájmově orientovaná reklama, jedná se o metodu cíleného přiřazování reklam na základě předchozí internetové aktivity daného uživatele).

EDPB v závazném rozhodnutí uvádí, že společnost Meta postrádala právní základ pro tato zpracování, když nevhodně

spoléhala na smlouvu jako právní základ pro zpracování osobních údajů pro účely behaviorální reklamy, přestože to nebyl hlavní prvek služby. Tyto údaje proto byly zpracovávány nezákonně – došlo k porušení čl. 6 odst. 1 GDPR. Kromě absence právního základu pro zpracování osobních údajů zjistil EDPB také porušení zásady korektnosti – Meta prezentovala své služby uživatelům zavádějícím způsobem, důvodná očekávání uživatelů byla ovlivněna porušením povinností týkajících se transparentnosti a vztah mezi společností Meta a uživateli byl nevyvážený. Původně navržená výše pokut podle IE DPA (36 miliónů EUR pro Facebook a 23 milionů EUR pro Instagram) pak ve výsledku dle EDPB nesplňovala požadavek účinnosti, přiměřenosti a odrazení. IE DPA ji proto ve svých konečných návrzích rozhodnutí několikanásobně zvýšil na celkovou částku 390 miliónů EUR.

V blízké době bude přijato také rozhodnutí vyplývající z již proběhlého šetření společnosti WhatsApp, jehož provozovatelem je také společnost Meta.

+ Shrnutí zprávy pracovní skupiny pro online služby společnosti Microsoft

Dne 25. 11. 2022 zveřejnila Německá Konference pro ochranu osobních údajů shrnutí zprávy Pracovní skupiny pro online služby společnosti Microsoft. Ta byla ustanovena před dvěma lety, aby vedla jednání se společností Microsoft v souvislosti se službou Microsoft Office 365 a uvedením do souladu s příslušnými požadavky GDPR.

Pracovní skupina zejména hodnotila, zda nové aktuální znění smluvního dodatku k ochraně osobních údajů odstranilo dříve zjištěné nedostatky. Pracovní skupina však nezjistila žádné významné zlepšení. Problémem zůstává předávání osobních údajů do třetích zemí, kdy pracovní skupina potvrdila, že službu Microsoft 365 nelze provozovat bez předání dat do Spojených států amerických (kdy je nezbytný přístup Microsoftu k ostrým nepseudonymizovaným datům, který většinou vylučuje možnost šifrování zpracovávaných dat). Jedná o dosud nevyřešený problém chybějících doplňkových opatření, která by mohla zajistit předávání údajů v souladu s GDPR (tak, jak jej vykládá rozsudek Soudního dvora EU ve věci Schrems II., který zrušil možnost předávat osobní údaje do USA na základě Štítu soukromí (Privacy Shield) pro nedostatečnou odpovídající úroveň soudní ochrany subjektů údajů americkým zákonodárstvím).

Dalším zásadním problémem, na který pracovní skupina poukazuje je, že i v průběhu celého dvouletého jednání není schopna rozlišit, které operace Microsoft provádí v roli zpracovatele a které jako samostatný správce. To pak zákazníkům, kteří tuto službu používají, prakticky znemožňuje naplňovat princip odpovědnosti dle GDPR (tj. schopnost správce prokázat realizaci práv). Pracovní skupina dále zdůrazňuje, že samotný fakt, že se Microsoft při poskytování služby Microsoft 365 zpracovává osobní údaje pro vlastní účely, vylučuje, aby tuto službu využívaly orgány veřejné moci (včetně škol), neboť jediný právní titul, který by se pro ně vztahoval – totiž zpracování za účelem oprávněného zájmu dle čl. 6 odst. 1 písm. f) GDPR, není pro orgány veřejné moci aplikovatelný.

Konference tak ve svém závěru konstatuje, že nově uvedený aktuální dodatek není (stále) dokladem prokazujícím, že služby Microsoft 365 jsou provozovány v souladu s legislativou ochrany osobních údajů.

HAVEN
ADVOKÁTNÍ KANCELÁŘ

+ Ochrana osobních údajů v digitální době – poznatky z konference Ochrana osobních údajů v době digitalizace

V pražském Lichtenštejnském paláci se dne 29. 11. 2022 uskutečnila konference zaměřená na ochranu osobních údajů v době digitalizace. Konferenci uspořádal Úřad vlády společně s Asociací pověřenců ČR. Na konferenci vystoupil i předseda ÚOOÚ Jiří Kaucký, některé body jeho projevu si Vám dovolujeme uvést v následujících řádcích.

Předseda Úřadu v úvodu poukazuje na to, že přesunem významné části komunikace do digitálního světa dochází k ohromnému a neustálému zpracování osobních údajů, které často podléhá zneužitím v důsledku kriminální činnosti i samotnými správci těchto údajů. Nejen to vedlo k zásadnímu zintenzivnění ochrany osobních údajů na úrovni EU i národních dozorových úřadů.

Pandemie COVID 19 ale i následná ruská agrese na Ukrajině a s ní spojená hybridní válka, dezinformace a kybernetické útoky podnítily větší zájem každého z nás na ochraně našich osobních údajů. Skutečná zranitelnost osobních údajů se dle předsedy ukazuje v souvislosti se stále častějšími kybernetickými útoky, které mohou mít dle slov předsedy vážné dopady nejen na konkrétní oběti, ale také na celou společnost v podobě dezinformací, manipulací nebo dokonce rozvratu určitých sektorů společnosti (např. masové manipulace veřejnosti, krádeže identit), může dojít k zahlcení a zhroucení některých služeb, zdravotnických zařízení ale i celé digitalizované státní správy (NÚKIB evidoval v lednu 2023 více než dvojnásobný nárůst kyber. incidentů oproti průměrné hodnotě posledního roku).

Dle slov předsedy Úřadu: *„Jakákoli digitalizace státní správy musí nezbytně jít ruku v ruce s kybernetickou bezpečností a zejména s ochranou osobních údajů těch, jejichž údaje jsou státem spravovány. Stát má mít jen tolik údajů, které k plnění svých zákonných povinností potřebuje a má je zpracovávat jen k účelu, pro který je má. Osobní údaje nota bene svěřené pod hrozbou sankce státu se například ani nepřímo nemohou stát objektem jejich monetizace.“*

Závěrem předseda Úřadu doufá v další vývoj ochrany osobních údajů nejen v podobě např. větší účasti na legislativních procesech zejména v oblasti posuzování vlivů na soukromí a ochranu osobních údajů (pozn. od 1. 4. 2023 platí nová úprava DPIA – posouzení vlivu na ochranu osobních údajů se bude nově povinně zpracovávat u každého návrhu právního předpisu, včetně nařízení vlády a vyhlášky) ale i v přeshraniční oblasti a společné koordinované činnosti dozorových orgánů.

+ Sociální síť TikTok a bezpečnostní rizika s ní spojená

Podle Úřadu britského komisaře pro informace (dále jen „**ICO**“) zpracovávala sociální síť TikTok údaje uživatelů mladších třinácti let bez příslušného souhlasu rodičů, neposkytla svým uživatelům informace stručným, transparentním a snadno srozumitelným způsobem a zpracovávala některé údaje zvláštní kategorie (např. sexuální orientace, rasový původ, náboženské vyznání apod.) bez právního důvodu. Za nedostatečnou ochranu soukromí svých uživatelů hrozí síti pokuta ve výši 27 miliónů liber (cca 746 milionů Kč). Ve věci zatím nebylo přijato konečné

rozhodnutí. Podle britského regulačního úřadu pro komunikace (Ofcom) používá ve Velké Británii sociální síť TikTok až 44 % dětí ve věku 8-12 let navzdory tomu, že je aplikace pouze pro osoby starší 13 let.

Užívání čínské sociální sítě TikTok je od 15. 3. 2023 zakázáno ve všech zařízeních využívaných pro služební potřeby zaměstnanců Evropské komise. Pokud z těchto zařízení aplikaci neodinstalují, nebudou mít jeho prostřednictvím přístup k interním systémům a informacím Evropské komise. Podobně postupovaly i Spojené státy americké, které aplikaci zakázaly pro všechna zařízení federální vlády. V obou případech jde o obavy z bezpečnostních rizik, která jsou s aplikací spojená zejména v souvislosti s čínským zákonem o národní bezpečnosti, který vyžaduje, aby čínské společnosti podporovaly, pomáhaly a spolupracovaly s národními zpravodajskými službami. Situace, kdy jsou čínské technologické společnosti propojeny s čínskými zpravodajskými službami a shromažďují velké množství dat z celého světa, představuje dle Evropské komise významná kybernetická a datová rizika pro unijní exekutivu.

Ani u nás nezůstala aplikace TikTok bez povšimnutí. Dne 8. 3. 2023 vydal NÚKIB varování před hrozbou v oblasti kybernetické bezpečnosti spočívající v instalaci a používání této aplikace, a to zejména na zařízeních, které mají přístup k informačním a komunikačním systémům kritické informační infrastruktury a jiným významným informačním systémům. Dle NÚKIB obavy vyplývají především z *„množství shromažďovaných dat o uživatelích a způsobu, jakým jsou sbírána, nakládání s nimi a v neposlední řadě také z právního a politického prostředí Čínské lidové republiky, jejímuž právnímu prostředí je podřízena společnost ByteDance, která vyvinula a provozuje sociální platformu TikTok“*. Varování je zejm. pro povinné osoby dle zákona o kybernetické bezpečnosti, NÚKIB však doporučuje aplikaci nepoužívat i tzv. zájmovým osobám (osoby ve vysokých politických, veřejných či rozhodovacích funkcích). Zvážit užívání této aplikace se doporučuje i široké veřejnosti.

+ Společná dohoda EU-US Data Privacy Framework

Dlouho očekávaný návrh nové dohody (Data Privacy Framework) mezi EU a USA o vytvoření programu, ve kterém budou američtí účastníci považováni za bezpečné dovozce osobních údajů a předaným osobním údajům z Evropy se poskytne rovnocenná ochrana v souladu s GDPR a judikaturou Evropského soudního dvora (zejm. výše zmíněný rozsudek ve věci Schrems II.), byl již předán předsedkyni Evropského sboru pro ochranu osobních údajů (EDPB).

V následujících měsících bude k předmětnému návrhu vypracováváno stanovisko. Tato dohoda na rozdíl od svých předchůdců jako byl program Privacy Shield bude odpovídat standardům nastaveným rozsudkem ve věci Schrems II., zejména v otázce americké zákonné úpravy přístupu státních orgánů k osobním údajům spravovaným americkými společnostmi.

+ Informace k výmazu osobních údajů z veřejného seznamu držitelů datových schránek

Úřad bude v souvislosti s velkým počtem žádostí fyzických osob o výmaz osobních údajů z veřejného seznamu držitelů datových schránek žádat správce těchto údajů – Ministerstvo vnitra ČR, o informace o způsobu a rozsahu zveřejnění osobních údajů a zároveň ověří dodržování zásad zpracování a ochrany osobních údajů dle GDPR, zejména podmínky přiměřenosti a minimalizace.

Fyzická osoba, pokud nesouhlasí s uvedením svých údajů v seznamu držitelů datových schránek, má právo na jejich vymazání z tohoto seznamu. Požadavek na výmaz se zadává prostřednictvím Klientského portálu ISDS na této adrese: https://www.mojedatovaschranka.cz/portal/ISDS/nastaveni/informace/sds. Další informace o právech subjektů údajů a zpracování osobních údajů uživatelů datových schránek jsou uvedeny Ministerstvem vnitra na tomto odkazu: https://info.mojedatovaschranka.cz/info/cs/1017.html.

Úřad v této věci dále sděluje, že veškeré dotazy týkající se zpracování osobních údajů v informačním systému datových schránek je třeba primárně obracet na správce osobních údajů, kterým je Ministerstvo vnitra ČR, nebo případně na jmenovaného pověřence pro ochranu osobních údajů, kterým je: Odbor bezpečnostní politiky na adrese: Nad Štolou 3, 170 34 Praha 7 (poštovní schránka: 21/OBP), s elektronickou adresou: Poverenec@mvcr.cz.

Nové právní předpisy v oblasti ochrany osobních údajů

+ Digital Markets Act – Nařízení o digitálních trzích

Nařízení o digitálních trzích má přispět k řádnému fungování vnitřního trhu stanovením harmonizovaných pravidel, které zajišťují pro všechny podniky spravedlivé trhy otevřené hospodářské soutěže v digitálním odvětví v celé EU, kde působí tzv. strážci přístupu (tj. podniky, které (1) mají významný dopad na vnitřní trh, (2) poskytují hlavní službu platformy, (3) mají zavedené a trvalé postavení ve své činnosti, nebo (4) rozhodne-li tak EK), ve prospěch podnikatelských i koncových uživatelů.

Za účelem zabránění zneužívání tržní síly bude strážcům přístupu (např. společnost Apple, Google, Amazon a další), tj. největším digitálním platformám, určen seznam povinností, jejichž nedodržení bude sankcionováno. Seznam strážců přístupu zatím nebyl uveřejněn.

+ Digital Services Act – Nařízení o digitálních službách

Nařízení o digitálních službách je předpisem pro regulování online zprostředkovatelských služeb k šíření obsahu generovaného uživateli. Slouží jako základ pro boj proti nezákonnému obsahu (např. nenávistné projevy, teroristický obsah, diskriminační obsah, nelegální výrobky a služby apod.) – významně omezuje práva provozovatelů hostingu/platforem a zavádí tzv. povinnost náležité péče včetně dohledu státu.

Cílem je stanovit pravidla a povinnosti pro digitální služby (jako online platformy, sociální sítě, online tržiště a obchody s aplikacemi apod.), aby tyto služby nebyly zdrojem rizik a nelegální aktivity. Uživatelé těchto služeb budou mít možnost nahlásit,

že nějaký obsah považují za nezákonný a zároveň budou vždy informováni, z jakých důvodu došlo např. ke smazání jejich příspěvku.

+ Směrnice o platformách pro sdílení videa

Jde o novelizovanou směrnici upravující oblast obsahu na video-platformách (typu YouTube), zejména ochranu před škodlivým obsahem ve vztahu k nezletilým osobám a spotřebitelům. Nově upravuje odpovědnost za škodlivý obsah i na platformách pro sdílení videonahrávek.

Směrnice je do českého právního řádu implementována zákonem o službách platforem pro sdílení videonahrávek, který se např. dotkne služeb jako je Ulož.to, Rajče a další. Provozovatelé těchto platforem budou mít nově povinnost dostatečně ověřovat věk uživatelů a chránit je před nelegálním obsahem (např. videonahrávkami, které podněcují k nenávisti či násilí z důvodu rasy, náboženství, sexuální orientace, barvy pleti a další), ale také hlídat obsah reklam, které tvůrci umísťují do svých videí.

Platformy, které mají sídlo v České republice mají povinnost zapsat se do seznamu poskytovatelů služby platformy, který je evidován Radou pro rozhlasové a televizní vysílání, na adrese https://www.rrtv.cz

+ Návrh nařízení o umělé inteligenci (AI Act)

AI Act neboli Akt o umělé inteligenci je nařízení, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci. Vymezuje zakázané praktiky, kam patří např. využívání zranitelnosti určité skupiny osob, používání systémů biometrické identifikace na dálku a další. Dále mimo jiné upravuje povinnosti pro výrobce a dovozce tzv. high risk systémů (např. systémy pro výběr zaměstnanců, povýšení nebo ukončení pracovního vztahu, biometrické identifikace na dálku, systémy jako detektory lži apod).

+ TERREG

Nařízení o potírání šíření teroristického obsahu online se zaměřuje na boj proti zneužívání hostingových služeb pro teroristické účely a má přispívat k veřejné bezpečnosti v celé EU.

V návaznosti na toto nařízení nabyl dne 30. 3. 2023 účinnost zákon o některých opatřeních proti šíření teroristického obsahu online, který zavádí mimo jiné možnost Policie ČR vydat příkaz k odstranění teroristického obsahu poskytovateli hostingových služeb, včetně přezkumu přeshraničních příkazu k odstranění.

+ Směrnice Omnibus

Tzv. Omnibus novela – novela zákona o ochraně spotřebitele a občanského zákoníku (směrnice EU 2019/2161, směrnice EU 2019/770) upravuje určité oblasti

spotřebitelského práva, mezi zásadní patří např. reklamace zboží (jak u prodeje on-line, tak v kamenných prodejnách), která bude nyní pro zákazníky snazší v tom, že bude na prodávajícím, aby prokázal, že zboží nebylo vadné při převzetí spotřebitelem v případě, kdy se vada projeví v prvním roce od zakoupení.

Novela se dále dotkne slevových akcí - u každé slevy musí být nově zavedena její nejnižší cena, za kterou bylo zboží v posledních 30 dnech před poskytnutím slevy prodáváno. Uvedená sleva pak musí být vypočtena z této nejnižší ceny. Cílem je zabránit (v praxi běžným) situacím, kdy je cena u zboží navyšována těsně před zahájením slevové akce.

Kromě toho přináší novela řadu dalších změn pro e-shopy, ty musí dle nové úpravy upravit obchodní podmínky (nově platí povinnost poskytnout zákazníkovi obchodní podmínky platné v době uskutečněné objednávky, např. zasláním v PDF formátu současně s potvrzujícím e-mailem o objednávce), reklamační řády a informace na webu, ale také upravit vzhled tlačítka „*objednat*“, ze kterého dle nové úpravy musí být patrné, že součástí tohoto kroku je i povinnost za zboží či služby zaplatit (doporučované je např. označení „*objednávka zavazující k platbě*“).

U změn uzavírání smluv po telefonu nově platí, že předmětná smlouva bude uzavřena až poté, co spotřebitel obdrží od podnikatele písemný návrh smlouvy a tu písemně (elektronicky nebo na papíře) potvrdí. Tato změna se týká především ochrany seniorů před zneužíváním v rámci uzavírání smluv po telefonu.

Nově bude dále zveřejňování falešných recenzí v zákoně označeno za nekalou obchodní praktiku pod hrozbou pokuty od České obchodní inspekce. Pro spotřebitele pak z nové úpravy vyplývá např. požadavek, aby zboží zakoupené v e-shopu před jeho vrácením vyzkoušel pouze do té míry, jak by jej zkoušel v kamenné prodejně.

Judikatura

+ Sankce ve výši 1,4 mil. Kč za šíření obchodních sdělení

Nejvyšší správní soud svým rozsudkem ze dne 16. 3. 2023 potvrdil rozhodnutí Úřadu z roku 2018, kterým Úřad shledal žalobkyni vinnou ze spáchání přestupků spočívajících v šíření obchodních sdělení z různých e-mailových adres bez souhlasů adresátů těchto sdělení, přičemž v těchto sdělení žalobkyně neuváděla totožnost odesílatele, jehož jménem se komunikace uskutečňovala, a ani v nich neuváděla platnou adresu, na kterou by se adresát mohl případně obrátit s odmítnutím zasílání dalších sdělení. Kasační stížnost Nejvyšší správní soud zamítl a potvrdil tak rozhodnutí Úřadu, kterým se žalobkyni za uvedené delikty ukládá pokuta ve výši 1,4 mil. Kč.

Nejvyšší správní soud svým rozhodnutím potvrzuje dlouhodobý výklad Úřadu v otázce zasílání obchodních sdělení. Úřad opakovaně zdůrazňoval, že odpovědnost za šíření obchodních sdělení nese jak samotný rozesílatel, tak i ten, kdo zasílání obchodních sdělení inicioval ve svůj prospěch – ať už objednáním služby, udělením příkazu nebo jiného pokynu, včetně využívání nástrojů lead marketingu apod. Jak již bylo uvedeno výše, tato odpovědnost je objektivní – osoba, v jejíž prospěch jsou obchodní sdělení šířena tak odpovídá i za případný exces těchto rozesílatelů. Úřad proto zdůrazňuje, že je nezbytné, aby si všichni šiřitelé těchto sdělení (zadavatelé i faktičtí rozesílatelé) dostatečně ověřili, že jim adresáti

obchodních sdělení udělili pro zasílání souhlas.

+ Rozsudek Soudního dvora o předběžné otázce týkající se čl. 55 odst. 3 GDPR

V rámci soudního řízení byl účastník a jeho zástupce osloveni novinářem, u kterého si jmenovaní všimli, že disponuje dokumenty z předmětného spisu, ve kterých jsou uvedeny jejich údaje. Státní rada Nizozemska dotčeným sdělila, že novinářům poskytuje určité dokumenty, aby mohli sledovat jednání (kopie návrhu na zahájení řízení, žalobní odpovědi, kopii soudního rozhodnutí apod.), přičemž tyto dokumenty jsou na konci dne zničeny. Účastník a jeho zástupce se následně obrátili na Úřad pro ochranu osobních údajů Nizozemska s žádostí o přezkum dané situace. Úřad však odvětil, že podle čl. 55 odst. 3 GDPR („*Dozorové úřady nejsou příslušné k dozoru nad operacemi zpracování, které provádějí soudy jednající v rámci svých soudních pravomocí*.“) nemá pravomoc vykonávat dozor nad danými operacemi zpracování osobních údajů prováděné Státní radou. Toto rozhodnutí napadl účastník a jeho zástupce u soudu pro centrální Nizozemsko, ten řízení přerušil a obrátil se na Soudní dvůr s předběžnou otázkou, zda má být čl. 55 odst. 3 GDPR vykládán v tom smyslu, že do soudních pravomocí patří i umožnění nahlížet do procesních písemností, které obsahují osobní údaje, poskytnutím jejich kopií novinářům.

Soudní dvůr pak s důrazem na ochranu záruk nezávislosti a nestrannosti soudní moci došel k závěru, že článek 55 odst. 3 GDPR skutečně stanoví, že operace zpracování, které provádějí soudy jednající v rámci svých soudních pravomocí, nespadají do pravomoci dozorového úřadu. Z pravomoci dozorového úřadu jsou tak vyloučeny operace zpracování, u nichž by dohled nad nimi ze strany dozorového orgánu mohl přímo nebo nepřímo ovlivnit nezávislost jejich členů nebo ovlivnit jejich rozhodnutí.

S ohledem na výše uvedené Soudní dvůr na položenou otázku odpovídá tak, že čl. 55 odst. 3 GDPR musí být vykládán v tom smyslu, že dočasné poskytnutí procesních písemností, které obsahují osobní údaje, novinářům ze strany soudu, aby mohli lépe informovat o průběhu soudního řízení, spadá do oblasti jednání tohoto soudu v rámci jeho soudních pravomocí a je tedy nepřezkoumatelné dozorovým úřadem.

+ Rozsudek Soudního dvora k souhlasu zákazníka telekomunikačního operátora

V rozsudku ze dne 27. 10. 2022 dospěl Soudní dvůr k závěru, že k uvedení osobních údajů účastníka služeb telekomunikačního operátora v účastnických seznamech zveřejňovaných jinými poskytovali, něž je tento operátor, je vyžadován souhlas tohoto účastníka ve smyslu GDPR.

Soudní dvůr v dané věci uvádí, že účastníci jsou před zápisem do účastnických seznamů informováni o jejich účelu, a to včetně možnosti vyhledávání těchto údajů. To pak umožňuje účastníkům vyslovit souhlas s uvedením jejich údajů v těchto seznamech, který je pro zpracování údajů nezbytný.

Tento souhlas se váže pouze na zveřejnění osobních údajů v daném seznamu, nikoli ke konkrétní totožnosti poskytovatele seznamu – nebrání tedy tomu, aby byly údaje předávány dalším poskytovatelům účastnických seznamů (opětovný souhlas se nevyžaduje). Nicméně pokud by strana, která údaje shromažďuje (nebo třetí strana), chtěla údaje využít pro jiné účely, bude potřeba získat od účastníka obnovený souhlas, který musí být svobodný, konkrétní, informovaný a jednoznačný.

NEJSTE NA TO SAMI
YOU'RE NOT ALONE
SIE SIND NICHT ALLEIN

www.ak-haven.cz

HAVEN ++ HAVEN ++ HAVEN ++ HAVEN