PRO

OCHRANA OSOBNÍCH ÚDAJŮ V PRAXI

LETNÍ SPECIÁL

Číslo 7–8/2023, ročník III. Měsíčník SMS - služby s. r. o. www.dpopro.cz

Pro životaschopné zajištění ochrany osobních údajů v jakékoli organizaci považuji za klíčové povědomí a důvěru

Banky patří mezi největší zpracovatele osobních údajů v České republice a ani ta centrální – ČNB nezůstává v tomto ohledu pozadu. O tom, jak probíhá zpracování osobních údajů v této instituci a čím se liší od zpracování u běžných bank, jsem si povídala s jejím pověřencem Ladislavem J. A. Maczvaldou.

Rozhovor

Česká bankovní asociace vytvořila pracovní skupinu pro ochranu osobních údajů v rámci implementace obecného nařízení (GDPR). Spolupracovala tato skupina s ČNB?

ČBA, přesněji zmiňovaná pracovní skupina pro ochranu osobních údajů iniciovala diskusi s ČNB v souvislosti s implementací GDPR v bankovním sektoru. Následně ČNB již s touto pracovní skupinou přímo nespolupracovala. V rámci spolupráce mezi ČBA a ČNB se ochrana osobních údajů řeší jako dílčí aspekt určitého projektu, a to přímo s věcně zaměřenou pracovní skupinou; přičemž pracovní skupinu pro ochranu osobních údajů vnímám spíše jako podpůrně průřezovou.

Krásné prázdninové dny, vážení čtenáři!

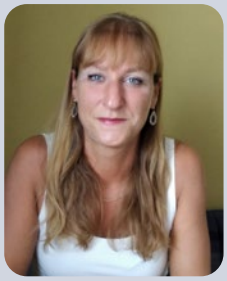
Patrně všechny větší organizace mají v současné době již vytvořený a zavedený formální rámec ochrany osobních údajů. Ochrana osobních údajů ve většině z nich i přesto zůstává okrajovou záležitostí, míní pověřenec Ladislav J. A. Maczvalda. Rozhovorem s ním otevíráme prázdninové dvojčíslo časopisu DPO PRO, měsíčníku nejen pro pověřence pro ochranu osobních údajů. Co dalšího v něm najdete?

Ve zpravodaji ani tentokrát nechybí aktuální informace o činnosti Spolku pro ochranu osobních údajů, který ani o prázdninách tak úplně nespí a na podzim připravuje vzdělávací akce i výroční konferenci.

V březnu italský úřad pro ochranu osobních údajů (Garante) oznámil, že službě ChatGPT zakázal zpracovávat data místních uživatelů a prošetří činnost firmy, která za programem stojí. Itálie se tak zařadila mezi první státy, které ChatGPT zakázaly. Co bylo důvodem? Dočtete se to v článku Václava Řehoře.

Od 1. srpna přichází další zkouška, která otestuje funkčnost GDPR v mnoha organizacích. Tou je nový zákon č. 171/2023 Sb., o ochraně oznamovatelů. Zákon o whistleblowingu. Předpis, který důvěrnost a důraz na soukromí staví na první místo. Na co myslet při implementaci whistleblowingu z pohledu GDPR? Shrnutí toho nejdůležitějšího přináší článek Jiřího Hradského.

V naší globalizované společnosti dochází k velkému množství přeshraničních přenosů osobních údajů, které navíc usnadňuje elektronická komunikace. Ta však má i svá úskalí, protože sdílení dat může probíhat i jakoby mimoděk. Jaká jsou rizika přeshraničního předávání osobních údajů v rámci koncernu? Tímto tématem se zabýval Alexander Kult.



Ptáte se, zda je to vše? Kdepak. Časopis obsahuje i další informace a inspirativní podněty pro vaši práci.

Ničím nerušené čtení a pohodové dny vám přeje

Eva Janečková
šéfredaktorka

Zabývá se vůbec ČNB metodickým vedením bank i v této oblasti?

ČNB neposkytuje metodické vedení k problematice ochrany osobních údajů zpracovávaných v rámci bankovního sektoru. Určitý údaj v bankovním sektoru může být předmětem dohledu různých dohledových orgánů, a to dle jejich působnosti stanovené zákonem. ČNB není dozorovým orgánem v oblasti ochrany osobních údajů – působnost v této oblasti náleží Úřadu pro ochranu osobních údajů. S tím pak souvisí i zvyšování povědomí v oblasti této působnosti, případně i metodické vedení. Z mého pohledu i dosavadní zkušenosti je Úřad pro ochranu osobních údajů aktivní a vždy ochotný např. ke konzultaci, na druhou stranu je nutné mít na paměti, že zde není od toho, aby nahrazoval činnost jednotlivých správců.

Banky obvykle předávají osobní údaje do zahraničí. Podle informací poskytnutých podle čl. 13 a 14 obecného nařízení (GDPR) tak činí i ČNB. Kam jsou osobní údaje takto předávány, za jakými účely a jak se ČNB vypořádává s touto problematickou činností?

Ačkoli předpokládám, že zahraničím se v tomto případě myslí především třetí země či mezinárodní organizace ve smyslu kapitoly V GDPR, pro úplnost uvedu, že ČNB na úrovni EU spolupracuje s jinými orgány dohledu nad finančním trhem, včetně institucí EU; zpracování osobních údajů v těchto případech probíhá v režimu GDPR, případně také EUDPR, je-li příjemcem instituce EU. Jedná-li se o již zmíněné předání osobních údajů do třetí země či mezinárodní organizaci, v praxi dochází k předání osobních údajů za účelem výkonu dohledových činností ČNB, tedy v souvislosti s plněním závazků, jež pro ČNB vyplývají z participace na mezinárodní dohledové spolupráci nad finančním trhem. Pro lepší představu, může se jednat o předávání osobních údajů např. v rámci výkonu dohledu v oblasti AML/CFT, odborné péče a ochrany spotřebitele, plnění obezřetnostních požadavků atd. Příjemci jsou jiné orgány dohledu nad finančním trhem, přičemž alespoň teoreticky tyto orgány mohou být z jakékoli třetí země, pro níž je k dispozici příslušné rozhodnutí Evropské komise o odpovídající ochraně, nebo třetí země, v níž působí orgány dohledu nad finančním trhem, jež jsou signatáři správního ujednání pro předávání osobních údajů mezi úřady pro finanční dohled v Evropském hospodářském prostoru a úřady pro finanční dohled mimo Evropský hospodářský prostor.

Ladislav J. A. Maczvalda
působí jako pověřenec pro ochranu osobních údajů ČNB. Vystudoval psychologii na Filozofické fakultě Masarykovy univerzity a dále právo na Právnické fakultě Univerzity Karlovy a evropské právo na Faculteit der Rechtsgeleerdheid Universiteit Leiden. Získal řadu certifikací v oblasti ochrany osobních údajů (CIPP/E, CIPM, CIPT, EIPA Data Protection Certification). V rámci profesního působení ve finančních a EU institucích se vždy věnoval i oblasti ochrany osobních údajů. V ČNB působí od roku 2016, implementoval GDPR v ČNB a nadále se zde komplexně podílí na zajišťování ochrany osobních údajů. Vzhledem k působnosti a rozsahu činností ČNB se zabývá problematikou ochrany osobních údajů na mezinárodní, evropské i národní úrovni.

Jedná se o problematickou záležitost?

V tomto případě ne – ačkoli řada rozhodnutí Evropské komise o odpovídající ochraně je použitelná pouze pro „soukromoprávní" oblast, a nikoli i pro oblast „veřejnoprávní", do níž spadá i výkon dohledových činností ČNB, v tomto případě ČNB spoléhá na zmíněné správní ujednání, jež je nástrojem „ušitým na míru" pro předávání osobních údajů v rámci mezinárodní dohledové spolupráce nad finančním trhem. Jedná se o správní ujednání, jež zahrnuje vhodné záruky a vymahatelná a účinná práva subjektu údajů, tedy nástroj pro předávání osobních údajů podle čl. 46 odst. 3 písm. b) GDPR, na jehož vypracování spolupracovaly instituce EU a národní orgány dohledu nad finančním trhem. Následně byl tento nástroj schválen jak Evropským sborem pro ochranu osobních údajů, tak jednotlivými národními dozorovými orgány v oblasti ochrany osobních údajů, včetně Úřadu pro ochranu osobních údajů. Pro specifické situace podle čl. 49 GDPR se pak jako případná záloha dají použít výjimky, jejichž využívání bylo předmětem živých diskusí s Evropským sborem pro ochranu osobních údajů, zejména v souvislosti s přijetím pokynů 2/2018 k výjimkám podle čl. 49 nařízení (EU) 2016/679.

Dlouhodobě je jedním ze sporných témat zpracování osobních údajů, včetně nahlížení bankami, v rámci Bankovního registru klientských informací (BRKI) a Nebankovním registru klientských informací (NRKI). Jaký je vztah ČNB k těmto registrům a způsobu zpracování osobních údajů? Řeší nějakým způsobem ČNB i tuto činnost?

Z pohledu zákonem vymezených činností ČNB nedohlíží na BRKI ani na NRKI. Z hlediska ochrany osobních údajů jde o samostatné správce – ČNB a CNCB (provozovatel NRKI), a dále o zpracovatele CBCB (provozovatel BRKI), jenž zpracovává osobní údaje pro banky, jakožto společné správce. Nastavení ochrany osobních údajů v rámci BRKI a NRKI je záležitostí příslušných správců, nejde o záležitost ČNB.

Na webových stránkách ČNB je uvedeno, že „ČNB zpracovává osobní údaje za účelem evidence činností a přístupů uživatelů do informačních systémů, jakož i evidence přístupů k aktivům ČNB. Právním základem pro tento účel zpracování osobních údajů je ochrana oprávněných zájmů ČNB v oblasti bezpečnosti informačních systémů, jakož i plnění právních povinností v oblasti kybernetické bezpečnosti." Můžete tuto informaci blíže vysvětlit? Komu jsou přístupné informační systémy ČNB?

K vybraným informačním systémům provozovaným ČNB mají přístup externí uživatelé. V praxi se jedná např. o informační systém pro sběr dohledových údajů, kdy externí uživatel – fyzická osoba zastupující dohlížený subjekt, např. banku, poskytne požadované informace týkající se tohoto dohlíženého subjektu. Dalším příkladem z praxe může být informační systém pro provádění plateb, kdy externí uživatel – fyzická osoba zastupující účastníka platebního systému, např. banku,

Další obsah

sleduje toky celkových objemů plateb za příslušnou banku. V těchto případech tedy ČNB zpracovává osobní údaje takového externího uživatele, a to jednak jeho přístupové údaje, a dále údaje týkající se jeho přístupů a činností, čímž se samozřejmě rozumí sběr auditních logů.

Veřejnost může využít i služeb badatelny archivu ČNB. Obsahují archivní materiály i osobní údaje žijících lidí? Pokud ano, jak je ošetřeno nahlížení do těchto dokumentů?

V první řadě je nutno uvést, že archivace, k níž dochází v ČNB, je archivací ve veřejném zájmu. Ačkoli GDPR mimo jiné pro tyto účely stanovuje určité odchylky, pořád jde o zpracování osobních údajů, na něž se vztahují legislativní požadavky. Přestože mezi vznikem dokumentu a jeho zařazením mezi archiválie může uplynout doba i v řádu desítek let, mohou se vyskytnout případy, kdy bude archiválie obsahovat osobní údaje žijícího člověka. Požádá-li badatel o takovouto archiváliі, obdrží pouze kopii bez osobních údajů žijících lidí, přesněji osobní údaje těchto lidí jsou zde začerněny.

ČNB je velká instituce s mnoha kompetencemi. U takto velkých správců osobních údajů není postavení pověřence pro ochranu osobních údajů vždy jednoduché, obtížné bývá přimět ke spolupráci všechny odpovědné osoby a útvary. Daří se vám dosáhnout toho, aby vše fungovalo k vaší spokojenosti?

Patrně všechny větší organizace mají v současné době již vytvořený a zavedený formální rámec ochrany osobních údajů, ochrana osobních údajů ve většině z nich i přesto zůstává okrajovou záležitostí. Pověřenec pro ochranu osobních údajů přitom představuje úhelný kámen rámce ochrany osobních údajů v organizaci a plněním svých úkolů, jež jsou v řadě případů nad rámec výčtu v čl. 39 GDPR, obvykle vymezuje i úroveň ochrany osobních údajů v organizaci. Já osobně pro životaschopné zajištění ochrany osobních údajů v jakékoli organizaci považuji za klíčové povědomí a důvěru. A to se netýká jen toho, že zaměstnanci, tedy řadoví zaměstnanci i vedoucí zaměstnanci všech stupňů, jsou schopni identifikovat, že se určitá situace týká ochrany osobních údajů, ale že mají představu i o tom, jak tuto situaci řešit, včetně např. povědomí o tom, že nejsou-li si zcela jisti, jak postupovat, mohou požádat pověřence o radu. Zaměstnanci jsou v ČNB vedeni k tomu, že ochrana osobních údajů je komplexním a společným dílem – bez jejich zapojení nelze řádně plnit požadavky na ochranu osobních údajů. Důvěra pak souvisí s tím, že rady a možné návrhy řešení poskytnuté pověřencem jsou praktické a zasazené do reality, tzn. že sledují potřeby a současně berou v potaz možnosti dané organizace. Pokud bych vyšel z těchto dvou aspektů, vzhledem k tomu, že se dle mých připomínek či doporučení postupuje a ročně obdržím od zaměstnanců stovky žádostí o poskytnutí poradenství, mohu konstatovat, že jsem s úrovní spolupráce při zajišťování ochrany osobních údajů v ČNB spokojen.

Rozhovor vedla Eva Janečková

Spolek nespí ani o prázdninách. Na podzim připravuje vzdělávací akce i výroční konferenci

Léto je i pro Spolek pro ochranu osobních údajů spíše ve znamení odpočinku a přípravy na podzimní aktivity. S jednou výjimkou: 20. července se uskutečnil online workshop členky Výboru Spolku Jany Pattynové na téma Metaverse z pohledu regulace a ochrany dat. Workshop byl určen pro členské asociace Evropské federace pověřenců pro ochranu osobních údajů, které je Spolek zakládajícím členem.

Stanoviska a jiná aktuální témata

Ještě před prázdninami jsme se také věnovali stanoviskům na aktuální témata a otázky týkající se různých aspektů zpracování dat a ochrany soukromí. Spolek připravil Stanovisko k omezování dostupnosti rodných čísel, Vyjádření k návrhu metodiky ÚOOÚ k provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů a Stanovisko k problematice zveřejňování údajů z datových schránek jako otevřených dat.

Řadu vzdělávacích akcí plánuje Spolek i na podzimní měsíce

V září se uskuteční seminář, na kterém Jakub Berthoty ze společnosti Dagital Legal seznámí účastníky se zkušenostmi získanými během schvalování závazných podnikových pravidel slovenským dozorovým úřadem. Na Slovensku se jednalo o první schválení tohoto nástroje pro předávání osobních údajů mimo Evropskou unii, resp. Evropský hospodářský prostor. Žádná závazná podniková pravidla dosud neschválil ani český dozorový úřad, kterým je Úřad pro ochranu osobních údajů. Pro členy Spolku budou praktické zkušenosti a poznatky ze schvalování v praxi přínosné.

Další přednášky a semináře se dotknou zejména otázek kybernetické bezpečnosti, nových právních předpisů či aktuální judikatury v oblasti zpracování osobních údajů a ochrany soukromí.

Začne sběr nominací na ocenění nejlepších pověřenců roku 2023

Na podzim rovněž Spolek zahájí sběr nominací na ocenění Pověřenec pro ochranu osobních údajů roku 2023. Začne tak šestý ročník, ve kterém opět dojde na ocenění nejlepších pověřenců z veřejného i soukromého sektoru. Záštitu tomuto ročníku udělil místopředseda vlády pro digitalizaci a ministr pro místní rozvoj Ivan Bartoš.

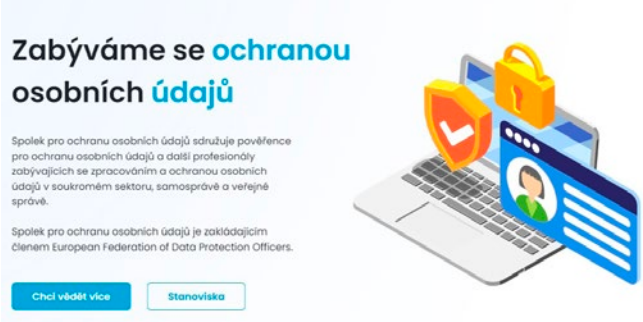
Jak dopadla soutěž o nejlepšího pověřence na Slovensku?

V červnu vyhlásil nejlepší pověřence také náš partnerský slovenský Spolok pre ochranu osobných údajov. Pověřencem roku za veřejný sektor se stal Miroslav Ilavský, který funkci pověřence vykonává pro více správců a zpracovatelů, včetně města Stupava. V soukromém sektoru pak byla oceněna Lucia Váryová, která je pověřenkyní ve společnosti Slovak Parcel Service, s.r.o. Více se dočtete ve zprávě na webových stránkách slovenského Spolku.

Tradiční výroční konference Spolku se koná 5. října

Vrcholem podzimních akcí bude tradiční výroční konference Spolku, která se koná už po sedmé, tentokrát ve čtvrtek 5. října v Praze. Účastníci se mohou těšit na řadu zajímavých českých i zahraničních hostů a workshopy na aktuální témata. Registrace pro zájemce je otevřena od poloviny července.

Více informací jak o výroční konferenci, tak o dalších aktivitách a vzdělávacích akcích Spolku lze najít na našich nových webových stránkách na známé adrese: www.ochranaudaju.cz.



Zablokování ChatGPT v Itálii a vztah GDPR k AI

Od loňského listopadu v médiích a veřejném prostoru stále častěji slýcháme o umělé inteligenci a jejím využití snad ve všech možných sférách. Právě tehdy došlo k významnému milníku, když firma OpenAI zpřístupnila veřejnosti k používání svého chatbota OpenGPT. Technologie postupují mílovými kroky vpřed. Jak je to ale s dodržováním stávající legislativy?

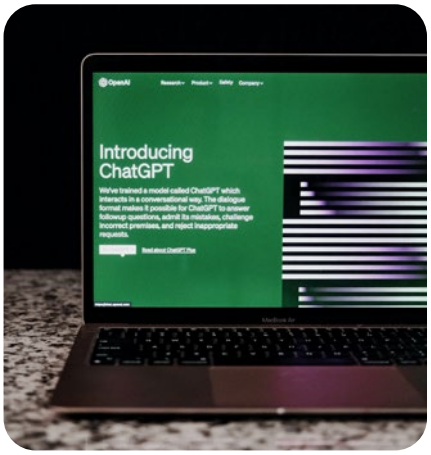
Itálie se v oblasti uplatňování GDPR v technologiích řadí mezi nejaktivnější

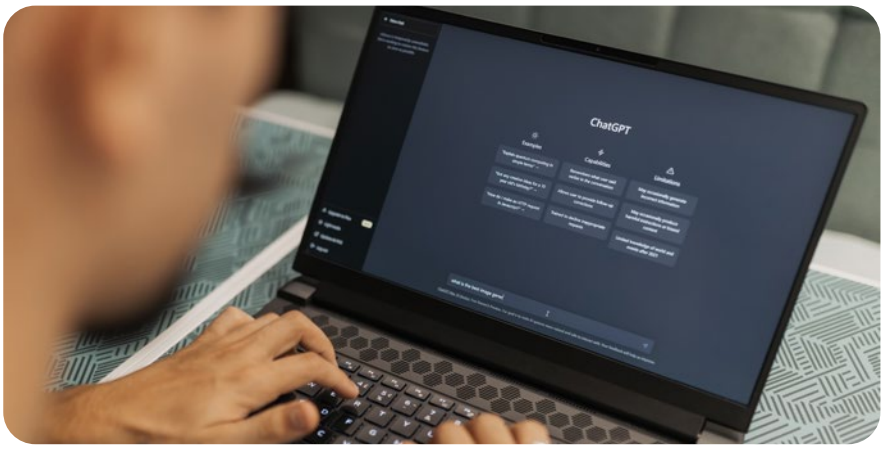
V březnu italský úřad pro ochranu osobních údajů (Garante) oznámil, že službě zakázal zpracovávat data místních uživatelů a prošetří činnost firmy, která za programem stojí. Itálie se tím zařadila mezi první státy, které ChatGPT zakázaly. Do té doby to byly nedemokratické země jako Rusko, Čína nebo Írán. Na západě blokují ChatGPT některé školy, aby technologie nemohla být použita k podvádění při výuce. Nicméně Itálie se v oblasti uplatňování GDPR v technologiích řadí mezi nejaktivnější. Garante byl mezi prvními při zákazu AI chatbota Replika, pokutování softwaru na rozpoznání obličeje Clearview AI i při omezování sítě TikTok v Evropě.

Co vlastně stálo za zablokováním ChatGPT?

Podle Garante aplikace neověřuje věk uživatelů (přitom se jedná o službu, která by měla být dostupná až od 13 let), dále sbírá a využívá osobní údaje uživatelů bez jejich informovaného souhlasu s cílem dalšího vylepšování funkčnosti jazykového modelu. Navíc 20. března došlo ke ztrátě údajů týkajících se uživatelů a informací o platbách předplatitelů placené služby, a tím tedy k porušení ochrany osobních údajů. Díky tomu se například zjistilo, že chyba v jedné z datových knihoven umožňovala některým uživatelům zobrazit historie chatu jiných aktivních uživatelů.

Podle Garante je nejzávažnějším důvodem pro pozastavení služby absence právního základu, který by ospravedlňoval masivní shromažďování a uchovávání osobních údajů za účelem trénování algoritmů, na nichž je fungování platformy založeno. Informace poskytnuté ChatGPT ne vždy odpovídají skutečným údajům, a tak dochází k nepřesnému zpracování údajů. Úřad proto vydal seznam opatření, která musí provozovatel splnit pro povolení služby:





- **OpenAI na svém webu zveřejní návrh dokumentu popisující logistiku a zpracování dat a práva uživatelů i neuživatelů. Informace o zpracování dat se zobrazí všem registrovaným.**
- **OpenAI změní podmínky používání služby tak, aby se sběr dat neopíral o plnění smlouvy, nýbrž buď o aktivní souhlas, případně o konstrukt oprávněného zájmu.**
- **Uživatelé i neuživatelé mají nárok na opravu svých dat, pokud byla nesprávně vygenerována, případně na výmaz, pokud opravu nelze provést. OpenAI na to poskytne snadno dostupné nástroje.**
- **Uživatelé i neuživatelé mají nárok odmítnout používání osobních dat pro účely trénování algoritmu.**
- **Italští uživatelé a uživatelky ChatGPT musí potvrdit, že je jim 18 nebo více let. Do 31. května musí provozovatel předložit plán, jak bude věk ověřovat dále. Do 30. září 2023 musí z platformy odstranit účty dětí do 13 let věku a účty dětí ve věku 13–18 let, jejichž rodiče s používáním služby nesouhlasili.**
- **OpenAI do 15. května podpoří osvětovou kampaň v Itálii, která veřejnost informuje o tom, že její data používá pro trénink algoritmu.**

Itálie neblokovala ChatGPT ze své strany, požádala provozovatele, aby přístup Italům ke službě zamezil. Společnost tomu vyhověla a chatbot geoblokovala. Společnost OpenAI dostala 20 dní na nápravu (do 30. dubna 2023), jinak by jí hrozila pokuta až 20 milionů EUR nebo čtyři procenta z ročních tržeb. Dne 28. dubna Sam Altman, CEO OpenAI, bez dalších podrobností na svém Twitteru napsal: *„Jsme nadšeni, že ChatGPT je v Itálii opět dostupný."* Podle dalších vyjádření společnosti byly všechny připomínky *„vyřízeny nebo vyjasněny"*. Nástroj nyní ověřuje věk a uživatelé mohou zvolit možnost nezpracovávání dat pro další učení chatbota. Italský regulátor oznámil, že vítá opatření, která firma přijala, a bude pokračovat v činnostech zaměřených na zjišťování informací ohledně OpenAI i pod záštitou ad-hoc pracovní skupiny, kterou zřídila Evropská rada pro ochranu údajů (EDPB). Přijatá opatření jsou dostatečná na to, aby italské úřady povolily OpenAI v zemi působit, a očekává se, že společnost splní další požadavky. Mezi nimi je i informační kampaň o právech Italů odmítnout zpracování jejich osobních údajů za účelem trénování algoritmů umělé inteligence.

Celá situace vzbudila velký zájem i ze strany dalších regulátorů

Francie, Irsko a Německo si vyžádaly další informace a projevily zájem na koordinovaném postupu ohledně ochrany dat. Rovněž další země (nejen v rámci EU) začínají s procesem revize a hodnocení dopadů používání umělé inteligence.

Proces vzbudil velký zájem veřejnosti, a i když ChatGPT patří mezi největší hráče na poli jazykových modelů, rozhodně není jediným. Jedná se o jednu aplikaci, která je zaměřená pouze na tvorbu textů. Italský postup a celkově evropské vnímání dopadů technologií nejen na soukromí uživatelů určitě hrály roli v rozhodnutí firmy Google znepřístupnit svého chatbota Bard pro celou EU. I další firmy spíše vyčkávají na rozhodnutí týkající se plánu Evropské unie pro oblast AI (tzv. AI Act).

EU by se v případě přijetí AI Act stala prvním velkým globálním trhem s jasnými pravidly pro regulaci umělé inteligence

Pokud by byl AI Act přijat, stane se EU prvním velkým globálním trhem, který bude mít jasná pravidla pro regulaci umělé inteligence. Návrh legislativy počítá s rozřazením využití AI do čtyř kategorií podle rizika. V první kategorii je použití umělé inteligence nepřípustné – jedná se o vytváření sledovacích algo-

ritmů podobných čínskému kreditovému systému. Druhou kategorií je nasazení AI do kritických systémů (energetika, soudy...). To je klasifikováno jako vysoce rizikové (high risk) a využití AI podléhá náročným standardům. Generativní AI a jazykové modely, mezi které se řadí i ChatGPT, spadají pod „transparency systems" s nižšími nároky na regulaci a volnějším použitím. Ostatní využití AI (herní systémy, spam filtry apod.) budou ponechány z větší části bez regulace. AI Act se tedy zabývá tím, jak využití umělé inteligence klasifikovat a následně regulovat podle úrovně rizikovosti. Nastavuje základní pravidla používání a učení umělé inteligence na půdě EU a v předstihu se chystá na éru pokročilých generativních AI, které se na trhu objeví jako nástupci současných technologií. Evropa se tím chce vyhnout chybě z minulosti, kdy nedokázala účinně regulovat sociální sítě a následně se pouze snažila dohnat vývoj. Akt o umělé inteligenci byl schválen plenárním zasedáním Evropského parlamentu a nyní se jím bude zabývat Rada EU.

AI Act se ovšem nedotýká GDPR a stejně tak není upraveno postavení DPO

Společnosti a systémy spadající pod AI Act musí splňovat i pravidla GDPR, přestože se tato pravidla často překrývají. I u aplikací, které splní předpisy vyplývající z aktu o umělé inteligenci, bude tedy potřeba, aby stávající regulátoři a DPO kontrolovali správnost a dodržování pravidel ochrany osobních údajů. A také aby postupovali podobně, jako italský úřad v případě ChatGPT.

Václav Řehoř
Autor je pověřenec pro ochranu osobních údajů

Whistleblowing – nová výzva pro společnosti i jejich DPO

Už je to více než pět let od účinnosti nařízení, které způsobilo revoluci v oblasti ochrany osobních údajů. Od té doby bylo GDPR několikrát „podrobeno zkoušce". Například v době covid-19 se ukázalo, jak jsou společnosti připraveny na zpracování zvláštních kategorií osobních údajů. V minulém roce se společnosti musely začít prát se soubory cookies, které prostě, chtě nechtě, s GDPR souvisí.

Od 1. srpna 2023 přichází další zkouška, která otestuje funkčnost GDPR v mnoha organizacích. Tou je nový zákon č. 171/2023 Sb., o ochraně oznamovatelů. Zákon o whistleblowingu. Předpis, který důvěrnost a důraz na soukromí staví na první místo. Na co myslet při implementaci whistleblowingu z pohledu GDPR? Tady je shrnutí toho nejdůležitějšího.

Jak spolu whistleblowing a GDPR souvisí?

Zákon o ochraně oznamovatelů zavádí povinnost vytvořit vnitřní oznamovací systém u společností nad 50 zaměstnanců, veřejných zadavatelů, obcí, orgánů veřejné moci a dalších subjektů uvedených v § 8 daného zákona. Pod pojmem vnitřní oznamovací systém si nemusíte představovat software, nýbrž souhrn procesních pravidel, která zajistí, že každý oznamovatel může v klidu a bezpečí oznámit protiprávní jednání na pracovišti.

Zákon zavádí také novou pozici příslušné osoby, neboli řešitele oznámení, který má za úkol oznámení přijímat, vyřizovat a navrhovat společnosti opatření.

Každý oznamovatel tak musí být chráněn, pokud učiní oznámení o trestném činu, přestupku nad 100 000 Kč, porušení předpisů v oblasti životního prostředí, ochrany spotřebitele apod. Ochrana spočívá v zajištění, že nebudou vůči oznamovateli přijata žádná odvetná opatření a že se bude společnost jeho oznámením zabývat a provede nápravu.

To tedy v praxi znamená, že každá povinná společnost musí přijmout interní předpisy, jmenovat řešitele oznámení, informovat oznamovatele a zajistit další procesní oblasti spojené s whistleblowingem.

Oblast ochrany oznamovatelů s sebou přináší základní povinnosti související s ochranou osobních údajů. Český zákon o ochraně oznamovatelů se vydal cestou, kdy jsou chráněna jen oznámení, ve kterých je oznamovatel identifikován. Z tohoto důvodu se budou ve společnostech hromadit evidence, které z povahy věci budou obsahovat osobní údaje pracovníků – oznamovatelů. Co si musí tedy společnosti pohlídat?

- Poučení všech pracovníků o pravidlech nakládání s osobními údaji ve společnosti
- Informování subjektů údajů o zavedeném vnitřním oznamovacím systému
- Vytvoření záznamu o činnosti zpracování
- Vyřešení procesních otázek práva na přístup k osobním údajům
- Uložení záznamů v souvislosti s whistleblowingem

Poučení všech pracovníků o pravidlech nakládání s osobními údaji ve společnosti

Jednou z oblastí, na kterou se vztahuje zákon o ochraně oznamovatelů, je porušení pravidel v oblasti ochrany osobních údajů, soukromí a bezpečnosti sítí elektronických komunikací. Jinými slovy, oznamovatelé jsou chráněni také v případě, že učiní oznámení v souvislosti s tímto odvětvím.

Pokud je tak například zaměstnanec na pracovišti svědkem situace, v rámci které jiný zaměstnanec zasílá obchodní sdělení na všechny zákazníky – fyzické osoby, může o tom učinit

oznámení podle zákona a zaměstnavatel se tím musí zabývat.

Z tohoto důvodu by si společnosti měly zopakovat základní pravidla nakládání s osobními údaji, aby vše probíhalo v souladu s právními předpisy.

Informování subjektů údajů o zavedeném vnitřním oznamovacím systému

Oznámení obsahuje údaje o jménu, příjmení a datu narození, nebo jiné údaje, z nichž je možné dovodit totožnost oznamovatele. Tak zní ustanovení § 2 odst. 2 zákona o ochraně oznamovatelů. Zákon tedy nepřikládá ochranu anonymním oznámením a dá se předpokládat, že mnoho společností se vydá cestou rozsahu zákona a bude přijímat pouze identifikovaná oznámení.

Tak jako tak je zřejmé, že bude docházet ke zpracování osobních údajů. V podstatě dojde k rozšíření osobních údajů, které budou zaměstnavatelé zpracovávat na základě plnění právních povinností. Společnosti by tak neměly zapomenout na aktualizaci poučení o zpracování osobních údajů vůči oznamovatelům.

Zejména by se společnosti měly zaměřit na uváděný rozsah zpracovávaných údajů v rámci plnění povinností dle zákona o ochraně oznamovatelů, příjemce osobních údajů (pokud je do zpracování zapojený externí řešitel nebo software, který zajišťuje příjem oznámení) a vyřizování práv subjektů údajů. V právech je potřeba zaměřit se zejména na otázku spojenou s vyřízením práva na přístup. To bude totiž specifické v případech, kdy o přístup požádá osoba, u které by vyhovění znamenalo zmaření nebo ohrožení podávaného oznámení. K tomuto viz dále v tomto článku.

Vytvoření záznamu o činnostech zpracování

Jelikož má docházet ke zpracování osobních údajů, bude potřeba také aktualizovat záznamy o činnostech zpracování. V této aktualizaci by neměl být žádný problém. Účelem zpracování bude řešení jednotlivých oznámení o možném porušení stanovených předpisů. Právním základem plnění zákonných povinností dle čl. 6 odst. 1 písm. c) GDPR. Důležité je také popsat všechny příjemce osobních údajů. Každý správce by se měl v záznamech zaměřit také na dobrý popis technických a bezpečnostních opatření, která budou, v souvislosti se zachováním důvěrnosti oznámení, velmi důležitým faktorem dobře nastaveného oznamovacího systému.

Specifika práva na přístup k osobním údajům

Představte si následující příklad. Problémový zaměstnanec se obrátí na řešitele oznámení dle zákona o ochraně oznamovatelů (například interního pracovníka, který dostal tuto agentu na starost) a požádá ho o přístup k osobním údajům, které se týkají jeho osoby. Zároveň v souvislosti s chováním tohoto zaměstnance přišlo v minulosti již několik oznámení, tudíž společnost bezesporu zpracovává osobní údaje o této osobě.

Otázkou tedy je: *„Musí společnost žádosti vyhovět?"*

Nemusí. Řešitel oznámení v tomto případě musí vyhodnotit, zda by vyhověním práva nedošlo k maření prošetřování oznámení, ztížení přijetí nápravných opatření či odhalení totožnosti oznamovatele. Zajímavý závěr přineslo Ministerstvo spravedlnosti na své osvětové stránce k whistleblowingu, kde uvedlo: *„O výsledku posouzení žádosti pak příslušná osoba informuje přímo žadatele, bude-li takový postup adekvátní."*

Z tohoto závěru tak vyplývá, že v některých případech nemusí příslušná osoba (řešitel oznámení) informovat o odmítnutí žádosti ani samotného žadatele, pokud by tím byl zmařen účel. Například by tím vyšlo najevo, že je aktuálně projednáváno oznámení v souvislosti s tímto žadatelem. Jde ale o oblast, která prozatím nebyla konzultována s Úřadem pro ochranu osobních údajů, a lze předpokládat, že ten se k celé problematice v budoucnu ještě vyjádří.

Pokud by žádost o vyřízení tohoto práva přišla přímo pověřenci pro ochranu osobních údajů, nesmí se touto žádostí DPO zabývat a musí ji postoupit přímo řešiteli oznámení. Důvodem je, že k oznámením má přístup pouze tento řešitel a nikdo jiný. Proto ani fakticky DPO nemůže takovou žádost vyřídit.

Uložení záznamů v souvislosti s whistleblowingem

Jednou z dalších oblastí, kterou musí každá povinná osoba řešit, je nastavení doby uložení dokumentace související s podanými oznámeními. Odpověď na otázku, jak dlouho dokumentaci uchovávat, upravuje § 21 odst. 2 zákona o ochraně oznamovatelů.

Lhůta je nastavena na pět let ode dne přijetí oznámení. Po tuto dobu tedy musí každá povinná společnost uchovávat veškerou dokumentaci a oznámení. Pokud se tedy na společnost obrátí bývalý zaměstnanec, který dostal na základě podaného oznámení výpověď, s žádostí o výmaz svých osobních údajů, nemusí zaměstnavatel této žádosti vyhovět také v rozsahu zákona o ochraně oznamovatelů.

Další specifika k zamyšlení

Dalšími oblastmi, které uvádíme k zamyšlení pro všechny, kteří mají na starost kontrolu implementace whistleblowingu ve společnosti, jsou bezesporu zpracovatelské smlouvy s poskytovateli software pro řešení oznámení. Externí poskytovatelé takových software zajišťují minimálně uložení osobních údajů. Další specifickou oblastí, která bude mít dopad na ochranu osobních údajů, jsou externí řešitelé oznámení. Z povahy věci musí být řešitelé oznámení nestranní a nemohou dostávat pokyny pro svou funkci, které by mohly ohrozit vyřizování oznámení. Z tohoto důvodu vidíme jako velmi problematické postavení externího řešitele oznámení jako zpracovatele osobních údajů. Spíše se domníváme, že budou v pozici samostatného správce, protože pro zpracování osobních údajů budou určovat vlastní účely a prostředky zpracování.

Existují však také přesně opačné názory ze strany odborné veřejnosti, kdy externí řešitel oznámení bude v pozici zpracovatele osobních údajů, neboť svou činnost vykonává právě pro povinnou osobu, která je správcem osobních údajů. Nezbývá než vyčkat, zda nebude vydáno oficiální stanovisko ze strany dozorového orgánu.

Zákon o ochraně oznamovatelů tak bude velkým milníkem pro společnosti s 50 a více zaměstnanci. Zároveň bude znamenat také výzvu pro ochranu osobních údajů. Pokud působíte ve společnosti jako pověřenci pro ochranu osobních údajů, nezapomeňte správce náležitě poučit a vysvětlit, jaká specifika whistleblowing přináší.

Jiří Hradský
Autor je advokát v SEDLAKOVA LEGAL, s. r. o.

Přeshraniční předávání osobních údajů v rámci koncernu

V naší globalizované společnosti dochází k velkému množství přeshraničních přenosů osobních údajů, které jsou navíc usnadněny elektronickou komunikací. Ta však přináší i svá úskalí, protože sdílení dat může probíhat i jakoby mimoděk. Nejeden z nás si ani nemusí uvědomit, že pouhým uložením dat do sdílené složky či přidáním dalšího adresáta do kopie e-mailu může přenést osobní údaje do států, které nezaručují srovnatelnou ochranu osobních údajů dle požadavků nařízení GDPR.[1] Je třeba si včas uvědomit, že jím poskytovaná ochrana „cestuje" spolu s osobními údaji. Pravidla na jejich ochranu tak platí i nadále bez ohledu na to, kde se nacházejí nebo komu jsou zpřístupněny.

Skupina společností představuje korporátní strukturu, která má úplně anebo alespoň částečně totožnou vlastnickou strukturu. Nejedná se ovšem o konkrétní právní pojem, se kterým bychom mohli v oblasti ochrany osobních údajů bez dalšího pracovat. V užším smyslu se sice může jednat o skupinu společností, která sestavuje konsolidovanou účetní závěrku na základě společného výsledku hospodaření, v širším smyslu ale může jít o jakkoli majetkově propojené společnosti. Můžeme tak hovořit jak o nadnárodních koncernech, tak i menších, lokálních vlastnických strukturách. Vlastnictví zúčastněných společností může být rozděleno mezi více významných akcionářů, kteří mohou mít přístup k jimi zpracovávaným osobním údajům. Zapomínat nesmíme ani na pobočky bez právní subjektivity, které mohou patřit společnostem se sídlem v České republice a být umístěny v zahraničí, nebo se naopak jedná o pobočky společností z jiných členských států EU, ale i z třetích zemí, které jsou umístěny zde.

S ohledem na výše nastíněná specifika je pak třeba nahlížet na důvody, na jejichž základě k předávání osobních údajů dochází. Mnohým z nás se může zdát zcela přirozené sdílet informace o zaměstnancích, klientech či obchodních partnerech s kolegy z jiných společností ve skupině, zahraničních poboček stejné společnosti nebo s pracovníky naší „domácí" společnosti, kteří vycestovali do zahraničí, ať již na dovolenou, nebo na služební cestu. Předány mohou být například e-mailem, telefonicky, ale mohou být rovněž obsaženy ve sdílených informačních systémech. Všechny tyto prvky tak mohou mít zásadní vliv na oprávněnost předávání a zpracování osobních údajů, na které se následně podíváme blíže.

Právní subjektivita – dceřiná společnost či pobočka?

Evropská komise může svým rozhodnutím prohlásit třetí stát (mimo EU/EHP) za zemi poskytující odpovídající úroveň ochrany. Pokud bylo vydáno rozhodnutí o adekvátnosti, osobní údaje mohou být předány jinému subjektu do této země stejně jako v rámci EU. Pokud však rozhodnutí o adekvátnosti vydáno nebylo, musejí být subjektům údajů poskytnuta vymahatelná práva a účinné právní prostředky nápravy a je třeba poskytnout vhodné záruky[2] formálního charakteru (musejí být prokázány při případné kontrole dohledového orgánu).

První variantou je „právně závazný a vymahatelný nástroj mezi orgány veřejné moci nebo veřejnými subjekty". Ten tedy pro zde diskutovanou situaci nepřipadá v úvahu.

Další variantou je využití tzv. závazných podnikových pravidel.[3] Jenže ta musí být schválena příslušným dozorovým úřadem,[4] a to na základě mechanismu jednotnosti. Nejedná se tedy o snadný ani rychlý postup, který by byl hojně využíván. Může totiž zahrnovat několik orgánů dohledu, protože skupina, která žádá o schválení svých závazných podnikových pravidel, může pojímat entity ve více než jednom členském státě. Pokud tedy např. určitý koncern podá svůj návrh závazných podnikových pravidel v České republice Úřadu pro ochranu osobních údajů, měly by se k němu vyjádřit příslušné dohledové orgány ve státech, jejichž příslušnost zahrnuté entity mají s tím, že ÚOOÚ by měl následně sdělit svůj návrh rozhodnutí Evropskému sboru pro ochranu osobních údajů (EDPB), který vydá stanovisko k závazným podnikovým pravidlům. Jakmile jsou závazná podniková pravidla dokončena v souladu se stanoviskem EDPB, příslušný orgán, tedy v tomto případě ÚOOÚ, závazná podniková pravidla schválí. Kvůli složitosti tohoto postupu tak bylo v Evropské unii schváleno doposud pouze 48 závazných podnikových pravidel, v České republice pak ještě žádné. Jedná se tedy spíše o náročné administrativní cvičení než praktickou možnost řešení.

Následují dvě varianty standardních smluvních doložek dle čl. 46 odst. 2 písm. c) a d). Pokud jsou tedy osobní údaje předávány jiné společnosti, ať již v rámci koncernu nebo nikoli, lze tyto smluvní doložky včlenit do smluv o předávání a zpracování osobních údajů. Příjemce se pak musí zavázat, že bude uplatňovat vhodná opatření na ochranu předávaných údajů. Pro použití v zahraniční pobočce bez právní subjektivity však nejsou aplikovatelné, společnost nemůže uzavřít smlouvu s vlastní pobočkou.

Další možností je tzv. schválený kodex chování podle čl. 40 GDPR, který však musí být schválen dozorovým orgánem, v České republice na základě § 54 odst. 1 písm. f) zákona č. 110/2019 Sb., o zpracování osobních údajů. Tyto kodexy však mohou vydávat pouze sdružení nebo jiné subjekty zastupující různé kategorie správců nebo zpracovatelů, nikoliv samy společnosti – ty je mohou pouze dodržovat, tedy v podstatě se dobrovolně přihlásit k jejich aplikaci a učinit je vnitřně závaznými rozhodnutím statutárního orgánu či vnitřním předpisem. EDPB vydal k tvorbě těchto kodexů Pokyny 1/2019 týkající se kodexů chování a subjektů pro monitorování podle nařízení 2016/679.[5] Dále se bez jakéhokoli přímého zmocnění dle GDPR vyjadřuje k návrhům jednotlivých dohledových orgánů členských států na pravidla schvalování těchto kodexů (taková pravidla by vydával náš ÚOOÚ vyhláškou, jejíž vydání zákon předvídá). Jak vidno, opět se jedná o náročný administrativní proces spíše než účelnou možnost řešení. Autorovi není známo, že by nějaký takový kodex chování byl již schválen.

1) 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
2) GDPR, čl. 46.
3) GDPR, čl. 4 odst. 20, čl. 47.
4) GDPR, čl.
5) European Data Protection Board. Pokyny 1/2019 týkající se kodexů chování a subjektů pro monitorování podle nařízení 2016/679. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_cs.pdf

Např. britská Information Commisioner´s Office na svých stránkách uvedla, že žádný takový kodex ještě neschválila.[6] V ČR by jej mohl vydat například Spolek pro ochranu osobních údajů.

Poslední variantou je schválený mechanismus pro vydání osvědčení podle čl. 42 GDPR, který musí být spojen se závaznými a vymahatelnými závazky správce nebo zpracovatele ve třetí zemi uplatňovat vhodné záruky; i ten musí podléhat vydání osvědčení. I český zákon č. 110/2019 Sb., o zpracování osobních údajů, zmiňuje tuto variantu v § 54 odst. 1 písm. d), na jehož základě může ÚOOÚ stanovit vyhláškou kritéria nebo požadavky vydávání takového osvědčení. Taková vyhláška vydána nebyla.

Jak tedy sdílet osobní údaje s pobočkou?

Pokud má společnost zřízenou pobočku, jedná se o její součást, která nemá právní subjektivitu. Takový je nejen pohled českého právního řádu, jedná se o úpravu běžnou v rámci celé EU. Má-li zahraniční společnost v ČR pobočku, pak tato pobočka nemá právní subjektivitu jak v případě společností ze členských států EU/EHP, tak v případě třetích států. Možnosti sdílení osobních údajů jsou však pro oba tyto případy rozdílné. Pobočka společnosti ze státu EU/EHP může se svojí centrálou sdílet veškeré osobní údaje, které zpracovává, protože správcem osobních údajů je společnost jako celek. Pobočka společnosti ze třetího státu však bude v jiném postavení, neboť předání osobních údajů do třetích zemí je bez dalších opatření možná jen do států s odpovídající úrovní ochrany osobních údajů. Takové třetí země jsou považovány z hlediska ochrany osobních údajů za bezpečné, zatímco ostatní státy nikoliv. Lze tak říci, že pobočka společnosti ze třetího státu, který nedisponuje odpovídající úrovní ochrany nebo není schopen ji patřičně demonstrovat, bude muset zachovat subjektivitu svého druhu právě ve vztahu ke správě a zpracování osobních údajů. Není důvod, aby osobním údajům přenášeným v rámci jedné společnosti byla poskytována nižší ochrana než osobním údajům předávaným dceřinou společností mateřské. Je tedy bez pochyb, že aniž by bylo vyhověno požadavkům GDPR, pobočka nebude moci svojí centrále předávat např. informace o výši mezd svých zaměstnanců. Otázkou je, zda lze takto striktní přístup zaujmout k osobním údajům, které nemají citlivý charakter, jako jen např. jméno a příjmení zaměstnance. Pravidla ochrany osobních údajů plně nekorespondují s jedinou (nebo chceme-li společnou) subjektivitou společnosti a její pobočky, resp. GDPR nemá pro takovou situaci jednoznačné řešení. Dle názoru autora je ovšem možné, aby společnost, která zřizuje či má zahraniční pobočku, jednoduše vydala vnitřní předpis, kterým stanoví pravidla přenosu a zpracování osobních údajů, a to bez ingerence jakéhokoli dohledového orgánu. Zřizování poboček namísto dceřiných společností by se tak z pohledu přenosu osobních údajů za hranice EU/EHP mohlo jevit jako výhodnější řešení než zřizování dceřiných společností.

Souhlas se zpracováním

Evropská komise uvádí, že pokud neexistují vhodné záruky, mělo by být předání možné provést například tehdy, pokud fyzická osoba výslovně souhlasila s navrhovaným předáním poté, co jí byly poskytnuty všechny nezbytné informace o rizicích spojených s předáním.[7] Jak známo, souhlas se zpracováním osobních údajů by měl být využíván pouze jako prostředek *ultima ratio*. Tedy jen neexistuje-li jiný právní titul jejich zpracování. S ohledem na výše zmíněný postoj Evropské komise by souhlas se zpracováním osobních údajů, resp. s jejich předáváním do zahraničí, měl být legitimní volbou. GDPR ovšem neobsahuje natolik přesné mantinely, aby byl postoj dohledových orgánů plně předvídatelný. Vyžadování souhlasu po zaměstnancích a klientech však není příliš praktické, neboť pokud někdo souhlas neposkytne nebo jej později odvolá, musely by být jeho osobní údaje zpracovávány jiným způsobem (tedy bez přenosu do třetí země), což zejména v případě hromadného elektronického zpracování představuje zásadní faktické komplikace. Co se týče předávání údajů mezi centrálou a pobočkou, i zde si lze takový souhlas teoreticky představit. Např. i údaje zaměstnance, které jsou jinak zpracovávány na základě titulů, jako je plnění pracovní smlouvy či plnění souvisejících právních povinností, by však v případě, že jejich zpracování proběhne ve třetí zemi, musely být předány pouze se souhlasem. Vzhledem k tomu, že předávání probíhá ve většině případů elektronickou formou, musely by takové přenosy podléhat specifické kontrole, díky které by bylo zajištěno, aby v případě odvolání souhlasu byla dostupnost takových údajů ve třetí zemi eliminována.

Jak upozorňuje ÚOOÚ, nesprávné a nedůvodné vyžadování souhlasu bez odpovídající informace pak může být ve svém důsledku posouzeno jako porušení základních zásad pro zpracování, včetně podmínek týkajících se souhlasu a práv subjektů údajů, ve smyslu článku 83 odst. 5 písm. a) a písm. b) GDPR.[8]

Závěr

Přeshraniční přenos osobních údajů může zahrnovat osobní údaje obchodních partnerů, klientů, ale nejčastěji zaměstnanců. Nejeden z nás si jistě všiml, že osobní údaje často kolují e-mailem v rámci celého koncernu bez ohledu na hranice. Jsou obsaženy v outlookových adresářích, informačních systémech nebo sdílených složkách. Mateřskou společností či centrálou, které patří pobočka, však může být například společnost čínská či americká. Ve vztahu k USA existuje zatím pouze návrh nového rozhodnutí o adekvátnosti právního rámce ochrany osobních údajů.[9] Ve vztahu k Číně jej v brzké době nelze ani očekávat.

Výhodou pobočky oproti dceřiné společnosti je, že společnost, které tato pobočka patří, může vydat vnitřní předpis, jímž předávání osobních údajů do třetích zemí upraví. Obsahově sice bude muset splňovat takové požadavky, aby vyhověla pravidlům GDPR na zabezpečení osobních údajů, ovšem z hlediska formy se zde žádné meze nekladou. Obsah se bude moci do značné míry inspirovat standardními smluvními doložkami, které budou jediným aplikovatelným řešením v případě dceřiných společností. Ve všech případech je však třeba myslet i na zavedení a dodržování technických a organizačních opatření, neboť pouhý formální postup může vést k nemalým sankcím – příkladem z poslední doby může být společnost Meta, které byla nedávno udělena pokuta ve výši 1,2 miliardy eur.

Alexander Kult
Právnická fakulta Univerzity Karlovy,
katedra finančního práva

6) Information Commisioner´s Office. Codes of Conduct. Dostupné z: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/
7) Evropská komise. Jaká pravidla platí, pokud naše organizace předává osobní údaje mimo EU? Dostupné z: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_cs
8) Úřad pro ochranu osobních údajů. K vyžadování souhlasu. Dostupné z: https://www.uoou.cz/k-vyzadovani-souhlasu/ds-5047/p1=5047
9) Evropská komise. Questions & Answers: EU-U.S. Data Privacy Framework, draft adequacy decision. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/cs/qanda_22_7632

Je nové evropské nařízení DORA spíše Pandorou? A co přináší?

Vzpomínáte? Už v minulém roce se časopis DPO věnoval v té době vyjednávanému evropského legislativnímu návrhu nařízení o digitální provozní odolnosti finančního sektoru (DORA) a jeho očekávaným přesahům do další evropské legislativy, GDPR nevyjímajíc. Pojďme si představit nyní již známé požadavky finálního znění nařízení DORA [1] jako takového a stručně nastínit i kontext celkového legislativního rámce, na který tento významný předpis navazuje.

Proč se problematika posílení kybernetické bezpečnosti (nejenom) finančních institucí obecně dostává do centra zájmu?

Důležitost odolných informačních a komunikačních technologií (ICT) se výrazně projevila v souvislosti s pandemií covidu-19, která vedla k bezprecedentnímu nárůstu kybernetické aktivity, což s sebou přináší výzvy, příležitosti, avšak rozhodně i možnosti zneužití. Silnou politickou motivaci Evropské komise k přijetí komplexního legislativního rámce upravujícího kybernetickou bezpečnost lze dovodit z revize směrnice NIS2 [2], aktuálně projednávaných nových návrhů (např. návrh Aktu o kybernetické odolnosti nebo Aktu o kybernetické solidaritě) a taktéž výjimečně rychlého vyjednávání DORA. Společným cílem těchto iniciativ je posílení odolnosti a reakceschopnosti v kontextu rychlého technologického vývoje a souvisejících nových hrozeb. V poslední době tak došlo k několika významným změnám v evropských legislativních předpisech v oblasti kybernetické bezpečnosti.

Finančním sektorem rezonuje především téma DORA

Evropská komise publikovala návrh tohoto nařízení v září 2020 v rámci balíčku k digitálním financím obsahujícím i Digitální finanční strategii. Po navazující veřejné konzultaci započaly v lednu 2022 trialogy. Ve srovnání s tradičním evropským legislativním procesem, který se často táhne, tyto netrvaly ani půl roku a závěrem minulého roku tak došlo k publikaci nařízení DORA v Úředním věstníku EU. Finální verze však ještě bude v následujícím období doplněna početnými level 2 předpisy, a to především regulačními technickými standardy (RTS) a implementačními technickými standardy (ITS). Otázkou tedy zůstává, jestli DORA není, alespoň prozatím, tak trochu Pandorou.

DORA, kterou doplňuje změnová směrnice [3], nabyla platnosti 16. 1. 2023, její účinnost započne 17. 1. 2025. Vzhledem k povaze právního podpisu, a tedy nařízení, je DORA závazná v celém rozsahu a přímo použitelná

ve všech členských státech. DORA je dle článku 2 aplikována na všechny finanční sektory, včetně bank, pojišťoven, zprostředkovatelů, úvěrových institucí, institucí elektronických peněz, investičních podniků, centrálních depozitářů cenných papírů apod.

Forma nařízení byla zvolena proto, že je jejím cílem odstranění národní dohledové i regulační fragmentace a co nejvyšší míra unifikace digitální odolnosti finančního sektoru v EU, což by mělo posílit i jeho globální konkurenceschopnost. Evropský zákonodárce si od toho slibuje posílení právní jistoty a spolupráce, odstranění přeshraničních překážek, což povede k rovné hospodářské soutěži, posílení důvěry a jistoty na finančních trzích a obzvláště posílení digitální odolnosti, prevence a stability evropského finančního systému vůči kybernetickým zranitelnostem a rizikům. Finanční sektor nejenže se digitalizoval jako celek, ale v důsledku digitalizace se rovněž prohloubila jeho vzájemná propojení a závislosti mezi ním a poskytovateli infrastruktury a služeb z řad třetích stran, čímž jsou myšleni poskytovatelé ICT. Proto DORA zavádí a harmonizuje požadavky na digitální operativní odolnost, a to tak, že dotčené společnosti jsou povinny zajistit schopnost odolat, reagovat a zotavit se ze všech typů narušení a hrozeb spojených s ICT.

Jednou z priorit během vyjednávání znění návrhu byla proporcionalita. Ta se naštěstí v textu DORA průběžně objevuje, např. právě u působnosti a výjimek pro mikropodniky, jelikož DORA rozumně bere v potaz nejenom velikost, povahu, charakter služeb dané finanční instituce, ale zejména její celkový rizikový profil. Vychází z racionálního předpokladu, že větší finanční subjekty mají k dispozici více prostředků a kapacit na rozvoj řídicích struktur, podnikových strategií apod.

DORA je tedy výrazně principiálně založená na *future proof a innovation friendly*, a to proto, aby obstála při turbulentním vývoji i z dlouhodobého hlediska. To text skutečně reflektuje v jednotlivých ustanoveních, která nejsou nadbytečně preskriptivní co do způsobu řešení, ale spíše vymezují cíle, které je finanční instituce povinna naplnit. Tato orientace na výsledek souvisí také s rizikovou a principiální založeností.

DORA se inspirovala mezinárodními normami pro kybernetickou bezpečnost z řady ISO/IEC 27000, což by mohlo zjednodušit implementaci požadavků. Jednotné požadavky na finanční subjekty se vztahují na řízení rizika v oblasti ICT, ohlašování, testování, sdílení operativních a jiných informací. Kromě toho je zásadní, že se evropský zákonodárce snažil zastat svého slova a konsolidoval, nebo se

1) Nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014. Dostupné z: https://eur-lex.europa.eu/legal-content/EN-CS/TXT/?from=EN&uri=CELEX%3A32022R2554.
2) Směrnice Evropského Parlamentu a Rady (EU) 2022/2555 ze 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2). Dostupné z: https://eur-lex.europa.eu/eli/dir/2022/2555.
3) Směrnice Evropského parlamentu a Rady (EU) 2022/2556 ze dne 14. prosince 2022, kterou se mění směrnice 2009/65/ES, 2009/138/ES, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 a (EU) 2016/2341, pokud jde o digitální provozní odolnost finančního sektoru. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32022L2556.

o to alespoň výrazně pokusil, také v praxi časté problematické asymetrické smluvní vztahy s poskytovateli ICT v postavení třetích stran (ICT TPPs). Neopomněl ani pravidla pro dohled nad ICT TPPs a obecná pravidla pro spolupráci dohledových orgánů.

Kapitola II se věnuje řízení rizik

Finanční subjekty mají mít zavedený interní řídicí a kontrolní rámec a jsou povinné stanovit odborný a nezávislý vedoucí orgán, který je plně odpovědný za dohled a jejich provádění. V rámci myšlenky kybernetické hygieny na všech úrovních obsahuje DORA požadavky na identifikaci, ochranu a prevenci, detekci, reakceschopnost, vzdělávání i komunikaci interně i navenek. Cílem je, aby měl finanční subjekt spolehlivý, ucelený a dobře zdokumentovaný rámec pro řízení rizik, který vytváří předpoklady pro rychlé, účinné a komplexní řešení. Ovšem i když může finanční subjekt zadat ověřování kompatibility interně anebo externímu subjektu, nese sám nadále odpovědnost. A ačkoli poskytování služeb ICT v rámci skupiny s sebou nese specifická rizika a přínosy, nemělo by být automaticky považováno za méně rizikové než poskytování služeb ICT poskytovateli mimo finanční skupinu. I proto by mělo podléhat stejnému regulačnímu rámci.

Principiální a proporcionální charakter formulací v DORA je znát i v požadavcích na aktualizované systémy, protokoly a nástroje ICT, které mají být přiměřené rozsahu operací, spolehlivé, vybavené dostatečnou kapacitou ke správnému zpracování dat potřebných k výkonu činností a včasnému poskytování služeb a k realizaci vysokých objemů objednávek, zpráv nebo transakcí, a to i v případě zavádění nové technologie, a technologicky odolné.

Jako součást rámce pro řízení rizik finanční subjekty identifikují, klasifikují a náležitě zdokumentují veškeré obchodní funkce, úlohy a povinnosti podporované ICT, informační aktiva a aktiva v oblasti ICT podporující tyto funkce a jejich úkoly a závislosti ve vztahu k rizikům v oblasti ICT. Finanční subjekty podle potřeby a alespoň jednou ročně přezkoumají přiměřenost této klasifikace a dokumentace.

Dále DORA vymezuje požadavky na nepřetržité sledování a kontrolu bezpečnosti a fungování systémů a nástrojů ICT a minimalizaci dopadu rizik.

Kromě toho jsou finanční subjekty povinny mít zavedeny mechanismy včasné detekce neobvyklých aktivit, včetně problémů s fungováním sítě ICT a incidentů souvisejících s ICT, a mechanismy identifikace potenciálních významných kritických míst. Všechny detekční mechanismy se pravidelně testují. Primárním cílem je zde prevence těchto nežádoucích aktivit do budoucna.

Finanční subjekty mají zavést ucelenou politiku zachování provozu ICT, kterou uplatňují prostřednictvím specializovaných postupů a mechanismů zaměřených na zajištění kontinuity zásadních nebo důležitých funkcí. Ve výsledku by měla být zajištěna rychlá, vhodná, účinná reakce na všechny incidenty, omezení škod a obnova činnosti. K tomu je potřeba neprodleně aktivovat specializované plány a dále odhad předběžných dopadů, škod a ztrát, popř. realizovat i krizovou komunikaci. Ta je založena na připravené krizové komunikační strategii, přičemž pro tyto účely je pověřena alespoň jedna osoba.

Na to navazuje nutnost politiky zálohování a postupy a metody obnovy, přičemž při obnově zálohových dat pomocí vlastních systémů finanční subjekty použijí systémy ICT, pochopitelně fyzicky a logicky odděleny od zdrojového systému. Při obnově provozu jednotlivých funkcí finanční subjekty zohlední, zda se jedná o zásadní nebo důležitou funkci a potenciální celkový dopad na tržní efektivitu.

Poté finanční subjekty shromažďují informace o zranitelnostech a kybernetických hrozbách a o incidentech souvisejících s ICT, zejména kybernetických útocích, a analyzují jejich pravděpodobný dopad. O tyto informace může požádat i dohledový orgán.

Kromě toho klade DORA důraz i na školení zaměstnanců a povědomí o bezpečnosti v oblasti ICT a průběžné sledování relevantního technologického vývoje.

Kapitola III upravuje povinnosti finančních subjektů

Kapitola III upravuje povinnosti finančních subjektů v oblastech řízení, klasifikace a hlášení incidentů, tedy zavádění a uplatňování konzistentní a integrované detekce, řízení a hlášení prostřednictvím ukazatelů včasného varování, postupy k identifikaci, sledování, evidenci, kategorizaci a klasifikaci ICT incidentů, postupy ke zmírnění dopadů apod. Klasifikace incidentů probíhá na základě několika kritérií vymezených v článku 18. Jedná se o počet dotčených klientů nebo transakcí, dobu trvání, územní rozsah, ztrátu údajů, význam zasažených služeb a ekonomický dopad.

K incidentům, které jsou klasifikované jako závažné, se vztahují další úkoly – povinné ohlašování dohledu (ČNB) a předložení relevantní dokumentace. Také je však možné dobrovolné ohlašování dohledu/CSIRT, pokud se finanční subjekty domnívají, že hrozba je relevantní pro finanční systém, uživatele služeb nebo klienty. Interakce, poskytnutí zpětné vazby dohledového orgánu, je vymezena jako možnost, stejně jako poskytnutí informací veřejným nefinančním orgánům, např. právě ÚOOÚ.

I u ohlašování DORA umožňuje outsourcing třetí strany, ale nadále platí plná a konečná odpovědnost finančního subjektu. Bližší informace a očekávanou standardizaci mají upravit level 2 předpisy.

Kapitola IV se zaměřuje na testování

Kapitola IV se věnuje testování digitální provozní odolnosti zásadních a důležitých funkcí. Pro účely posuzování připravenosti na řešení incidentů, identifikace slabých míst, vad a nedostatků a rychlého zavedení nápravných opatření finanční subjekty (jiné než mikropodniky) při zohlednění kritérií proporcionality vytvoří, udržují a aktualizují spolehlivý a ucelený program testování digitální provozní odolnosti jakožto nedílnou součást rámce pro řízení rizika. Tento program lze realizovat formou různých hodnocení, testů, nástrojů a politik, jako např. hodnocením a zjišťováním zranitelnosti, analýzou otevřených zdrojů, posouzením bezpečnosti sítě, analýzou nedostatků, přezkumy fyzické bezpečnosti, dotazníky a antivirovými softwarovými řešeními, v případě proveditelnosti přezkumy zdrojových kódů atd. Testování mohou realizovat externí či interní nezávislé subjekty, u kterých je nutná prevence střetu zájmů. Frekvence je minimálně jednou do roka.

Specificky je v DORA věnován prostor penetračnímu testování

Požadavky na subjekty provádějící penetrační testování vcelku extenzivně definuje článek 26 a následují. Určené finanční subjekty provádějí alespoň jednou za tři roky pokročilé testování s využitím penetračního testování na základě faktorů souvisejících s dopady, případných hledisek finanční stability, včetně systémové povahy finančního subjektu a kon-

krétního rizikového profilu v oblasti ICT, úrovně vyspělosti finančního subjektu v oblasti ICT nebo dotčených technologických prvků. Na základě rizikového profilu finančního subjektu a s přihlédnutím k provozním okolnostem může příslušný orgán v případě potřeby požádat finanční subjekt, aby tuto četnost snížil nebo zvýšil. Finanční subjekty posoudí, které zásadní nebo důležité funkce je třeba zahrnout do penetračního testování na základě hrozeb. Výsledek posouzení určí přesný rozsah penetračního testování na základě hrozeb a musí být potvrzen příslušnými orgány.

Pokud jsou do rozsahu penetračního testování na základě hrozeb zahrnuti ICT TPPs, přijme finanční subjekt nezbytná opatření a záruky k zajištění účasti těchto ICT TPPs na penetračním testování na základě hrozeb a po celou dobu si ponechá plnou odpovědnost. Finanční subjekty mají dále povinnost zajistit, aby ve smlouvách uzavřených s externími subjekty provádějícími testování byla požadována řádná správa výsledků penetračního testování na základě hrozeb a aby jakékoli související zpracování údajů, včetně jakéhokoli vypracování, uložení, agregace, návrhu, hlášení, sdělení nebo zničení, neohrozilo finanční subjekt.

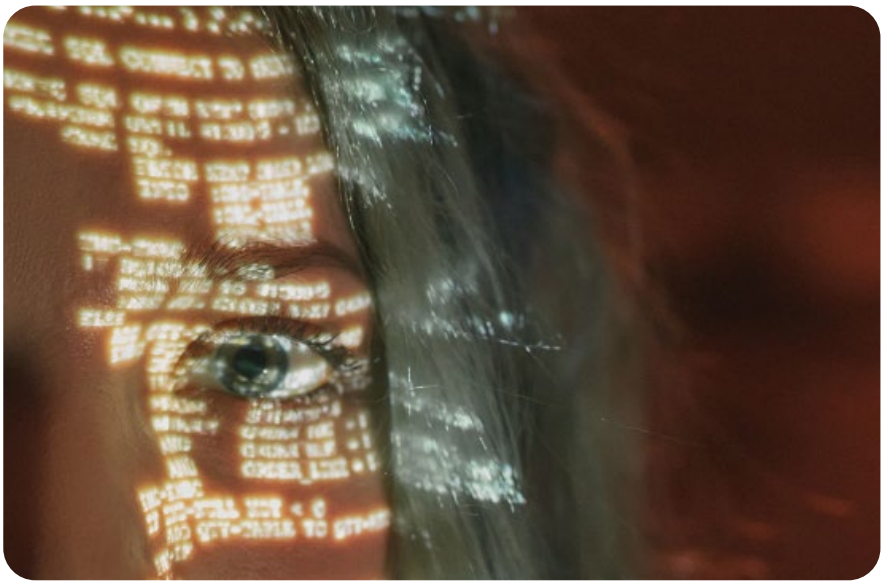
Na konci testování a po schválení zpráv a plánů nápravných opatření finanční subjekt, resp. externí subjekt, předloží orgánu souhrn příslušných zjištění, plánů, nápravných opatření a dokumentaci. Orgán vydá osvědčení o provedeném testu v souladu s požadavky. I pro tuto oblast DORA zdůrazňuje, že odpovědnost vždy nese finanční subjekt.

Kromě toho DORA pro *futuro* počítá s alternativou, že na základě odborných znalostí, které již některé příslušné orgány získaly, zejména pokud jde o provádění rámce TIBER–EU, by toto nařízení mělo členským státům umožnit, aby na vnitrostátní úrovni určily jediný veřejný orgán jako odpovědný za všechny záležitosti penetračního testování.

Kapitola V upravuje outsourcing

Kapitola V upravuje outsourcing, což je snaha právě o úpravu asymetrických smluvních vztahů s ICT TPPs, vč. sledování subdodavatelských řetězců. Kapitola bude dále doplněna level 2 požadavky, prozatím jsou formulace v nařízení spíš obecné. Je opětovně zdůrazňována plná odpovědnost finančního subjektu a také proporcionalita ve vztahu k povaze, rozsahu, složitosti a významu závislostí v oblasti ICT a rizik vyplývajících ze smluvních ujednání se zohledněním toho, jak zásadní či důležité jsou příslušné služby, procesy nebo funkce a jaký je potenciální dopad na kontinuitu a dostupnost finančních služeb a činností na individuální úrovni i na úrovni skupiny.

Kromě toho je zde vymezena povinnost finančního subjektu, který jako součást svého rámce pro řízení rizika vede a aktualizuje registr informací s ohledem na všechna smluvní ujednání. Smluvní ujednání se řádně zdokumentují, přičemž se rozlišuje mezi těmi, která se týkají služeb ICT podporujících zásadní nebo důležité funkce, a těmi, která se jich netýkají. Finanční subjekty alespoň jednou ročně nahlásí příslušným orgánům počet a charakter nových ujednání.



Relativně detailně jsou však definovány požadavky na finanční subjekty před uzavřením smluvního ujednání o využívání služeb ICT, avšak nadále budou doplňovány level 2 předpisy. Je nezbytné posoudit několik faktorů – zda se smluvní ujednání týká využívání služeb ICT podporujících zásadní nebo důležité funkce; zda jsou splněny podmínky dohledu pro uzavření smlouvy; identifikace a posouzení relevantních rizik, včetně možnosti, kdy smluvní ujednání může přispívat k zesílení rizika koncentrace dále definovaného článkem 29; přezkum vhodnosti ICT TPPs a identifikace případných střetů zájmů, které mohou smluvní ujednání způsobit.

DORA a požadavky na formu smlouvy

DORA zakotvuje i požadavky na formu smlouvy, která musí být písemná, ať už v listinné podobě, nebo v jiném formátu, který lze stáhnout, je trvalý a přístupný. Obsah má být srozumitelný a má zahrnovat např. úplný popis všech funkcí a služeb; ustanovení týkající se dostupnosti, hodnověrnosti, integrity a důvěrnosti; požadavky na penetrační testování; povinnost a práva ICT TPPs; právo nepřetržitě sledovat výsledky ze strany finančního subjektu; výpovědní lhůty a povinnosti hlášení; exitovou strategii atd.

Důkladné a praktické nastavení exitové strategie

Další z priorit v předchozí fázi vyjednávání bylo právě důkladné a praktické nastavení exitové strategie. To je v DORA obsaženo pro případy, pokud ICT TPPs zásadním způsobem poruší platné právní předpisy nebo smluvní podmínky; pokud by se sledováním rizika zjistily okolnosti, u nichž se má za to, že mohou změnit plnění funkcí poskytovaných prostřednictvím smluvního ujednání; pokud by byla v rámci celkového řízení rizika v oblasti ICT TPPs zjištěna slabá místa, a to zejména s ohledem na zajištění dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů, ať již osobních, či jiných citlivých údajů, nebo jiných než osobních údajů, nebo pokud by příslušný orgán již nedokázal dále efektivně dohlížet na finanční subjekt v důsledku podmínek příslušného smluvního ujednání nebo okolností s ním souvisejících. Pak by bylo možné smluvní vztah bez dopadu na kontinuity poskytovaných služeb a dodržování regulatorních požadavků ukončit. Finanční subjekt má mít připravenou strategii ukončení smluvního vztahu, která zohlední rizika jako např. případné selhání, snížení kvality poskytovaných služeb a funkcí, jakékoli narušení činnosti v důsledku nevhodného či chybného poskytování služeb nebo jakéhokoli vážného rizika nebo v případě ukončení smluvních ujednání za kterékoli z okolností výše. Dále má mít finanční subjekt identifikována alternativní řešení a vypracovány plány přechodu, které mu umožní odebrání nasmlouvaných služeb a příslušných dat od ICT TPPs a jejich bezpečný a integrovaný přenos k alternativnímu poskytovateli nebo jejich začlenění v rámci vlastní organizace.

DORA specificky přistupuje k oblasti dohledu

V podstatě jej lze rozdělit do dvou separátních kategorií – dohled nad finančními institucemi a nově také dohled nad kritickými ICT TPPs.

Dohledové pravomoci nad finančními institucemi náleží ČNB, nicméně hlášení a řešení incidentů spadá pod NÚKIB. Příslušné orgány mají všechny kontrolní, vyšetřovací (např. kontroly na místě, přístup k dokumentaci apod.) a sankční pravomoci nezbytné k plnění svých povinností. Rozhodnutí o uložení správních sankcí nebo nápravných opatření musí být řádně odůvodněna, aby bylo možné podat proti nim opravný prostředek. Rozhodnutí jsou publikovaná na webu. Členské státy se mohou rozhodnout, že nestanoví správní sankce nebo nápravná opatření za ta porušení, na která se podle jejich vnitrostátního práva vztahují trestní sankce. Tak či

tak však sankce musí být účinné, přiměřené a odrazující a musí zohledňovat, do jaké míry bylo porušení způsobeno úmyslně nebo z nedbalosti, a všechny ostatní relevantní okolnosti.

Nová struktura dohledu nad kritickými ICT TPPs má odlišné rysy

Evropské orgány dohledu (ESAs) prostřednictvím společného výboru a na základě doporučení fóra dohledu (ESAs, zástupce dozorového orgánu z každého státu, ECB, ESRB, Komise, ENISA, případně zástupci NIS úřadů) a kritérií určí ICT TPPs, kteří jsou kritičtí pro finanční subjekty, a jmenují hlavním orgánem dohledu pro jednotlivé kritické ICT TPPs 1 z ESAs na základě největšího podílu aktiv z hodnoty celkových aktiv. Relevantními kritérii jsou např. systémový dopad na stabilitu, kontinuitu nebo kvalitu poskytování finančních služeb; systémová povaha či význam finančních subjektů; počet globálních systémově významných institucí (G-SVI) nebo jiných systémově významných institucí (J-SVI), které spoléhají na daného ICT TPPs; míra nahraditelnosti ICT TPPs s přihlédnutím k těmto parametrům atd. Po finalizaci administrativního procesu ICT TPPs, poté, co byl určen jako kritický, informuje daný ICT TPPs finanční subjekty, kterým poskytuje služby. DORA zvážila také specifika ICT TPPs ze třetích zemí. Ty mají povinnost mít dceru v EU do jednoho roku od určení kritičnosti. Zároveň je významnou odchylkou to, že kritičtí poskytovatelé platí za dohled poplatky.

Dále DORA prozatím na dobrovolné bázi upravuje možnost finančních subjektů vzájemně si vyměňovat operativní informace o kybernetických hrozbách a kolektivně využívat individuálních znalostí a praktických zkušeností na strategické, taktické a provozní úrovni, a zlepšuje tak schopnost adekvátního posuzování a sledování kybernetických hrozeb, obrany před nimi a reakce na ně.

Na základě výše uvedeného by implementace DORA v rámci finančního sektoru mohla probíhat následovně:

I. Analýza současného stavu: provést komplexní analýzu svých současných IT systémů a procesů, aby se zjistilo, jak jsou odolné vůči kybernetickým hrozbám. Tato analýza by měla zahrnovat také posouzení rizik spojených s kybernetickou bezpečností.
II. Vývoj strategie pro digitální odolnost: na základě analýzy vytvořit strategii pro zlepšení své digitální odolnosti. Tato strategie by měla zahrnovat plán pro zlepšení IT infrastruktury a procesů, aby byly odolnější vůči kybernetickým útokům.
III. Implementace změn: provést potřebné změny v jejich IT systémech a procesech podle strategie. To může zahrnovat například výměnu zastaralých systémů, zlepšení bezpečnostních opatření nebo vývoj nových nástrojů pro detekci a řešení kybernetických hrozeb.
IV. Ověřování a monitorování: po implementaci změn provést ověřování, aby se finanční sektory ujistily, že jejich systémy a procesy jsou nyní odolnější vůči kybernetickým útokům. Také by měly zřídit systémy pro průběžné monitorování a reportování kybernetických hrozeb.
V. Školení zaměstnanců: investovat do školení zaměstnanců v oblasti kybernetické bezpečnosti. Toto školení by mělo zaměstnancům poskytnout potřebné znalosti a dovednosti pro identifikaci a řešení kybernetických hrozeb.
VI. Pravidelné revize: pravidelně revidovat a aktualizovat svou strategii pro digitální odolnost, aby se finanční sektory ujistily, že zůstávají na vrcholu vývoje v oblasti kybernetické bezpečnosti.

DORA není izolovaným předpisem

Jak jsem naznačila hned v úvodu, DORA není izolovaným předpisem. Během implementace je proto nutné myslet na případné návaznosti, zejména na nově revidovanou směrnici NIS2, která zavádí nová, obecná (nikoli sektorově specifická) pravidla pro posílení kybernetické bezpečnosti po celé EU. Zároveň posiluje kybernetické požadavky pro středně velké a velké subjekty, které provozují a poskytují služby v klíčových sektorech. Na některé subjekty, např. banky, tak již dopadají povinnosti z NIS2 i DORA.

Směrnice NIS2 pokrývá více sektorů a činností než dříve, sjednocuje hlášení o povinnostech a řeší bezpečnost dodavatelských řetězců. Směrnice zakotvuje zřízení evropské sítě styčných organizací pro kybernetické krize, tzv. EU-CyCLONe k podpoře koordinovaného řízení rozsáhlých kybernetických bezpečnostních incidentů. Implementace NIS2 se překlopí do novelizovaného zákona č. 181/2014 Sb., o kybernetické bezpečnosti, s účinností od 18. 10. 2024 (v souladu s transpoziční lhůtou NIS 2). Aktuálně probíhá mezirezortní připomínkové řízení.

Vztah DORA k NIS2 je určen jakožto lex *specialis*. To znamená, že pro finanční sektor se primárně aplikuje DORA. Detailní informace o NIS2 lze najít na dedikovaném webu NÚKIB [4].

Co se týká dalších kroků, momentálně je klíčový obsah a časový rámec vydání level 2 předpisů, které jsou relevantní pro řádnou interpretaci a implementaci. Tyto předpisy budou z pera ESAs, resp. i ECB a ENISA. Konkrétně DORA avizuje 8 RTS, 2 ITS, 2 obecné pokyny a prováděcí nařízení Komise ke klasifikaci incidentů a harmonizaci obsahu a vzorů hlášení. Kromě toho mají být vypracované technické rady Komise ke kritériím, podle kterých jsou ICT TPPs určeni jako kritičtí pro subjekty na finančním trhu a ke zmíněným poplatkům za dohled ESAs. Vydání level 2 budou předcházet veřejné konzultace ve dvou kolech, momentálně probíhá první z nich.

Nadále tedy zůstávají nejasné některé podstatné oblasti. Délka prací a následný termín publikace level 2 ukážou, zda bude vytvořen dostatečný časový prostor pro implementaci doplňujících, ale určujících požadavků. Také se projeví, zda se povedlo zabránit duplicitním či kontradiktorním požadavkům DORA ve vztahu k ostatním legislativním předpisům či např. pokynům ESAs. Otázkou také zůstává, jak bude de facto probíhat ohlašování kompetentním orgánům a zda se (i v delším časovém měřítku) povede tento proces zefektivnit. Dnes by např. některé finanční instituce v případě jednoho kybernetického incidentu s dopadem na osobní údaje musely ohlašovat NÚKIB dle NIS2, ČNB dle DORA a ÚOOÚ dle GDPR.

Evropský zákonodárce si od unifikační DORA slibuje nejenom dosažení v úvodu popsaných cílů a technologickou bezpečnost, ale taktéž tzv. bruselský efekt po vzoru GDPR. To znamená, že by principiálně a rizikově formulovaná DORA mohla být i v globálním kontextu pojata jako minimální standard v oblasti kybernetické bezpečnosti, který bude inspirací i pro jurisdikce ze třetích zemí. To by pochopitelně zlepšilo i spolupráci se subjekty z EU.

Pokračování příště…

Příště se budeme věnovat specifickému vztahu DORA a GDPR, který chápu tak, že koncept kybernetické bezpečnosti je nadstavbou GDPR a zároveň důvodem, proč je kybernetická bezpečnost relevantní i pro malé a střední podniky nejenom v rámci finančního sektoru.

Jana Lix Andraščiková
Autorka je právník, koordinátor evropské agendy a gestor kybernetické bezpečnosti v České asociaci pojišťoven.

4) Dostupné z: https://osveta.nukib.cz/course/view.php?id=145.

Anonymizace v praxi povinných subjektů

Anonymizace je nedílnou součástí práce povinných subjektů při poskytování informací. Není samoúčelná. Má zabránit neodůvodněným zásahům do soukromí dotčených osob a zajistit ochranu dalším údajům, které si ji po právu zaslouží.

Má-li být provedena důsledně, může jít o poměrně náročný proces. Připomeneme si proto základní principy anonymizace, její smysl a účel. Pokusíme se ozřejmit, které údaje anonymizujeme, jak právo chrání soukromí žadatelů o informace a co musí strpět žadatelé profesionálové.

Anonymizace před poskytnutím informací

Poprvé a nejčastěji provádí povinné subjekty anonymizaci v souvislosti s poskytováním informací. V této souvislosti anonymizací rozumíme **vyhledávání informací (osobních a dalších údajů), které nelze poskytnout**.[1] Primárním smyslem anonymizace je ochrana soukromí[2] a dalších údajů, jejichž poskytnutí by mohlo představovat neodůvodněný zásah do práv a oprávněných zájmů dotčených osob.

Proces anonymizace v tradičním pojetí správní a soudní praxe znamená de-identifikaci, tj. **znemožnění ztotožnění subjektu údajů, kterého se poskytované informace týkají**. Při posuzování, zda je subjekt údajů identifikovatelný, povinný subjekt přihlíží ke všem prostředkům, jejichž použitelnost správcem i jinými osobami (v prvé řadě žadatelem) za účelem identifikace subjektu údajů může rozumně předpokládat.[3] Měl by tedy mj. zvážit existující možnosti žadatele s pomocí dalších, např. na internetu dostupných informací subjekt údajů identifikovat.

Smyslem anonymizace je zabránit identifikaci subjektu údajů nevratně. Pokud mají být údaje anonymizovány, neměly by poskytnuté informace obsahovat žádný údaj, který by při vynaložení přiměřeného úsilí žadatele mohl posloužit k opětovné identifikaci subjektu údajů (dotčených osob). Z pohledu povinných subjektů, coby správců osobních údajů, představuje provádění anonymizace v souvislosti s poskytováním informací a jejich následným zveřejněním (podrobněji dále v textu) **spíše pseudonymizaci**,[4] protože de-anonymizace není provedena nevratně (anonymizované osobní údaje správce trvale nevymazává, pouze je znepřístupní žadatelům o informace). Povinné subjekty dál (ve svých spisech, evidencích, informačních systémech) anonymizované údaje zpracovávají. Není tedy vyloučeno je kdykoliv v budoucnu přiřadit konkrétní osobě.

V případě, kdy povinný subjekt k anonymizaci využívá zvláštní software (elektronický nástroj), tzv. „anonymizér", tento sám o sobě plní bezezbytku funkci anonymizace, protože osobní údaje v konkrétním dokumentu (rozsudku, rozhodnutí apod.) odstraňuje nevratně. Povinný subjekt v pozici správce osobních údajů odstraněné údaje ale dále zpracovává v jiných databázích, uložištích či na analogových nosičích a má možnost, např. prostřednictvím čísla jednacího, sp. zn., z těchto zdrojů osobní údaje obnovit. V této spojitosti je na místě připomenout, že **osobními údaji jsou jak věcné informace vypovídající o určité osobě**, které jsou ve své podstatě samy o sobě způsobilé zasáhnout do jejího soukromí, a proto o nich má jednotlivec právo rozhodnout si, komu je zpřístupní (například informace, kde daná osoba pracuje, zda je vdaná, má děti, kde bydlí).[5] Vedle toho jsou osobními údaji i **informace spočívající pouze v tom, že jejich obsahem je prakticky pouze jejich vztah k určité osobě** (typicky telefonní číslo, číslo IP adresy, e-mailová adresa). Striktně vzato tyto údaje ale samy o sobě nejsou nositeli informací o soukromí dotčené osoby. Přesto i šíření těchto údajů podléhá dohledu subjektu údajů, aby nedocházelo k jejich zneužití, například nevyžádanému kontaktování, zasílání nevyžádaných zpráv.

Anonymizace typově prvé skupiny osobních údajů přináší ochranu soukromí dané osoby. Anonymizace údajů typu telefonního čísla sleduje spíše jen zamezení identifikace subjektu údajů (zde zabránění možnosti jej kontaktovat).[6]

1) Týká se v zásadě všech informací, které nelze podle § 7, § 8a, § 9, § 10 a § 11 zákona o svobodném přístupu k informacím poskytnout (zejména informace týkající se osobnosti, projevů osobní povahy, soukromí fyzické osoby a osobní údaje, pokud by jejich poskytnutí bylo v rozporu s právními předpisy upravujícími jejich ochranu). Srov. rozsudek Nejvyššího správního soudu ze dne 31. 7. 2014, čj. 5 As 76/2014-23. Rozsudek Nejvyššího správního soudu ze dne 27. 2. 2014, čj. 7 As 20/2013 - 23.
2) Srov. rozsudek Nejvyššího správního soudu ze dne 10. 5. 2006, č. j. 3 As 21/2005 - 105, publ. pod č. 927/2006 Sb. NSS
3) Srov. rozsudek ze dne 19. října 2016 ve věci C-582/14, Breyer proti Spolkové republice Německo. Podle Soudního dvora kritérium identifikovatelnosti není splněno, pokud identifikaci subjektu údajů zákon zakazuje nebo je prakticky vyloučena, protože vyžaduje nepřiměřené úsilí z hlediska času, nákladů, lidské síly, takže se riziko ztotožnění subjektu údajů zdá být zanedbatelné.
4) Srov. článek 4 odst. 5 nařízení Evropského parlamentu a Rady (EU) 2016/679, 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).
5) K právu na informační sebeurčení srov. zejména nález Ústavního soudu ze dne 11. 11. 2005, sp. zn. I. ÚS 453/03, či nález ze dne 20. 11. 2002, sp. zn. I. ÚS 512/02.
6) Srov. rozsudek Nejvyššího správního soudu ze dne 12. 2. 2009, čj. 9 As 34/2008-68: *„Plná identita fyzické osoby v současných podmínkách technologicky vyspělé společnosti, tj. za vysokého stupně rozvoje elektronických a jiných médií, která jsou většině populace snadno dostupná, ve své podstatě neznamená nic jiného, než možnost tuto osobu určitým způsobem kontaktovat, aniž by bylo nutno znát místo jejího aktuálního pobytu. Proto se výklad pojmu ‚osobní údaj' nemůže omezit striktně jen na znalost např. rodného čísla, adresy či pracoviště subjektu údajů. Z tohoto pohledu je za osobní údaj třeba považovat i číslo mobilního telefonu určité osoby, jakkoli může být takové číslo používáno příslušnou osobou jen dočasně, a zároveň nijak nespecifikuje jeho fyzickou, psychickou, ekonomickou, kulturní nebo sociální identitu. Prostřednictvím tohoto čísla je však možno daný subjekt v určitém časovém úseku přímo kontaktovat (což se ostatně stalo i v posuzovaném případě), a tento subjekt je tak dosažitelný a jistým způsobem určitelný, a to případně i bez znalosti jeho jména a dalších údajů, které již vazbu na jeho fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu mají."*

Rozlišování mezi jednotlivými typy osobních údajů má svůj praktický význam právě při provádění anonymizace, protože **některé informace jsou osobními údaji, jen pokud samy identifikují určitou osobu**. Takovými údaji jsou přímé identifikátory typu jméno a příjmení, telefonní číslo, rodné číslo. **Jiné informace jsou osobními údaji, jen pokud jsou na základě dodatečných informací spojené (přiřaditelné) k určité (konkrétní) osobě**. Pro ně platí, že mohou přestat být osobními údaji, aniž by byl změněn jejich obsah nebo forma, pokud se povinnému subjektu podaří odstranit možnost jejich přiřazení ke konkrétní osobě (vyloučit možnost identifikace osoby, které se týkají). K zajištění odpovídající ochrany osobních údajů by tedy zpravidla mělo postačit, anonymizuje-li povinný subjekt přímé identifikátory, čímž znemožní identifikaci subjektu údajů, kterého se týkají dále v textu (dokumentu, rozhodnutí) poskytované údaje. Bohužel ne vždy bude tato „základní" anonymizace v konkrétním případě dostatečná, neboť subjekt údajů bude identifikovatelný buď z věcných informací obsažených v textu, nebo ve spojení s dalšími informacemi, které si může s vynaložením přiměřeného úsilí opatřit např. na internetu.

Obdobně zcela specifickou a v praxi obvyklou situací je, když se žadatel přímo v žádosti ptá na konkrétní osobu (*typicky žádám o kopii rozhodnutí o přestupku pana Josefa Nováka, narozeného... bytem...* apod.). Pokud je tedy subjekt údajů předem určený, „vymazání" ryze identifikačních údajů, které nadto žadatel zpravidla sám zná a uvádí, nepředstavuje dostatečný prostředek ochrany jeho soukromí. Řešením těchto situací je zpravidla odmítnutí poskytnutí požadované informace jako celku, neboť jakoukoliv informaci, kterou by se o panu Novákovi měl žadatel od povinného subjektu dozvědět, počínaje informací, zda úřad řešil přestupek jmenovaného a jak o něm rozhodl, lze považovat za osobní údaj.

Zásada minimalizace údajů [7] vyžaduje zpracování osobních údajů pouze v rozsahu nezbytném pro naplnění legitimního účelu. [8]

I anonymizaci je třeba provést pouze v rozsahu nezbytném. V právní rovině to znamená poměřování – posuzování přiměřenosti omezení práva na ochranu osobních údajů v konkurenci s právem na informace, veřejným zájmem na transparentnosti a otevřenosti výkonu veřejné moci; provedení testu proporcionality. [9]

Znečitelnění v autentickém textu je dostatečnou ochranou osobních údajů

Požadavek na nezbytnost anonymizace v praktické rovině znamená, že povinný subjekt před vlastním poskytnutím informace (např. celého rozhodnutí, dokumentu, zápisu atd.) důkladně projde požadovanou informaci a identifikuje údaje, na základě kterých by mohl žadatel rozpoznat totožnost osoby, k níž se poskytovaná informace váže (např. účastníky řízení, jejich zástupce, svědky), pokud tyto informace žadateli poskytnuty být nemohou. [10] Zjištění přítomnosti těchto údajů v požadovaném dokumentu ale nemůže být důvodem k odepření poskytnutí kopie celého dokumentu, ale toliko jen důvodem k vyloučení právě těch údajů, které povinný subjekt poskytnout nesmí. Pokud dokument obsahuje např. osobní údaje, povinný subjekt kopii takové listiny žadateli poskytne, a to v anonymizované podobě, tedy v podobě, kde budou na listině uvedené osobní údaje znečitelněny (vymazány). [11] Za této situace, není přípustné odmítat celý dokument. [12]

Obdobně povinný subjekt vyhledá informace, jejichž poskytnutím by mohlo být dotčeno jiné právo (např. autorské) či právem chráněný zájem (např. ochrana důvěrnosti majetkových poměrů). Není přípustné odmítat celý dokument. [13]

Když anonymizuji, musím rozhodnout o odmítnutí žádosti?

Z procesního hlediska je důležité nezapomínat, že anonymizace znamená nevyhovění (alespoň částečně) žádosti žadatele. O každém odmítnutí informace musí povinný subjekt vydat rozhodnutí. [14] Předposlední novela zákona o svobodném přístupu k informacím [15] připustila ale významnou výjimkou v případě tzv. minimalistické anonymizace, pokud si o rozhodnutí o odmítnutí žádosti žadatel neřekne. [16]

7) Srov. článek 5 odst. 1 písm. c) Obecného nařízení o ochraně osobních údajů.
8) Prakticky totožný požadavek vyplývá i z ústavního imperativu vyjádřeného v článku 4 odst. 4 Listiny základních práv a svobod. Srov. rozsudek Nejvyššího správního soudu ze dne 10. 10. 2003, č. j. 5 A 119/2001 – 38.
9) Srov. nález Ústavního soudu sp. zn. Pl. ÚS 24/11 ze dne 20. 12. 2011 (N 217/63 SbNU 483; 43/2012 Sb.).
10) V Kanceláři veřejného ochránce práv máme za tímto účelem nastaveno tzv. pravidlo 4 očí, tj. jedna osoba anonymizuje, druhá kontrola.
11) Srov. rozsudek Nejvyššího správního soudu ze dne 28.03.2008, čj. 3 As 13/2007 – 75.
12) Srov. rozsudek Nejvyššího správního soudu ze dne 14.01.2004, čj. 7 A 3/2002.
13) Srov. rozsudek Nejvyššího správního soudu ze dne 14.01.2004, čj. 7 A 3/2002.
14) Srov. § 15 odst. 1 zákona o svobodném přístupu k informacím: Pokud povinný subjekt žádosti, byť i jen zčásti, nevyhoví, vydá ve lhůtě pro vyřízení žádosti rozhodnutí o odmítnutí žádosti, popřípadě o odmítnutí části žádosti (dále jen „rozhodnutí o odmítnutí žádosti"), s výjimkou případů, kdy se žádost odloží.
15) Zákon č. 241/2022 Sb., kterým se mění zákon č.106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, zákon č. 123/1998 Sb., o právu na informace o životním prostředí, ve znění pozdějších předpisů, a zákon č.130/2002 Sb., o podpoře výzkumu, experimentálního vývoje a inovací z veřejných prostředků a o změně některých souvisejících zákonů (zákon o podpoře výzkumu, experimentálního vývoje a inovací), ve znění pozdějších předpisů.
16) Srov. § 15 odst. 3 zákona o svobodném přístupu k informacím: Pokud povinný subjekt poskytuje informaci formou kopie dokumentu, z něhož vyloučil pouze osobní údaje nebo informace, které jsou bankovním nebo obchodním tajemstvím a které získal při postupech podle správního, daňového nebo kontrolního řádu, nemusí vydat rozhodnutí o odmítnutí žádosti. Sdělí-li žadatel v podané žádosti anebo do 15 dnů ode dne doručení požadované informace způsobem stanoveným tímto zákonem pro podání písemné žádosti o informace povinnému subjektu, že trvá na vydání rozhodnutí o odmítnutí žádosti v rozsahu vymezených osobních údajů nebo bankovního anebo obchodního tajemství, povinný subjekt jej vydá ve lhůtě pro vyřízení žádosti anebo do 15 dnů ode dne doručení sdělení žadatele.

V rozhodnutí o odmítnutí žádosti povinný subjekt vždy uvede jaké kategorie osobních údajů znečitelnil, např. že se jednalo o identifikační údaje účastníka, údaje o jeho povolání, rodinných příslušnících atd.[17]

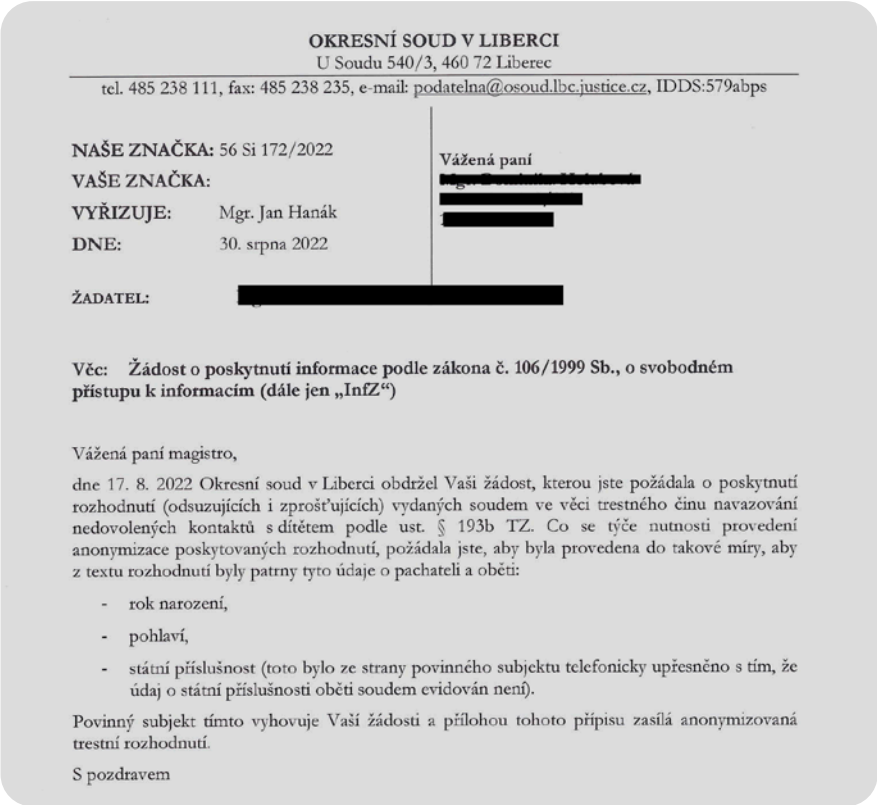
Jak anonymizovat?

Při práci s textem v elektronické podobě můžeme anonymizovaný údaj nahradit rovnou informací, o jaký údaj šlo, např. jméno účastníka „Jan Holý" nahradit informací „jméno účastníka", bydliště „U Branky, č. p. 65, Ostrava" nahradit informací „bydliště účastníka". Existují ale i další způsoby, jak anonymizovat:

- Začernění, nahrazení xxxxxxxx (např. pan xxxxxxx uvedl…)
- Ponechání počátečních písmen, iniciál (např. pan J. H. uvedl…)[18]
- Nahrazení smyšlenými iniciály (např. pan A. B. uvedl…)[19]
- Zobecnění (např. účastník řízení uvedl…)
- Nahrazení smýšlenými jmény (např. pan Kříž uvedl…)

Je vždy vhodné vybrat jeden ze způsobů anonymizace a tento důsledně uplatňovat pro celý anonymizovaný text.

Pokud se požadované informace nachází pouze v listinné podobě, lze dokument obsahující chráněné údaje vytisknout, informace, které nelze poskytnout, začernit černou fixou nebo je zabělit, a teprve takto upravenou listinu (dokument) nakopírovat. Při poskytování elektronicky lze zaslat jako PDFko.



OKRESNÍ SOUD V LIBERCI
U Soudu 540/3, 460 72 Liberec
tel. 485 238 111, fax: 485 238 235, e-mail: podatelna@osoud.lbc.justice.cz, IDDS:579abps

NAŠE ZNAČKA: 56 Si 172/2022
VAŠE ZNAČKA:
VYŘIZUJE: Mgr. Jan Hanák
DNE: 30. srpna 2022

ŽADATEL: [redacted]

Vážená paní [redacted]

Věc: Žádost o poskytnutí informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím (dále jen „InfZ")

Vážená paní magistro,

dne 17. 8. 2022 Okresní soud v Liberci obdržel Vaši žádost, kterou jste požádala o poskytnutí rozhodnutí (odsuzujících i zprošťujících) vydaných soudem ve věci trestného činu navazování nedovolených kontaktů s dítětem podle ust. § 193b TZ. Co se týče nutnosti provedení anonymizace poskytovaných rozhodnutí, požádala jste, aby byla provedena do takové míry, aby z textu rozhodnutí byly patrny tyto údaje o pachateli a oběti:

- rok narození,
- pohlaví,
- státní příslušnost (toto bylo ze strany povinného subjektu telefonicky upřesněno s tím, že údaj o státní příslušnosti oběti soudem evidován není).

Povinný subjekt tímto vyhovuje Vaší žádosti a přílohou tohoto přípisu zasílá anonymizovaná trestní rozhodnutí.

S pozdravem

I před zveřejněním poskytnutých informací prověřte, zda není potřebná anonymizace

Informace, které povinný subjekt poskytne na žádost, do 15 dnů od poskytnutí informace zveřejní,[20] a to způsobem umožňujícím dálkový přístup (tj. na webových stránkách povinného subjektu).

Lze zveřejnit sdělení povinného subjektu obsahující poskytnuté informace (odpověď na žádost) nebo jen poskytnuté informace. Není vyloučeno ani zveřejnění rozhodnutí o odmítnutí žádosti.[21]

Pozor ale, pokud je žadatelem např. účastník řízení, občan obce[22] nebo osoby, jichž se poskytované údaje týkají, **tzv. privilegovaní žadatelé**. Tito žadatelé mají neomezený přístup k vybraným informacím z titulu svého postavení. Zveřejnění jejich osobních údajů „běžnému žadateli" by ale mohlo představovat nepřiměřený zásah do soukromí dotčených osob či ohrozit jiné chráněné zájmy. Je tedy na místě přistoupit k anonymizaci a poskytnuté informace zveřejnit pouze v rozsahu, v jakém k nim má přístup „běžný žadatel".[23]

Údaje žadatelů o informace se nezveřejňují. Výjimku představují profesní údaje

Zákonná povinnost zveřejnit poskytnuté informace nezahrnuje zveřejnění informací o žadateli (zpravidla jméno, příjmení, datum narození a adresa trvalého pobytu, případně adresa pro doručování, e-mail).[24]

Nižší míru anonymizace osobních údajů (zveřejnění jména a příjmení) musí strpět žadatelé, u nichž je podávání žádostí o informace součástí jejich profesního života, např. v pozici obecného zmocněnce, jakožto „svého druhu profesionála".[25] **Zveřejnění data narození žadatele nelze tolerovat ani u žádajícího podnikatele – profesionála, neboť s podnikáním nesouvisí.**[26]

Jakkoli je u podnikatelů – profesionálů do jisté míry oslabena ochrana osobních údajů

17) Ukázku soudního přezkumu anonymizace provedené Kanceláří veřejného ochránce práv představuje rozsudek Krajského soudu v Brně ze dne 31. 10. 2014, č. j. 31 A 1/2014 – 93 ve spojení s potvrzujícím rozsudkem Nejvyššího správního soudu ze dne 11.3. 2015, čj. 1 As 229/2014.

18) Takto má zavedeno např. Ústavní soud ČR. Tento způsob anonymizace bývá někdy označován jako „poloanonymizace", protože v některých případech mohou dopomoci k ztotožnění osoby.

19) Oproti předešlé variantě bezpochyby ztěžuje deanonymizaci dotčených osob.

20) Srov. § 5 odst. 3 a § 4b zákona o svobodném přístupu k informacím. Pozor na dodržení otevřeného a strojově čitelného formátu!

21) Srov. rozsudek Nejvyššího správního soudu ze dne 8. 11. 2019, čj. 9 As 241/2019 Sb. *„Citované ustanovení výslovně zakotvuje pouze povinnost zveřejňovat poskytnuté informace, standardním způsobem jeho naplnění je však právě to, že povinné subjekty zveřejňují veškerá svá rozhodnutí ve věci poskytování informací, včetně rozhodnutí negativních, což zde žalovaný legitimně odůvodnil snahou informovat veřejnost o typech žádostí o informace, které budou odmítány. Takový extenzivní výklad § 5 odst. 3 zákona o svobodném přístupu k informacím tedy není svévolný, naopak naplňuje smysl zákona. Jakmile je pak rozhodnutí zveřejňováno, je úplná či částečná anonymizace odůvodněna právě tehdy, pokud by jinak došlo k neodůvodněnému a nepřípustnému zveřejnění osobních údajů."*

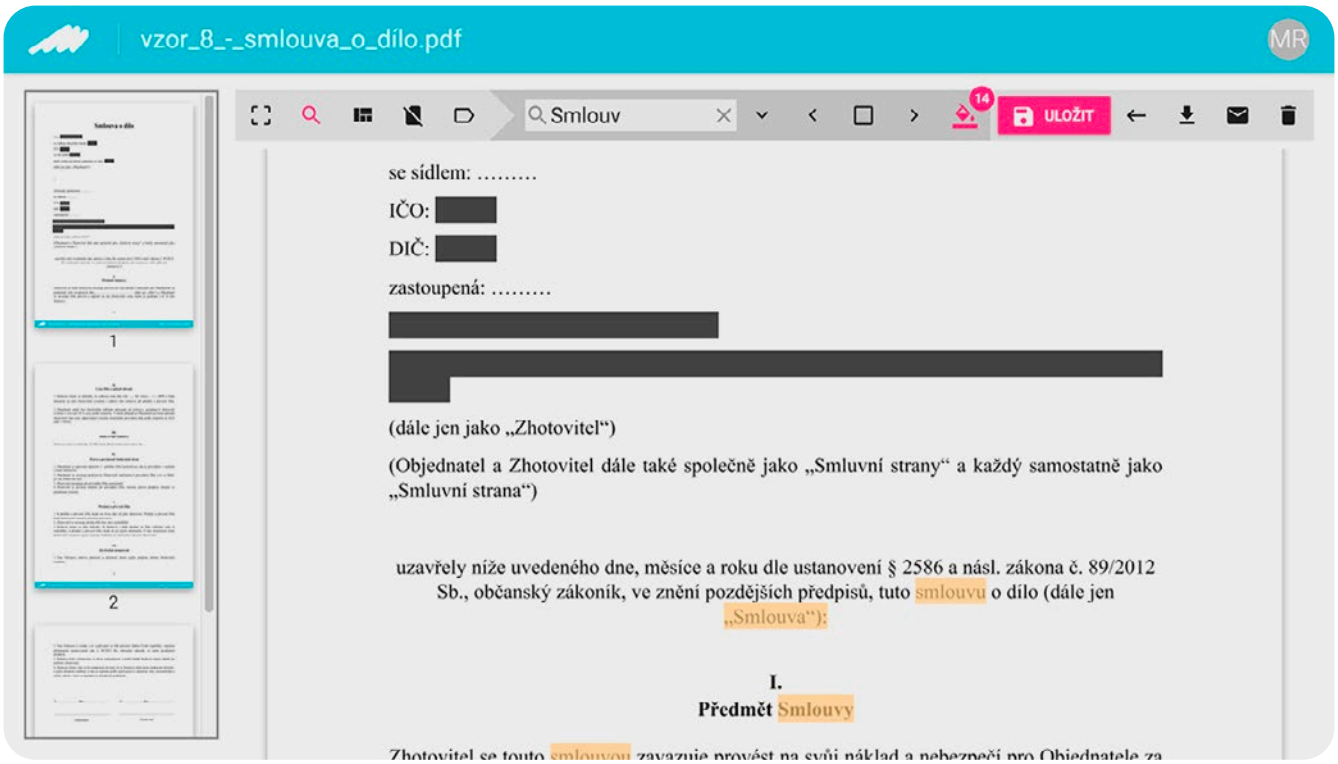
22) Při poskytování informací dle §16 odst. 2e) zákona o obcích.

23) Srov. stanovisko ODK MV 1/2012 dostupné:https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=12177

24) Srov. rozsudek Nejvyššího správního soudu ze dne 21. 8. 2018, č. j. 9 As 198/2018 – 37. *„Žadatel je povinen osobní údaje do žádosti uvést proto, aby tato mohla být ve smyslu zákona vyřízena. Osobní údaje však poskytuje výhradně pro potřeby identifikace žadatele a vedení řízení o podané žádosti, přičemž tento účel byl plně zkonzumován již vyřízením žádosti. Jakékoliv další zpracování (zveřejňování) takto získaných osobních údajů zákon nepředpokládá…. Následné zveřejnění osobních údajů tedy nepochybně překračovalo stanovený účel, pro který mohl stěžovatel dané osobní údaje zpracovávat, čímž došlo k porušení práv žalobce."*

25) Srov. rozsudek Nejvyššího správního soudu ze dne 8. 11. 2019, čj. 9 As 242/2019-47: musí strpět, že jeho jméno není anonymizováno při postupu podle § 5 odst. 3 zákona o svobodném přístupu k informacím. Není zde totiž ve hře ochrana jeho soukromí."

26) Srov. rozsudek Krajského soudu v Ústí nad Labem ze dne 21. 11. 2020, čj. 15 A 37/2019-86.



(zákon předvídá, resp. vyžaduje, aby řada osobních údajů byla uvedena v různých veřejných rejstřících, ve kterých jsou veřejně přístupné)[27], mohou se dovolávat ochrany svých osobních údajů, které se nevztahují k jejich podnikání.

Každý podnikatel by měl strpět neprovedení anonymizace svého jména, příjmení, adresy sídla či místa podnikání, neboť tyto údaje běžně ve spojitosti se svým podnikáním používá.[28]

Není nutné anonymizovat jména advokátů[29]**, daňových poradců či obdobných zástupců**, kteří před soudem či povinnými subjekty vystupují v rámci své profesionální činnosti. Lze tedy kupříkladu poskytnout informace o tom, kdo jako advokát, daňový poradce či obecný zmocněnec zastupoval anonymizovaného účastníka X. Y. v konkrétním řízení. Je tomu tak proto, že zastupování či poskytování jiné právní či odborné pomoci je součástí jejich veřejného a profesního života, nikoli života soukromého, v němž by bylo třeba respektovat jejich soukromí, informační sebeurčení a osobní údaje. Výjimkou může být jedině situace, kdy profesionálové vystupují v řízeních ryze ve své soukromé záležitosti nebo do výkonu jejich profesní činnosti zasáhne veskrze soukromá událost, například důvodem omluvy z účasti na jednání je nemoc, porod či jiná osobní událost.

Není nezbytné anonymizovat osobní údaje veřejně činných osob, pokud v řízení vystupují právě v souvislosti se svou veřejnou činností, resp. je-li znalost jejich účasti v daném řízení relevantní skutečností pro tvorbu veřejného názoru o kvalitách osoby, která veřejnou funkci vykonává nebo usiluje o její výkon.[30]

Veronika Gabrišová
Autorka pracuje v Kanceláři veřejného ochránce práv, je vedoucí odboru veřejného pořádku a místní správy, pověřenkyní pro ochranu osobních údajů a členkou rozkladové komise Úřadu pro ochranu osobních údajů.

27) Srov. rozsudek NSS ze dne 21. 8. 2018, čj. 9 As 198/2018-37, bod 29 – připomíná, že samotná okolnost, že se údaje fyzických osob nachází v otevřeném zdroji, sama o sobě další zpracování nelegalizuje. Nutno dodat, že obecné nařízení nepočítá s právním titulem, který obsahoval § 5 odst. 2 písm. d) zrušeného zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, tj. s možností zpracování oprávněně zveřejněných osobních údajů.

28) Srov. rozsudek Krajského soudu v Ústí nad Labem ze dne 21. 11. 2020, čj. 15 A 37/2019-86. Soud otevřeně přiznává, že korigoval své závěry vyslovené v rozsudku ze dne 4. 3. 2020, č. j. 15 A 215/2018-36 (v něm konstatoval nezákonný zásah spočívající ve zveřejnění osobních údajů žalobce na webových stránkách statutárního města Děčín, a to konkrétně jména a příjmení žalobce a ID datové schránky žalobce v rozhodnutí o odmítnutí poskytnutí informace), protože v němž nevycházel z aktuální judikatury Nejvyššího správního soudu.

29) K neanonymizaci jmen advokátů v soudních rozhodnutích viz rozsudek Nejvyššího správního soudu ze dne 31. 5. 2012, č. j. 9 Ans 5/2012 – 29; obdobně k neanonymizaci jména a příjmení kárně proviněného advokáta srov. rozsudek Nejvyššího správního soudu ze dne 21. 12. 2018, čj. 4 As 330/2018, bod 41.

30) Srov. rozsudek Nejvyššího správního soudu ze dne 20. 12. 2018, čj. 6 As 168/2018. Obdobně rozsudek Nejvyššího správního soud ze dne 6. 2. 2019, čj. 9 As 429/2018-35, č. 3864/2019 Sb. NSS.

DPO PRO. Ročník III, číslo 7–8. Vychází každého 28. dne v měsíci v Praze. Cena ročního předplatného činí 1 990 Kč bez DPH. Vydávají SMS-služby s. r. o. se sídlem V Rovinách 40, 140 00 Praha 4-Podolí, IČ: 067 84 771. Adresa redakce: Národní 41, 110 00 Praha 1-Staré Město. Webové stránky: https://www.dpopro.cz. Minimální rozsah 12 stran A4. Evidenční číslo: MK ČR E 24123. ISSN 2695-1363. Šéfredaktorka: JUDr. et Mgr. Eva Janečková, eva.janeckova@sms-sluzby.cz. Redakční rada: JUDr. et Mgr. Eva Janečková, Ing. Mgr. Oldřich Kužílek, Ing. Michal Merta, MBA, MSc., LL.M., JUDr. Adam Furek. Jazyková redakce: Marie Machačová. Předplatné: Magdalena Komárková, magdalena.komarkova@sms-sluzby.cz, tel.: +420 723 644 867. Grafické práce: Studio Matrix. Redakční uzávěrka: 25. 7. 2023.