PRO

OCHRANA OSOBNÍCH ÚDAJŮ V PRAXI

Číslo 9/2023, ročník III. Měsíčník SMS - služby s. r. o. www.dpopro.cz

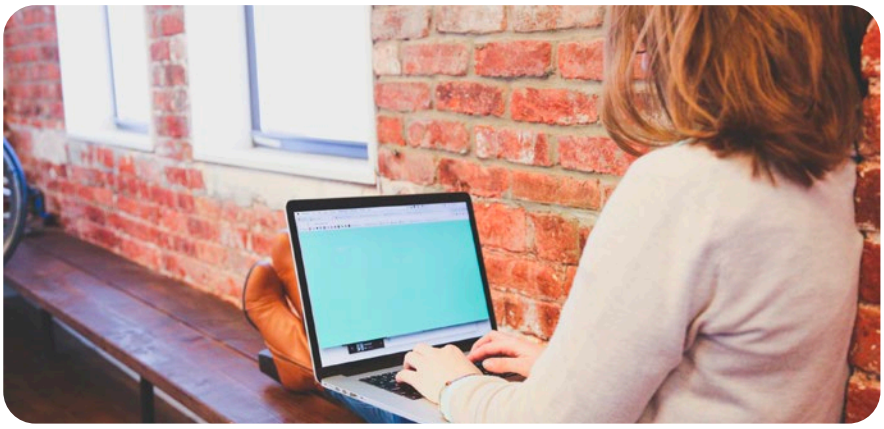
Nejproblematičtější je narušování soukromí zaměstnanců na pracovišti

Rozhovor

Ani inspektoráty práce se při své činnosti nevyhnou kontrolám, které úzce souvisí s ochranou osobních údajů. Týká se to zejména kontroly dodržování § 316 odst. 2 zákoníku práce, tedy zákazu narušování soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele. Nejen o tom, jak inspektoráty postupují při svých kontrolách, jsem si povídala s Dalimilou Solnickou, která je vedoucí Úseku inspekce PPV.

Sdílí mezi sebou jednotlivé inspektoráty informace o kontrolách včetně osobních údajů?

Co se týká sdílení informací o kontrolách mezi Státním úřadem inspekce práce (SÚIP) a jednotlivými oblastními inspektoráty práce (OIP), k určitému sdílení samozřejmě v rámci kontrolní činnosti musí docházet. Jedná se například o situace, kdy je kontrola jednoho zaměstnavatele v místní příslušnosti více oblastních inspektorátů práce (zaměstnavatel má například více pracovišť v různých krajích, centrální vedoucí pracoviště a pobočky atp.).



Jak takové sdílení ještě probíhá?

Typickými příklady sdílení jsou pak případy, kdy SÚIP uplatňuje svou řídící nebo metodickou působnost vůči OIP – např. při vyřízení stížnosti na provedení či výsledek kontroly OIP je nezbytné, aby se SÚIP seznámil s celým kontrolním spisem. Obdobně se tak děje při tzv. vnitřní kontrole, kdy SÚIP kontroluje vybrané výstupy OIP a výstupem je pak metodické vedení OIP, sladění postupů OIP, statistické analýzy atp. Platí, že sdílení informací získaných kontrolní činností, včetně osobních údajů, se děje v odůvodněných případech a nikoli nahodile nebo bezúčelně. Zásadní v této souvislosti je, že příslušní zaměstnanci orgánů inspekce práce jsou vázáni povinností zachovávat mlčenlivost o všech skutečnostech, které se dozvěděli v souvislosti s výkonem kontroly, a povinností nezneužívat takto získaných informací. Tato povinnost trvá i po skončení pracovněprávního vztahu pracovníka inspekce práce (ust. § 20 zákona č. 255/2012 Sb., o kontrole [kontrolní řád]).

V případě, kdy je výstup z reálné kontroly použit jako příklad v rámci metodického vedení ostatních OIP, školení inspektorů apod., je materiál vždy upraven ve smyslu znemožnění náhledu na osobní údaje.

Krásné podzimní dny, vážení čtenáři!

Jednou z nejproblematičtějších oblastí ve vztahu k ochraně osobních údajů je narušování soukromí zaměstnanců na pracovišti, říká vedoucí Úseku inspekce pracovněprávních vztahů Dalimila Solnická. Rozhovorem s ní otevíráme poprázdninové číslo 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 vás zve například na tradiční výroční konferenci, jež se uskuteční ve čtvrtek 5. října v Praze.

Jakých informací se týká právo na přístup k osobním údajům uvedené v článku 15 obecného nařízení (GDPR)? Touto otázkou se jako předběžnou zabýval také Soudní dvůr a my o tom podrobně informujeme.

Ochrana osobních údajů a kybernetická bezpečnost patří k sobě, konstatuje ve svém článku Jana Lix Andraščiková, v němž se zabývá vztahem obecného nařízení (GDPR) a nařízením DORA.

Nad riziky propojených nemocničních informačních systémů pro bezpečnost osobních údajů se pozastavil Ondřej Fiala. Ve svém textu uvádí mimo jiné, že problematickým se tyto komplexní zpracovatelské procesy stávají v momentě, kdy jednotliví aktéři nesprávně posoudí své role při zapojení do zpracování osobních údajů.

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

V praxi se stávalo, že kontrolované osoby odmítaly poskytnout kontrolnímu úřadu dokumenty požadované v rámci kontroly s tím, že dokumenty obsahují osobní údaje, a není je proto možné poskytnout. Setkávají se s touto argumentací inspektoři stále nebo už se povědomí o právech kontrolujících osob mezi zaměstnavateli zlepšilo a tento problém zmizel?

Se situacemi, kdy kontrolovaný zaměstnavatel odmítá nebo se zdráhá předložit požadované dokumenty ke kontrole s tím, že tyto dokumenty obsahují osobní údaje, se inspektoři setkávají, avšak víceméně ojediněle. Po poučení a vysvětlení kompetencí orgánů inspekce práce (poučení o povinnosti poskytnout součinnost kontrolujícímu orgánu – ust. § 10 kontrolního řádu, o povinnosti kontrolujícího zachovávat mlčenlivost dle § 20 kontrolního řádu) kontrolovaná osoba nakonec požadované dokumenty inspektorovi vždy předloží (nebo jsou důvody pro jejich nepředložení jiné, než je obava kontrolované osoby o ochranu osobních údajů).

Historicky vždy inspektoráty práce a Úřad pro ochranu osobních údajů diskutovaly, do čí kompetence spadá řešení prohřešků proti § 316 zákoníku práce, který zaměstnavateli zakazuje bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci. Situace se vyjasnila přidáním nového ustanovení do zákona o inspekci práce – Přestupky na Úseku ochrany soukromí a osobních práv zaměstnanců. Jak probíhá kontrola a správní trestání na tomto úseku?

Pokud jde o samotné nakládání zaměstnavatele s osobními údaji zaměstnanců, tato oblast nespadá do kontrolní působnosti orgánů inspekce práce (Státního úřadu inspekce práce a oblastních inspektorátů práce), ale do působnosti Úřadu pro ochranu osobních údajů. Orgány inspekce práce se v rámci své

kontrolní činnosti zaměřují na oblast ochrany soukromí a osobních práv zaměstnanců, a tedy na dodržování povinností ze strany zaměstnavatele dle ust. § 316 zákoníku práce.

Před rokem 2020 byla ochrana soukromí a osobních práv zaměstnanců opakovaně zařazována mezi hlavní kontrolní oblasti Státního úřadu inspekce práce a patřila mezi kontrolní priority. V posledních letech tomu tak není (prioritními se staly jiné, také aktuální úkoly, například kontrola pracovních podmínek zaměstnanců v době karantény či kontrola pracovních podmínek držitelů dočasné ochrany z Ukrajiny), to ovšem neznamená, že by oblast ochrany soukromí a osobních práv zaměstnanců přestala být kontrolována. Kontroly na Úseku ochrany soukromí a osobních práv zaměstnanců probíhají v převážné většině u těch zaměstnavatelů, o nichž orgány inspekce práce získají informace o možném porušování právních předpisů v oblasti ochrany osobních práv zaměstnanců nebo o provozování kamerového systému zaměstnavatelem, prostřednictvím podnětů ke kontrole či na základě poskytovaného poradenství.

Jak již bylo řečeno, předmětem kontrol v oblasti ochrany osobních práv zaměstnanců je ust. § 316 zákoníku práce. Dle ust. § 316 odst. 1 zákoníku práce *„zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.“* Dále podle ust. § 316 odst. 4 *„zaměstnavatel nesmí vyžadovat od zaměstnance informace, které bezprostředně nesouvisejí s výkonem práce a se základním pracovněprávním vztahem uvedeným v § 3. Nesmí vyžadovat informace zejména o:*

a) těhotenství,
b) rodinných a majetkových poměrech,
c) sexuální orientaci,
d) původu,
e) členství v odborové organizaci,
f) členství v politických stranách nebo hnutích,
g) příslušnosti k církvi nebo náboženské společnosti,
h) trestněprávní bezúhonnosti;

to, s výjimkou písmen c), d), e), f) a g), neplatí, jestliže je pro to dán věcný důvod spočívající v povaze práce, která má být vykonávána, a je-li tento požadavek přiměřený, nebo v případech, kdy to stanoví tento zákon nebo zvláštní právní předpis. Tyto informace nesmí zaměstnavatel získávat ani prostřednictvím třetích osob.“

Výše uvedená ustanovení ovšem nejsou ze strany zaměstnanců příliš problematická a v podnětech se jiné oblasti, než je narušení soukromí prostřednictvím kamerových systémů, objevují spíše výjimečně.

Samostatnou kapitolou jsou právě kamerové systémy jako specifická forma sledování. V posledních letech se na evropské půdě objevilo několik soudních rozhodnutí, která minimálně zdánlivě tuto problematiku rozvolňují. Jak se na tuto otázku dívá SÚIP?

Nejproblematičtějším a nejvíce porušovaným ustanovením je dlouhodobě porušení ustanovení § 316 odst. 2 zákoníku práce, tedy situace, kdy inspektor shledá absenci závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele (vysvětleno níže) a zjistí narušování soukromí zaměstnanců na pracovišti, popřípadě ve společných prostorách zaměstnavatele. V praxi je nejběžnějším způsobem

Další obsah

narušení soukromí prostřednictvím kamerových systémů. Do této oblasti taktéž směřuje největší počet obdržených podnětů, neboť pro zaměstnance může být narušení jejich soukromí prostřednictvím kamerového systému nejcitelnějším zásahem do jejich osobnostních práv.

Dle ust. § 316 odst. 2 zákoníku práce zaměstnavatel nesmí narušovat soukromí zaměstnanců na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci, aniž by k tomu neměl závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele. V případě, že není tento důvod u zaměstnavatele dán, nesmí narušit chráněné hodnoty (soukromí) zaměstnanců ani v případě, že by s tím zaměstnanci souhlasili.

Dále se inspektoři v rámci kontroly zaměřují na skutečnost, aby v případě, že je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti odůvodňující zavedení daného kontrolního mechanismu, byli zaměstnanci o rozsahu kontroly a o způsobech jejího provádění přímo informováni.

V souvislosti s ochranou osobních práv zaměstnanců orgány inspekce práce dlouhodobě apelují na zaměstnavatele, aby i v kontextu zákonných podmínek závažného důvodu spočívajícího ve zvláštní povaze činnosti podrobovali užití daných prostředků testu proporcionality. V rámci testu proporcionality se posuzuje užití daného monitorovacího prostředku z hlediska:

- vhodnosti – zda je daný prostředek způsobilý k dosažení cíle,
- potřebnosti – zda není možné cíle dosáhnout jiným způsobem a šetrněji,
- přiměřenosti – zda jsou vyváženy střetávající se hodnoty (např. zájem zaměstnavatele na ochraně svého majetku na straně jedné a chráněný zájem (soukromí) zaměstnance na straně druhé).

Co může být například takovým závažným důvodem?

Z pohledu inspekce práce závažný důvod zpravidla není dán při výrobě běžných výrobků nebo při poskytování běžných služeb. Takovým závažným důvodem může být například skutečnost, že na pracovišti dochází k manipulaci s vyššími finančními částkami (typicky banka), je zde určité bezpečnostní riziko (benzinová čerpací stanice) nebo zvýšené riziko ohrožení zdraví osob nebo majetku (chemická výroba apod.). Hodnocení je však vždy třeba vztáhnout ke konkrétnímu pracovišti a konkrétnímu zaměstnavateli. Je nutno uvést, že na žádném pracovišti ovšem nemohou být monitorovány prostory, jako jsou toalety, šatny nebo sprchy. Kamery také nemohou primárně sloužit ke sledování zaměstnanců (jejich aktivity a pracovní výkonosti na pracovišti). Za přiměřené se považuje například monitorování prostoru pokladní přepážky v bance, avšak nikoli samotné osoby zaměstnance. Kamera má snímat prostor, kde zaměstnanec přebírá hotovost a ukládá ji do pokladny, tedy je zaměřena na ruce zaměstnance, a nikoli na jeho celou postavu.

Jak se postupuje v případě porušení právních předpisů na Úseku ochrany soukromí a osobních práv zaměstnanců nebo v případě neinformování zaměstnanců?

V případě zjištěného porušení právních předpisů na Úseku ochrany soukromí a osobních práv zaměstnanců je možno u kontrol provedených po 29. 7. 2017 zaměstnavateli uložit za nezákonné narušení soukromí zaměstnance a za vyžadování nedovolených informací od zaměstnance pokutu až do výše 1 000 000 Kč, v případě neinformování zaměstnanců o rozsahu a způsobu prováděné kontroly je to pak pokuta až do výše 100 000 Kč. Zaměstnavatelé si v některých případech nejsou vědomi omezení a podmínek, které jsou v zákoníku práce stanoveny, co se týká ochrany majetkových zájmů zaměstnavatele a ochrany osobních práv zaměstnanců, a v mnoha případech nejsou informováni o nabytí účinnosti novely zákona o inspekci práce, která umožnila orgánům inspekce práce za tato porušení ukládat pokuty.

Dalimila Solnická
vystudovala právo na Masarykově univerzitě, od roku 2010 pracuje na Státním úřadu inspekce práce v Opavě, kde se věnuje metodické a řídící činnosti na úseku kontrol zaměstnavatelů v oblasti dodržování práv a povinností v pracovněprávních vztazích; zabývala se zde také metodickou činností v oblasti zaměstnanosti a nelegální práce. Podílí se na odborném vzdělávání inspektorů práce, o činnosti orgánů inspekce práce v oblasti kontroly pracovněprávních vztahů referuje na vzdělávacích akcích, seminářích, konferencích. Dříve, než se zaměřila na pracovní právo, věnovala se právu trestnímu jako vyšetřovatelka v oblasti hospodářské trestné činnosti. Krátce také pracovala na Magistrátu města Opavy.

Kolik takových pokut už bylo uloženo?

V roce 2022 bylo v oblasti ochrany soukromí a osobních práv zaměstnanců uloženo celkem šest pokut v celkové výši 126 000 Kč. O výši pokuty je vždy rozhodováno dle konkrétních skutečností, mimo jiné se při stanovení výše pokuty přihlíží k povaze a závažnosti přestupku, ke způsobu jeho spáchání a jeho následkům a k okolnostem, za nichž byl spáchán (přihlíží se například k tomu, zda se zaměstnavatel dopustil jednání opakovaně, v jakém rozsahu se jednání dopustil, kolika zaměstnanců se pochybení týkalo apod.). V této souvislosti je třeba si uvědomit, že v zákoně o inspekci práce jsou obsaženy také přestupky, vykazující vyšší míru společenské škodlivosti, než je například přestupek spočívající v neinformování zaměstnanců o způsobu a rozsahu kontroly. Sankce je ukládána v případě vícero přestupků v souladu s tzv. absorpční zásadou, je tedy ukládána za nejzávažnější přestupek a v mnoha případech dochází k tomu, že je sankce zaměstnavateli uložena za jiný, z pohledu zákona o inspekci práce závažnější přestupek, který byl

v rámci kontroly a následujícího správního řízení u zaměstnavatele zjištěn.

Jak vypadá vaše spolupráce s Úřadem pro ochranu osobních údajů?

V případě, že Státní úřad inspekce práce obdrží podnět ke kontrole, ze kterého je na první pohled zřejmé, že nespadá do věcné působnosti inspekce práce (např. podnětem je upozorňováno na možné neoprávněné nakládání s osobními údaji zaměstnanců, nikoliv na porušování ust. § 316 zákoníku práce), postoupí jej SÚIP Úřadu pro ochranu osobních údajů. Stejný postup je aplikován i v případě, že Úřad pro ochranu osobních údajů obdrží podnět upozorňující na možné porušování ustanovení § 316 zákoníku práce, postoupí jej Státnímu úřadu inspekce práce. Obdobně se postupuje i v rámci poradenské činnosti.

V rámci mezinárodní spolupráce Státní úřad inspekce práce zajišťuje povinnosti a úkoly plynoucí z členství v evropských a mezinárodních organizacích a stejně tak i z ustanovení bilaterálních dohod o spolupráci se zahraničními partnery. Dochází v rámci této spolupráce k předávání osobních údajů do zahraničí, včetně předání mimo EU?

Co se týká předávání dokumentů obsahujících osobní údaje do zahraničí, je Státní úřad inspekce práce vázán do české legislativy transponovanými evropskými směrnicemi pro oblast vysílání pracovníků (vč. vysílání řidičů mezinárodní dopravy) a nařízením (EU) č. 1024/2012 ze dne 25. října 2012 o správní spolupráci prostřednictvím systému pro výměnu informací o vnitřním trhu (IMI). Po věcné stránce se jedná o:

- Směrnici Evropského parlamentu A Rady 96/71/ES ze dne 16. prosince 1996 o vysílání pracovníků v rámci poskytování služeb,
- Směrnici Evropského parlamentu A Rady 2014/67/EU ze dne 15. května 2014 o prosazování směrnice 96/71/ES,
- Směrnici Evropského parlamentu A Rady (EU) 2018/957 ze dne 28. června 2018, kterou se mění směrnice 96/71/ES,
- Směrnici Evropského parlamentu a Rady (EU) 2020/1057 ze dne 15. července 2020, kterou se stanoví zvláštní pravidla o vysílání řidičů v odvětví silniční dopravy.

Spočívá tato spolupráce také v předávání osobních údajů konkrétních osob?

Mimo jiné ano. Jedná se zejména o případy, kdy na základě žádosti zahraničních orgánů prostřednictvím modulu IMI (viz níže) pro oblast vysílání pracovníků dochází k poskytování informací o vyslaných pracovnících.

Systém IMI (modul Vysílání pracovníků) umožňuje registrovaným orgánům z členských států zasílat žádosti o zjištění/prověření informací mj. o vyslání konkrétních zaměstnanců, požadovat doručení pravomocného rozhodnutí o pokutě českému vysílacímu subjektu, a nakonec i žádat o vymožení pokuty tomuto subjektu uložené v zahraničí.

V rámci uzavřených dohod, popř. memorand o spolupráci s některými orgány typu národního inspektorátu práce, rovněž existuje teoretická možnost osobní informace poskytnout. V praxi je však jako jediný prostředek k předání osobních údajů do zahraničí využíván právě systém IMI. Tato spolupráce se ovšem týká výhradně orgánů členských států EU v systému IMI registrovaných.

Rozhovor vedla Eva Janečková

Podzim ve znamení vzdělávacích akcí a mezinárodní spolupráce

Po lehkém letním odpočinku se Spolek pro ochranu osobních údajů v plné síle vrátil ke svému hlavnímu poslání: Rozvíjet odbornou diskusi o tématech spojených se soukromím, zpracováním osobních údajů a ochranou informací. Tím Spolek pomáhá svým členům, i dalším profesionálům v těchto oblastech, řešit praktické otázky a připravit se na budoucí požadavky.

Setkání s judikaturou aneb Co všechno je osobní údaj?

Ve čtvrtek 7. září Spolek pro své členy uspořádal další setkání s judikaturou. Šlo o pravidelné online setkání, kde se analyzují nová rozhodnutí evropských i národních soudů, která mají přímý a významný dopad pro praxi. Tentokrát jsme se zabývali aktuálním rozsudkem Nejvyššího správního soudu k definici osobního údaje, ve kterém soud přistoupil k důsledně objektivnímu, a tedy širokému výkladu tohoto pojmu, a také rozsudkem Soudního dvora EU v kauze Meta ze dne 4. července 2023.

Zkušenosti ze schvalování závazných podnikových pravidel

Závazná podniková pravidla, používá se také anglický pojem Binding Corporate Rules (BCR), jsou jedním z nástrojů, kterými lze zajistit dostatečnou ochranu práv dotčených osob při předávání jejich dat mimo EU/EHP. BCR schvaluje dozorový úřad podle hlavního sídla správce údajů, často mateřské společnosti nebo hlavní pobočky pro EU. V praxi se jedná o relativně málo využívaný nástroj. Například český dozorový orgán, Úřad pro ochranu osobních údajů, zatím žádná BCR neschválil. Slovenský dozorový úřad ovšem v loňském roce první závazná podniková pravidla schvaloval. A také schválil. V úterý 19. září se s členy Spolku se svými zkušenostmi ze schvalovacího procesu podělil Jakub Berthoty z advokátní kanceláře Dagital Legal, který žadatele v řízení před slovenským úřadem zastupoval.

Tradiční konference Spolku se koná už 5. října

Vrcholem podzimních akcí bude tradiční výroční konference Spolku, která se bude konat už po sedmé, tentokrát ve čtvrtek 5. října v Praze. Konference bude opět rozdělena na dopolední část s vystoupeními řečníků z České republiky i zahraničí a odpolední paralelní workshopy na různá témata (umělá inteligence, kamerové systémy, kybernetická bezpečnost atd.).

Spolupráce s italskou asociací a společný workshop na téma whistleblowing

Náš Spolek navázal spolupráci s italskou asociací sdružující pověřence pro ochranu osobních údajů a další profesionály z oblasti ochrany dat z Apeninského poloostrova, Federprivacy. Prvním společným projektem bude online workshop na téma whistleblowing

a problematické body ochrany dat, který se uskuteční ve čtvrtek 26. října. Workshop bude mít formu panelové diskuse a vystoupí na něm zástupci za český Spolek, italskou asociaci a další partnerská sdružení, se kterými spolupracujeme v rámci Evropské federace pověřenců pro ochranu osobních údajů.

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.

Článek 15 GDPR nezakotvuje povinnost předat informace o totožnosti zaměstnanců správce, kteří prováděli tyto operace z jeho pověření

Dne 22. června 2023 vydal Soudní dvůr rozhodnutí ve věci C-579/21 o předběžné otázce týkající se rozsahu práva na přístup k informacím uvedeným v článku 15 obecného nařízení (GDPR). O jaký případ se jednalo?

Spor v původním řízení a předběžné otázky

V průběhu roku 2014 se J. M., tehdejší zaměstnanec a klient společnosti Pankki S, dozvěděl, že v období od 1. listopadu do 31. prosince 2013 zaměstnanci banky několikrát nahlíželi do jeho údajů jakožto klienta. [20]

Vzhledem k tomu, že J. M. měl pochybnosti o zákonnosti těchto nahlížení, požádal společnost Pankki S, aby mu sdělila totožnost osob, které nahlížely do jeho klientských údajů, přesná data nahlížení, jakož i účel zpracování uvedených údajů. [21]

V odpovědi společnost Pankki S, jakožto správce ve smyslu čl. 4 bodu 7 GDPR, odmítla sdělit totožnost zaměstnanců, kteří provedli operace nahlížení. Jako důvod uvedla, že informace představují osobní údaje těchto zaměstnanců. [22]

V téže odpovědi však společnost Pankki S poskytla podrobnosti o operacích nahlížení, které na její pokyn provedlo její oddělení interního auditu. Vysvětlila, že klient banky, jejímž klientským poradcem byl J. M., byl věřitelem osoby, která má rovněž iniciály J. M., takže si přála objasnit, zda žalobce v původním řízení a dotčený dlužník jsou jedna a tatáž osoba a zda mohlo dojít k nepřípustnému vztahu střetu zájmů. Společnost Pankki S dodala, že vyjasnění této otázky si vyžádalo zpracování údajů J. M. a že každý zaměstnanec banky, který tyto údaje zpracovával, předložil oddělení interního auditu prohlášení o důvodech tohoto zpracování údajů. Banka dále uvedla, že tato nahlížení umožnila vyloučit jakékoli podezření ze střetu zájmů, pokud jde o J. M. [23]

J. M. se obrátil na dozorový úřad ve smyslu čl. 4 bodu 21 GDPR, aby bylo společnosti Pankki S nařízeno poskytnout mu požadované informace. [24]

Rozhodnutím zástupce pověřence pro ochranu osobních údajů žádost J. M. zamítl. Vysvětlil, že účelem této žádosti bylo umožnit mu přístup k protokolovým souborům zaměstnanců, kteří zpracovávali jeho údaje, přičemž na základě jeho rozhodovací praxe takové soubory představují osobní údaje týkající se nikoli subjektu údajů, ale zaměstnanců, kteří zpracovávali údaje této osoby. [25]

J. M. podal proti tomuto rozhodnutí žalobu k předkládajícímu soudu. [26]

Uvedený soud připomíná, že článek 15 GDPR stanoví právo subjektu údajů získat od správce přístup ke zpracovávaným údajům, které se ho týkají, jakož i informace týkající se zejména účelů zpracování a příjemců údajů. Klade si otázku, zda se na sdělení protokolových souborů vytvořených v souvislosti s operacemi zpracování, které obsahují takové informace, zejména totožnost zaměstnanců správce, vztahuje článek 15 GDPR, jelikož tyto soubory mohou být pro subjekt údajů nezbytné pro posouzení zákonnosti zpracování, jehož předmětem byly jeho údaje. [27]

Za těchto podmínek se soud rozhodl přerušit řízení a položit Soudnímu dvoru následující předběžné otázky: [28]

„1) Musí být právo subjektu údajů na přístup, které mu přiznává čl. 15 odst. 1 [GDPR], vykládáno ve spojení s [pojmem] ‚osobní údaje' ve smyslu čl. 4 bodu 1 tohoto nařízení tak, že informace shromažďované správcem, z nichž vyplývá, kdo osobní údaje subjektu údajů, kdy a k jakému účelu zpracovával, nejsou informacemi, na jejichž zpřístupnění má subjekt údajů právo, zejména z toho důvodu, že se jedná o údaje, které se týkají zaměstnanců správce?

2) V případě kladné odpovědi na první otázku, tedy že subjekt údajů nemá na základě čl. 15 odst. 1 GDPR právo na přístup k informacím uvedeným v této otázce, jelikož nejsou ‚osobními údaji' subjektu údajů podle čl. 4 bodu 1 tohoto nařízení, je třeba se v projednávané věci ještě zabývat otázkou informací, k nimž má subjekt údajů právo na přístup podle čl. 15 odst. 1 písm. [a) až h)] tohoto nařízení:

a) Jak musí být vykládán ‚účel zpracování' ve smyslu čl. 15 odst. 1 písm. a) [GDPR] s ohledem na rozsah práva subjektu údajů na přístup k osobním údajům, tedy může účel zpracování zakládat právo na přístup k protokolovým souborům uživatele, které shromáždil správce, jako jsou například informace o osobních údajích osob provádějících zpracování osobních údajů subjektu údajů, době a účelu tohoto zpracování?

b) Mohou být osoby, které zpracovávaly v bance údaje o J. M. jakožto klientovi, v této souvislosti považovány za určitých podmínek za ‚příjemce' osobních údajů podle čl. 15 odst. 1 písm. c) [GDPR] ve vztahu, k nimž by měl subjekt údajů právo na informace?

3) Je pro projednávanou věc relevantní, že se jedná o banku, která vykonává regulovanou činnost, nebo že J. M. pracoval pro banku a zároveň byl jejím klientem?

4) Je pro posouzení výše uvedených otázek relevantní, že ke zpracování údajů o J. M. došlo před vstupem [GDPR] v platnost?"

Ke čtvrté otázce

Jak uvedl generální advokát v bodě 33 svého stanoviska, čl. 15 odst. 1 GDPR přiznává subjektům údajů procesní právo spočívající v získání informací o zpracování jejich osobních údajů. Jakožto procesní pravidlo se toto ustanovení použije na žádosti o přístup podané po dni, kdy se toto nařízení stalo použitelným, jako je žádost J. M. [35]

Za těchto podmínek je třeba na čtvrtou otázku odpovědět tak, že článek 15 GDPR musí být ve světle čl. 99 odst. 2 tohoto nařízení vykládán v tom smyslu, že se použije na žádost o přístup k informacím uvedeným v tomto ustanovení, pokud byly operace zpracování týkající se této žádosti provedeny přede dnem, kdy se uvedené nařízení stalo použitelným, ale žádost byla podána po tomto datu. [36]

K první a druhé otázce

Podstata první a druhé otázky předkládajícího soudu, které je třeba posoudit společně, spočívá v tom, zda musí být čl. 15 odst. 1 GDPR vykládán ve smyslu, že informace týkající se operací nahlížení do osobních údajů osoby, jež se týkají dat a účelů těchto operací, jakož i totožnosti fyzických osob, které tyto operace provedly, představují informace, které má tato osoba právo získat od správce na základě tohoto ustanovení. [37]

Z textové analýzy čl. 15 odst. 1 GDPR a pojmů v něm obsažených tedy vyplývá, že právo na přístup, které toto ustanovení subjektu údajů přiznává, se vyznačuje širokým rozsahem informací, které musí správce tomuto subjektu poskytnout. [49]

Pokud jde dále o kontext čl. 15 odst. 1 GDPR, je třeba v prvé řadě připomenout, že bod 63 odůvodnění tohoto nařízení stanoví, že každý subjekt údajů by měl mít právo vědět a být informován zejména o tom, za jakým účelem se osobní údaje zpracovávají, případně období, po které budou uchovávány, a kdo jsou příjemci osobních údajů. [50]

Mimoto, jak vyplývá z bodu 63 odůvodnění GDPR, cílem práva osoby na přístup k vlastním osobním údajům a k dalším informacím uvedeným v čl. 15 odst. 1 tohoto nařízení je především umožnit tomuto subjektu, aby se seznámil se zpracováním svých údajů a aby si ověřil zákonnost zpracování. Z tohoto bodu odůvodnění, a jak je uvedeno v bodě 50 tohoto rozsudku, vyplývá, že každý subjekt údajů by proto měl mít právo vědět a být informován zejména o tom, za jakým účelem se osobní údaje zpracovávají, případně období, po které budou uchovávány, kdo jsou příjemci osobních údajů a v čem spočívá logika zpracování osobních údajů. [56]

Konkrétně je toto právo na přístup nezbytné k tomu, aby subjekt údajů mohl případně vykonat právo na opravu, právo na výmaz („právo být zapomenut“) a právo na omezení zpracování, které mu přiznávají články 16 až 18 GDPR, právo na námitku proti zpracování svých osobních údajů stanovené v článku 21 GDPR, jakož i právo na soudní ochranu pro případ utrpěné škody, zakotvené. [58]

V projednávané věci není zpochybňováno, že operace nahlížení, jejichž předmětem byly osobní údaje žalobce v původním řízení, představují „zpracování“ ve smyslu čl. 4 bodu 2 GDPR, takže na základě nich mu podle čl. 15 odst. 1 tohoto nařízení vzniká nejen právo na přístup k těmto osobním údajům, ale rovněž právo na zpřístupnění informací v souvislosti s těmito operacemi, jak jsou uvedeny v posledně uvedeném ustanovení. [61]

Pokud jde o takové informace, jako jsou informace požadované J. M., sdělení především dat nahlížení může subjektu údajů umožnit získat potvrzení o tom, že jeho osobní údaje byly v daném okamžiku skutečně zpracovány. Mimoto vzhledem k tomu, že podmínky zákonnosti stanovené v článcích 5 a 6 GDPR musí být splněny v okamžiku samotného zpracování, představuje datum tohoto zpracování prvek umožňující ověřit jeho zákonnost. Dále je třeba uvést, že informace týkající se účelů zpracování je výslovně uvedena v čl. 15 odst. 1 písm. a) tohoto nařízení. Konečně čl. 15 odst. 1 písm. c) uvedeného nařízení stanoví, že správce informuje subjekt údajů o příjemcích údajů. [62]

Pokud jde konkrétně o protokolové soubory správce, sdělení kopie informací obsažených v těchto souborech se může ukázat jako nezbytné k tomu, aby byla splněna povinnost poskytnout subjektu údajů přístup ke všem informacím uvedeným v čl. 15 odst. 1 GDPR a aby bylo zaručeno spravedlivé a transparentní zacházení, což by mu umožnilo plně uplatnit práva, která pro něj vyplývají z tohoto nařízení. [69]

Zaprvé totiž takové soubory odhalují existenci zpracování údajů, tedy informace, ke kterým musí mít subjekt údajů přístup na základě čl. 15 odst. 1 GDPR. Kromě toho informují o četnosti a intenzitě operací nahlížení, a umožňují tak subjektu údajů ujistit se o tom, že prováděné zpracování je skutečně odůvodněno účely, které správce uvádí. [70]

Zadruhé tyto soubory obsahují informace týkající se totožnosti osob, které provedly operace nahlížení. [71]

Z předkládacího rozhodnutí nicméně zaprvé vyplývá, že informace obsažené v protokolových souborech, jako jsou informace dotčené ve věci v původním řízení, umožňují identifikovat zaměstnance, kteří provedli operace zpracování a obsahují osobní údaje těchto zaměstnanců ve smyslu čl. 4 bodu 1 GDPR. [76]

V tomto ohledu je třeba připomenout, že pokud jde o právo na přístup stanovené v článku 15 GDPR, bod 63 odůvodnění tohoto nařízení upřesňuje, že „tímto právem by neměla být nepříznivě dotčena práva ani svobody ostatních“. [77]

I když může být nezbytné, aby byl subjekt údajů informován o totožnosti zaměstnanců správce, aby se ujistil o zákonnosti zpracování svých osobních údajů, je nicméně pravděpodobné, že tím budou nepříznivě dotčena práva a svobody těchto zaměstnanců. [79]

Zadruhé z předkládacího rozhodnutí vyplývá, že J. M. nepožaduje sdělení informací o totožnosti zaměstnanců společnosti Pankki S, kteří nahlíželi na jeho osobní údaje, neboť ve skutečnosti nejednali z pověření a v souladu s pokyny správce, ale podle všeho pochybuje o pravdivosti informací týkajících se účelu těchto nahlížení, které mu sdělila společnost Pankki S. [81]

Z výše uvedených úvah vyplývá, že čl. 15 odst. 1 GDPR musí být vykládán v tom smyslu, že informace o operacích nahlížení do osobních údajů subjektu, které se týkají dat a účelů těchto operací, jsou informacemi, které má tento subjekt právo získat od správce podle tohoto ustanovení. Uvedené ustanovení naproti tomu takové právo nezakotvuje, pokud jde o informace o totožnosti zaměstnanců uvedeného správce, kteří prováděli tyto operace z jeho pověření a v souladu s jeho pokyny, ledaže jsou tyto informace nezbytné k tomu, aby subjekt údajů mohl účinně vykonávat práva, která mu toto nařízení přiznává, a za podmínky, že jsou zohledněna práva a svobody těchto zaměstnanců. [83]

Ke třetí otázce

Podstatou třetí otázky předkládajícího soudu je, zda okolnost, že správce vykonává bankovní činnost v rámci regulované činnosti a osoba, jejíž osobní údaje byly zpracovány jakožto klienta správce, byla rovněž zaměstnancem tohoto správce, je relevantní pro účely vymezení rozsahu práva na přístup, které jí přiznává čl. 15 odst. 1 GDPR. [84]

Úvodem je třeba zdůraznit, že pokud jde o oblast působnosti práva na přístup stanoveného v čl. 15 odst. 1 GDPR, žádné ustanovení tohoto nařízení nerozlišuje v závislosti na povaze činností správce nebo postavení osoby, jejíž osobní údaje jsou zpracovávány. [85]

Pokud jde dále o okolnost, že J. M. byl zároveň klientem a zaměstnancem společnosti Pankki S, je třeba uvést, že s ohledem nejen na cíle GDPR, ale i na rozsah práva na přístup k osobním údajům, které má subjekt údajů, jak jsou připomenuty v bodech 49 a 55 až 59 tohoto rozsudku, nemůže mít kontext, v němž tento subjekt žádá o přístup k informacím uvedeným v čl. 15 odst. 1 GDPR, žádný vliv na rozsah tohoto práva. [88]

Proto musí být čl. 15 odst. 1 GDPR vykládán v tom smyslu, že okolnost, že správce vykonává bankovní činnost v rámci regulované činnosti a osoba, jejíž osobní údaje byly zpracovány jakožto klienta správce, byla rovněž zaměstnancem tohoto správce, nemá v zásadě vliv na rozsah práva, které má tato osoba na základě tohoto ustanovení. [89]

Konečné rozhodnutí o předběžné otázce

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

1) Článek 15 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) musí být ve světle čl. 99 odst. 2 tohoto nařízení vykládán v tom smyslu, že se použije na žádost o přístup k informacím uvedeným v tomto ustanovení, pokud operace zpracování týkající se této žádosti byly provedeny přede dnem, kdy se uvedené nařízení stalo použitelným, ale žádost byla podána po tomto datu.
2) Článek 15 odst. 1 nařízení 2016/679 musí být vykládán v tom smyslu, že informace o operacích nahlížení do osobních údajů subjektu, které se týkají dat a účelů těchto operací, jsou informacemi, které má tento subjekt právo získat od správce podle tohoto ustanovení. Uvedené ustanovení naproti tomu takové právo nezakotvuje, pokud jde o informace o totožnosti zaměstnanců uvedeného správce, kteří prováděli tyto operace z jeho pověření a v souladu s jeho pokyny, ledaže jsou tyto informace nezbytné k tomu, aby subjekt údajů mohl účinně vykonávat práva, která mu toto nařízení přiznává, a za podmínky, že jsou zohledněna práva a svobody těchto zaměstnanců.
3) Článek 15 odst. 1 nařízení 2016/679 musí být vykládán v tom smyslu, že okolnost, že správce vykonává bankovní činnost v rámci regulované činnosti a osoba, jejíž osobní údaje byly zpracovány jakožto klienta správce, byla rovněž zaměstnancem tohoto správce, nemá v zásadě vliv na rozsah práva, které má tato osoba na základě tohoto ustanovení.

Zpracovala Eva Janečková

Ochrana osobních údajů a kybernetická bezpečnost patří k sobě – GDPR a DORA

Požadavky evropského nařízení o digitální provozní odolnosti finančního sektoru (DORA), které nově upravuje oblast kybernetické bezpečnosti tohoto sektoru, přiblížil v minulém čísle časopisu DPO PRO článek s názvem „Je nové evropské nařízení DORA spíše Pandorou? A co přináší?". Jelikož finanční instituce disponují velkým množstvím osobních údajů, častokrát i citlivého charakteru, jsou přirozeným cílem kybernetických útoků. Nová úprava zohledňující specifika finančního sektoru je také reakcí na kontinuální modernizaci. Finanční sektor nejenže se digitalizoval jako celek, ale v důsledku digitalizace se rovněž prohloubila jeho vzájemná propojení a závislosti a také propojení a závislosti mezi ním a poskytovateli infrastruktury a služeb z řad třetích stran.

Nové kyberbezpečnostní požadavky je tedy potřeba reflektovat nikoli izolovaně, ale v souvislostech s již existujícím nebo připravovaným legislativním rámcem.

Právě proto je jedním z klíčových předpisů, které je potřeba vnímat optikou kybernetické bezpečnosti vzhledem k faktickému nárůstu kybernetických hrozeb – na což ostatně reaguje i vývoj legislativní úpravy, rozhodně i rámec ochrany osobních údajů v minimální rovině zakotven v GDPR.

Cílem DORA není v přímočaré rovině úprava osobních údajů

Dle mého názoru je však z faktického hlediska podmínka nejvyššího možného zajištění kybernetické bezpečnosti fundamentálním předpokladem ke splnění podmínek pro vytvoření prostředí, v jehož rámci lze GDPR následně aplikovat. To ostatně deklarovala i Evropská komise již ve Zprávě o hodnocení a přezkumu GDPR z roku 2020 [1].

Dalo by se tedy říct, že DORA je ve srovnání s GDPR obecnější. Koncept kybernetické bezpečnosti počítá se zajištěním ochrany všech dat, tedy nejenom osobních údajů. Rámec DORA proto optikou ochrany osobních údajů vnímám jako určitou nadstavbu GDPR. K požadavkům na ochranu osobních údajů jako takovým, vymezeným v GDPR, je tak ze strany finančních subjektů potřeba přidat i techničtější rovinu jejich zabezpečení, kterou zakotvuje právě principiálně orientované nařízení DORA. Jedná se tedy o souběžné, vzájemně související úpravy, kdy je finanční instituce povinna nařízení DORA implementovat a z pohledu GDPR specificky posoudit, zda je dostatečně dodržena rovina ochrany osobních údajů cenných jak pro subjekty osobních údajů, tak pro finanční instituce.

DORA se v rámci finančního sektoru zabývá ochranou dat před kybernetickými hrozbami

GDPR je specifičtější – zakotvuje standardy pro ochranu osobních údajů a bezpečnostními hledisky se po technické stránce nezaobírá. V podstatě je koncept kybernetické bezpečnosti jako doplnění GDPR v zásadě o integraci a rozšíření GDPR s důrazem na bezpečnostní aspekty. Zatímco GDPR se zaměřuje na ochranu osobních údajů, DORA se v rámci finančního sektoru zabývá ochranou těchto dat před kybernetickými hrozbami.

V praktické úrovni to může znamenat implementaci pokročilých bezpečnostních opatření, jako jsou firewall, šifrování, antivirové programy a systémy pro detekci a prevenci narušení. To také zahrnuje vytváření bezpečnostních politik a postupů, které se zaměřují na ochranu dat a systémů, a školení zaměstnanců v oblasti bezpečnostních nejlepších postupů.

Zatímco GDPR může vyžadovat, aby organizace měla určitá bezpečnostní opatření na místě, kybernetická bezpečnost jako nadstavba by šla dále a zdůrazňovala neustálou ochranu a obranu proti novým a vznikajícím hrozbám.

Kybernetická bezpečnost a GDPR jsou těsně propojeny

Je důležité si uvědomit, že kybernetická bezpečnost a GDPR jsou těsně propojeny. Nedostatečná kybernetická bezpečnost – nesplnění standardů DORA, může vést k úniku dat, k nimž počítáme i osobní údaje, což by bylo porušením GDPR. Proto je důležité, aby organizace považovaly kybernetickou bezpečnost a GDPR za integrální součást svých celkových strategií ochrany dat.

Konkrétně spatřuji přesahy DORA a GDPR v několik rovinách, kterým se budu níže postupně věnovat.

Technická a organizační opatření a DPIA

Zaprvé se jedná o vhodná technické a organizační opatření, v GDPR rámcově specifikovaná článkem 32. Může se jednat např. o pravidelné testování, postupy pro důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování, pseudonymizaci, anonymizaci, šifrování apod. Zde nacházíme řadu požadavků, které musí organizace implementovat, aby chránily osobní údaje a zajišťovaly jejich náležitou správu a zpracování.

Z důvodu technologické neutrality a pro *futuro* aplikovatelnosti GDPR neobsahuje konkrétní seznam technických a organizačních opatření (obdobně jako DORA), která organizace musí přijmout, ale spíše hlavní principy a požadavky, které je následně potřeba zohlednit v posouzení vlivu na ochranu osobních údajů (DPIA). Především se jedná o proporcionalitu (vzhledem k velikosti a rizikovosti subjektu) a plnou odpovědnost finančního subjektu např. v oblastech:

- Zabezpečení osobních údajů: Organizace musí zabezpečit osobní údaje proti neoprávněnému nebo nezákonnému zpracování a proti náhodné ztrátě, zničení nebo poškození, a to pomocí vhodných technických nebo organizačních opatření.
- Princip minimalizace dat: Organizace by měly zpracovávat pouze osobní údaje, které jsou nezbytné pro konkrétní účel, a měly by je uchovávat pouze po nezbytně nutnou dobu.

1) Hodnotící zpráva EK o provádění obecného nařízení a o ochraně osobních údajů dva roky od začátku jeho uplatňování. Usnesení EP ze dne 25. 3. 2021, o hodnotící zprávě EK, o provádění obecného nařízení, o ochraně osobních údajů dva roky od začátku jeho uplatňování (2020/2717(RSP)) [online]. In: Úřední věstník [online], C 494/11, 25. 3. 2021 [cit. 21. 8. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52021IP0111&from=EN

- Povinnost informovat: Organizace musí informovat subjekty údajů o tom, jaké osobní údaje o nich shromažďují a jak je používají.
- Právo na přístup a opravu: Subjekty údajů mají právo požádat o přístup ke svým údajům, požádat o opravu nesprávných údajů a v některých případech požádat o výmaz údajů.
- Nápravná opatření: Pokud dojde k porušení ochrany dat, organizace musí podniknout kroky k nápravě a musí informovat jak subjekty údajů, tak dozorový orgán.

DORA je tedy potřeba implementovat tak, aby byla podpořena technická a organizační opatření dle GDPR a posílena kybernetická bezpečnost daného subjektu. U GDPR DPIA je tedy nutné zohlednit dostatečnou ochranu kybernetické bezpečnosti, třeba v oblastech jako ICT rizikový management, řízení, politiky, strategie, klasifikace a hlášení incidentů souvisejících s ICT, testování vč. penetračního, vztah ke třetím stranám, edukace zaměstnanců apod.

Dohled a ohlašování

Co se týče dohledu, v kontextu GDPR je dohledovým orgánem Úřad pro ochranu osobních údajů (ÚOOÚ). Legislativní úprava dohledu v rámci DORA je o něco komplikovanější, neobvykle totiž rozlišuje mezi dohledem nad finanční institucí a dohledem nad poskytovateli ICT služeb v postavení třetích stran. Důvodům, které evropského zákonodárce vedly k vymezení tohoto přístupu a kritérií pro určování těchto subjektů, jsem se věnovala v předchozím článku. V obou případech je však dohledovým orgánem Česká národní banka (ČNB), která ale při řešení kybernetických incidentů bude spolupracovat s Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB).

Optikou vztahu GDPR a DORA jsou však zajímavé potenciální přesahy v ohlašování kybernetických incidentů, u kterých došlo (rovněž) k porušení zabezpečení, jež vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně, neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených či jinak zpracovávaných osobních údajů. Postup ohlašování dle článku 33 a následujících GDPR je už i díky pokynům EDPB a praxi jasný. Máme k dispozici standardizovanou šablonu i časový rámec pro ohlašování.

Samotné nařízení DORA však tyto podstatné aspekty nedefinuje. Budou specifikovány až následně v regulatorních technických standardech (RTS) evropských orgánů dohledu (ESAs), jejichž publikaci lze očekávat příští rok. Ohlašované však mají být jediná událost nebo řada propojených událostí, které finanční subjekt neplánoval a které ohrožují bezpečnost sítí a informačních systémů a mají nepříznivý dopad na dostupnost, hodnověrnost, integritu nebo důvěrnost údajů nebo na služby, které finanční subjekt poskytuje. Dále DORA klasifikuje incidenty do dvou kategorií dle míry závažnosti na základě např. toho, jak zásadní jsou ohrožené služby, včetně transakcí a operací finančních subjektů, jaký je počet nebo význam klientů nebo finančních protistran a územní rozsah ohrožených oblastí.

Evropský zákonodárce v preambuli DORA vyjádřil rovněž snahu o prevenci duplicitních povinností – a tedy případů, kdy by se kybernetický incident s dopadem do integrity osobních údajů musel odděleně ohlašovat jak ÚOOÚ, tak ČNB (která to následně sdílí s NÚKIB), popř. je-li povinný subjekt regulován i NIS2, tak opětovně i NÚKIB. Cílem by tak měl být jednotný, zjednodušený rámec ohlašování. Zda se toho však povedlo dosáhnout, můžeme hodnotit nejdříve příští rok, resp. i o něco později, jelikož na evropské úrovni není vyloučená evropská centralizace hlášených incidentů u ESAs. V neposlední řadě se může jednat o vhodný nástroj pro studium a prevenci rapidně stoupajících kybernetických rizik s možným negativním dopadem na osobní údaje. Sjednocená evidence kybernetických událostí má nepochybné výhody, ještě znatelnější v případě přítomnosti osobních údajů.

Ohlašovací povinnosti je třeba nastavit efektivně

Suma sumárum, ohlašovací povinnosti v těchto režimech (GDPR, DORA, NIS2) a vůči různým autoritám je třeba nastavit efektivně, aby nedocházelo ke zbytečné administrativní zátěži povinných subjektů i dohledových orgánů. Ideální by byla jednotná, strukturovaná, anonymizovaná podoba za zachování granularity. GDPR sice reguluje incidenty, které mohou přinést negativní konsekvence vůči právům subjektů osobních údajů, kybernetické hrozby jsou však mnohem širší a dopad může být i nepřímý. Proto považuji za nezbytnou spolupráci napříč odvětvími na národní i evropské úrovni. Významnou roli v této věci může sehrávat ENISA a načrtnutý rámec dobrovolného sdílení informací o operativních a kybernetických hrozbách mezi finančními institucemi dle DORA. Komplikací však může být nejednotná taxonomie vedoucí ke komparačním a statistickým potížím.

Ostatně toho jsou si vědomy i evropské orgány, které např. do DORA zakomponovaly prozatím možnost, nikoli povinnost, dobrovolného sdílení informací o operativních a kybernetických hrozbách mezi finančními institucemi, kdy je možné také stanovit podmínky účasti a případně podrobnosti o zapojení veřejných orgánů a poskytovatelů ICT služeb v postavení třetích stran. DORA však vymezuje podmínky. Finanční subjekty si mohou mezi sebou vyměňovat operativní a jiné informace o kybernetických hrozbách, včetně ukazatelů narušení, taktiky, technik a postupů, výstrah v oblasti kybernetické bezpečnosti a konfiguračních nástrojů, pokud se toto sdílení operativních a jiných informací:

a) zaměřuje na zlepšení digitální provozní odolnosti finančních subjektů, zejména zvyšováním povědomí o kybernetických hrozbách, omezením nebo zabráněním možností šíření těchto hrozeb podporou obranných schopností, techniky detekce hrozeb, zmírňující strategie nebo fáze reakce a obnovy;
b) odehrává v důvěryhodných komunitách finančních subjektů;
c) provádí prostřednictvím ujednání o sdílení informací chránících potenciálně citlivou povahu sdílených informací, která se řídí pravidly chování plně respektujícími důvěrnou povahu obchodních informací, GDPR a dodržování pokynů týkajících se hospodářské soutěže.

Outsourcing

Co se týká outsourcingu, EDPS ve svém názoru k DORA [2] již v roce 2021 varoval před zvýšenou koncentrací rizik i pro ochranu osobních údajů plynoucích z outsourcingu a upozornil na důležitost zpracování osobních údajů na právních základech dle článku 6 GDPR a jasné vymezení rolí a povinností správců a zpracovatelů. Jako základní předpoklad kybernetické ochrany osobních údajů stanovil také zakotvení vhodných technických a organizačních opatření, DPIA a systému ohlašování porušení.

Zvýšenou koncentraci rizik EDPS indikoval především u přeshraničního zpracování. Proto je nutné nezapomínat na kapitolu 5 GDPR a Schrems II.

DORA zavádí minimální standardy aplikovatelné pro tuto oblast:

- Finanční subjekty řídí riziko v oblasti ICT spojené s poskytovateli služeb v postavení třetích stran jako nedílnou součást rizika v oblasti ICT ve svém rámci (článek 6 odst. 1) podle zásad plné odpovědnosti a proporcionality.
- Přijmou a pravidelně přezkoumávají strategii pro riziko (zásady využívání služeb ICT podporujících zásadní nebo důležité funkce).
- Smluvní ujednání se řádně zdokumentují, rozlišuje se 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 aktuální stav.
- Finanční subjekty smí uzavírat smluvní ujednání pouze s poskytovateli služeb v posta-

2) EDPS. *Opinion 7/2021 on the Proposal for a Regulation on digital operational resilience for the financial sector and amending Regulations (EC) 1060/2009, (EU) 648/2012, (EU) 600/2014 and (EU) 909/2014* [online]. Brussels: EDPS, 10. 5. 2021 [cit. 21. 8. 2023]. Dostupné z: https://edps.europa.eu/system/files/2021-05/2021-0203_d0943_opinion_digital_operational_resilience_for_the_financial_sector_en.pdf.

vení třetích stran, kteří splňují příslušné normy v oblasti bezpečnosti informací, přičemž DORA specifikuje formu i obsah smluv.

- Velmi podstatné je i zavedení podmínek tzv. exit strategie, a tedy ukončení smluvního vztahu. To je v praxi z důvodu asymetrického charakteru smluvních ujednání problematické. Na hledisko asymetrie smluvních vztahů mezi technologickými giganty a spotřebiteli či jinými podnikatelskými subjekty upozorňuje také Zuboff [3]. Ta varuje před negativními konsekvencemi adhezních smluv, kdy v rámci přístupu „take it or leave it" nemá subjekt v postavení slabší smluvní strany reálnou možnost ovlivnit obsah smluvních podmínek. To je častokrát způsobeno patovou situací, kdy omezený počet poskytovatelů služeb v postavení třetích stran na trhu v podstatě jednostranně určuje předem standardizované podmínky poskytování služeb.
  DORA vymezuje relevantní důvody, jako např. situace, kdy poskytovatel ICT služeb v postavení třetí strany zásadním způsobem poruší platné právní předpisy nebo smluvní podmínky;
  sledováním rizika v oblasti se zjistí okolnosti, u nichž se má za to, že mohou změnit plnění funkcí poskytovaných prostřednictvím smluvního ujednání, včetně podstatných změn ovlivňujících dané ujednání nebo situaci; anebo v rámci celkového řízení rizika jsou 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.

Závěr

I když DORA a GDPR mají některé podobné cíle, jako je ochrana dat včetně osobních údajů a zajištění kybernetické bezpečnosti, zaměřují se tyto legislativní předpisy na různé aspekty související problematiky.

Koncept kybernetické bezpečnosti, pro finanční sektor specificky DORA, jako nadstavby GDPR je v zásadě o integraci a rozšíření GDPR s důrazem na bezpečnostní aspekty. Zatímco GDPR se zaměřuje na ochranu osobních údajů, kybernetická bezpečnost jako nadstavba se zabývá ochranou těchto dat před kybernetickými hrozbami.

Kybernetická bezpečnost a GDPR jsou v dnešním datacentrickém světě těsně propojeny. Nedostatečná úroveň kybernetické bezpečnosti může vést k úniku dat, osobní údaje nevyjímajíc, což by bylo porušením GDPR. Proto je důležité, aby organizace považovaly kybernetickou bezpečnost a GDPR za integrální součást svých celkových strategií ochrany dat.

Na GDPR by mělo být pohlíženo jako na mantinel, na navazující úpravy pak jako na nadstavbu, přičemž společně se jedná o kompatibilní, rovnovážnou úpravu zakotvující právní jistotu pro všechny zúčastněné subjekty, formulující podmínky pro další růst, a především vytvářející ekvilibrium pro subjekty osobních údajů. Význam DORA v této oblasti ostatně reflektoval i EDPS v názoru zmíněném výše.

Oba předpisy byly přijaty ve znění, které není zbytečně preskriptivní, ale spíše principálně orientované, aby obstálo v dynamickém vývoji i z dlouhodobého hlediska. U obou předpisů byla zvolena forma nařízení s cílem unifikované aplikace napříč EU a u obou předpisů měl evropský zákonodárce na mysli dosažení tzv. bruselského efektu, a tedy aby byl daný předpis inspirací i pro právní řády mimo EU. Což by pochopitelně zlepšilo i spolupráci se subjekty z EU. Vidíme, že u GDPR je to úspěšné, neboť již dnes slouží jako globální vzor. Snad tomu tak bude stejně i u DORA.

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

3) ZUBOFF, Shoshana. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. London: Profile Books, 2019, s. 236–237. ISBN 978-1-78125-685-5.

Sdílení dat ve zdravotnictví pohledem pacienta a právní úpravy

Doba jde kupředu. Ba ne, spíše letí. Tryskem. Vše se zrychluje a do popředí se hrne „uživatelská přívětivost" klienta. Bude se to zdát zvláštní, ale je tomu tak i ve zdravotnictví. Obor, mnohými považován za konzervativní, zažívá za poslední roky digitální rozmach. Smutnou pravdou je, že hybným faktorem jsou kybernetické útoky, jimž nemocnice čelí. Pozitivem je, že nemocnice dokázaly tuto vpravdě negativní zkušenost chytře využít k modernizaci svých služeb. Jedním z takových kroků je budování propojených nemocničních informačních systémů (zkr. „NIS"). Služba, která znamená lepší uživatelský zážitek jak na straně pacienta, tak na straně zdravotnických pracovníků. Ale nepředstavuje to problém z hlediska ochrany osobních údajů?

Popis problému

V úvodu jsem uvedl, že propojené NIS pocítí jak pacient, tak i zdravotnický personál. Zaměříme se nyní čistě na pohled pacienta. Dopady pro zdravotnický personál si necháme třeba na jindy. A nyní se už podívejme na reálný případ.

Pacient je dlouhodobě léčen s diagnózou, pro kterou navštěvuje nemocnici „A". Souhrou okolností je nucen ve stejném kraji navštívit nemocnici „B", kde se bude řešit jiný úkon. Pro personál v nemocnici B jsou však zásadní poznatky ze zdravotnické dokumentace provedené nemocnicí A (např. rentgenové snímky plic). Protože zřizovatel nemocnic A a B byl prozíravý, vytvořil pro všechny jím zřizované nemocnice propojený NIS. V nemocnici B tak mají okamžitě přístup ke zdravotnické doku-

mentaci, která byla vedena v nemocnici A. Technicky je to zajištěno tak, že zdravotnická dokumentace je vedena v horní vrstvě počítačového clusteru, kam si každá nemocnice v případě nutnosti ošetření pacienta může „sáhnout“ a získat zde potřebné informace. Tyto pak může doplnit o své úkony. To za podmínky, že některá z nemocnic napojených na NIS pacientovi v minulosti poskytla zdravotní služby. Celou infrastrukturu pak zaštiťuje zřizovatel, který výsledný projekt financoval. Protože však nemá dostatek odborného personálu, fakticky infrastrukturu spravuje a provozuje technologická společnost, která se specializuje na vývoj moderního NISu.

Zasvěcení vědí, že z pohledu Obecného nařízení o ochraně osobních údajů (GDPR) řešíme základní role, od nichž se pak jednotlivým aktérům odvíjí práva a povinnosti. Máme tedy: správce údajů, zpracovatele, někdy i příjemce, a poté subjekt údajů. Patrně už tušíte, kam míříme, ale nebudu vás napínat.

Kdo je v tomto případě správce? A je pouze jeden? Je zde nějaký zpracovatel? Kdo jím bude? A je toliko jeden? A co případy, kdy se do NISu napojují další technologické společnosti se svými produkty. Dnes už není raritou, že NIS tvoří pouze horní vrstvu informací, která „jen“ sbírá různá data z dalších aplikací, nasazených v nemocnici.

Pověřencům v tuto chvíli patrně vstávají vlasy hrůzou. Ale není třeba se obávat.

Pohledem právní úpravy

Základním kamenem úspěchu je detailní schéma všech subjektů (nikoli ve smyslu subjektů osobních údajů), zapojených do procesu zpracování osobních údajů. Podle tohoto můžeme následně přiřadit jednotlivým aktérům odpovídající role. V návaznosti na to určíme jejich povinnosti podle GDPR.

Nejprve je třeba vyhodnotit, kdo bude správcem údajů.

Jako první se nabízí varianta, aby správcem byla vždy samostatně jednotlivá nemocnice. Prozradím vám, že v reálném případě (jenž mne inspiroval k sepsání příspěvku), se právě takto nemocnice ke zpracování údajů postavily. A já se domnívám, že je to špatně.

Běžné poskytování zdravotních služeb je z pohledu soukromého práva prováděno na základě smlouvy o péči o zdraví – uzavřené nejčastěji v ústní podobě. Z pohledu GDPR pak bývá takové zpracování prováděno na základě čl. 9 odst. 2 písm. h) GDPR.

Podíváme-li se na celou strukturu zpracování údajů, pak vidíme, že kromě *základního* účelu zpracování (běžné poskytování zdravotních služeb) je nad tím ještě jakýsi *nadstavbový* účel. A tím je sdílení těchto dat mezi nemocnicemi, aby mohly při vzájemné součinnosti poskytovat komfortněji své služby. A zde je potřeba se zastavit.

Jsem přesvědčen, že v celém procesu zpracování jde o zásadní faktor, který nemocnice jednak posouvá do postavení tzv. společných správců podle čl. 26 GDPR, ale také toto sdílení přesahuje původní účel zpracování a nemocnice pro něj musí najít odpovídající právní základ. Jak s tím naložit?

Je třeba uzavřít smlouvu o společném správcovství a především – informovat o všem pacienty. Protože subjekt údajů by v tomto případě měl být informován o tom, že jeho zdravotnická dokumentace je uchovávána v clusteru, k němuž mají přístup i jiné nemocnice. Nemocnice se totiž v konečném důsledku vzájemně podílí na tvorbě zdravotnické dokumentace, čímž vytváří rámec zpracování osobních údajů, jež také společně využívají. A zde se vracím k právnímu základu pro zpracování. Domnívám se, že pro takové sdílení údajů si již nelze vystačit s právním základem v podobě čl. 9 odst. 2 písm. h) GDPR, ale k onomu nadstavbovému sdílení by měl být dán souhlas ze strany subjektu údajů. To pochopitelně nemusí platit tam, kde nastane neodkladná potřeba sídlení zdravotních údajů s poskytovatelem zdravotních služeb, jenž pacientovi může poskytnout odpovídající a lepší péči, nota bene za situace, kdy ani pacient není schopen kvůli svému zdravotnímu stavu jakkoli právně jednat. Takové předání či sdílení údajů může být v nezbytném rozsahu založeno na základě čl. 9 odst. 2 písm. c) GDPR – pochopitelně jen za účelem provedení neodkladné zdravotní péče.

Teď vyřešme otázku postavení zřizovatele nemocnic (u soukromých nemocnic vlastník).

Na první pohled by se mohlo zdát, že mu také přiřadíme roli (společného) správce. Protože určil prostředky zpracování – rozhodl a zafinancoval IT infrastrukturu a k tomu zjevně stál na počátku rozhodnutí o propojení dat. I přesto bych zřizovatele / vlastníka nemocnic považoval spíše za zpracovatele. Jeho rolí v rámci struktury zpracování je ve výsledku „pouze“ poskytnutí technologické části. Bez toho, aniž by měl jakýkoli další vliv na podobu zpracování osobních údajů: neurčuje rozsah, dobu, ani jiné účely zpracování. Na samotném zpracování se nikterak dále aktivně nepodílí. Zjednodušeně řečeno: zřizovatel nevykonává nad osobními údaji takový *controlling*, abych ho označil za dalšího správce. Tím, kdo řídí a kontroluje osobní údaje, jsou ve vzájemné kooperaci nemocnice.

Přesto si dovedu představit situace, v nichž zřizovatel překročí rámec své působnosti a skrze svůj vliv na nemocnice bude zasahovat do zpracovatelských procesů způsobem, že jej budeme považovat za dalšího správce. Což mu ve výsledku přinese vyšší míru odpovědnosti za řádné zpracování osobních údajů. Na opačné straně pólu pak mohou být případy, kdy zřizovatel celému projektu poskytne „pouze“ finanční prostředky nemocnicím a finální smluvní vztahy celého IT řešení leží mezi nemocnicemi a IT dodavatelem. V takovém případě bych zřizovateli nepřiřadil ani zpracovatelskou roli.

Je tedy zřejmé, že určení rolí při zpracování osobních údajů není jednoznačně dogmatické. Naopak. Hranice mezi tím, kdy bude aktér správcem, zpracovatelem, nebo bude zcela stranou, není jednoznačnou a neprostupnou zdí. Je to spíše jemná síť, kterou mohou jednotliví aktéři v průběhu času prostupovat, v závislosti na charakteru daného zpracování a jejich zapojení v něm. Bystrý pověřenec by v takovém případě měl být ve střehu a průběžně analyzovat, zda jednotliví aktéři setrvávají na svém místě nebo zda se svou činností již nevychýlili k jiné roli. A nejinak je tomu u poskytovatelů IT řešení.

Řešený případ jsem záměrně v úvodu popsal tak, aby bylo zřejmé, že poskytovatel IT řešení bude zpracovatelem osobních údajů. Nicméně v duchu předchozího odstavce i tento závěr může být měněn. Opět bude záležet na charakteru služby, jenž bude technologická společnost dodávat – klíčovým prvkem bude vlastnictví serverů, na nichž se data nacházejí, a pak také charakter činnosti, kterou bude technologická společnost pro nemocnice provádět.

Práce pověřence v takovém případě nekončí. Měl by se hlouběji ponořit do rozboru architektury IT řešení a vyžádat si detailní informace. Dnes již není nic neobvyklého, že IT dodavatelé v rámci nabízeného řešení využívají další subdodavatele, kteří jim poskytují serverovou kapacitu k ukládání / zálohování dat. Jde o tzv. řetězení zpracovatelů.

Máme-li přiřazeny základní role při zpracování osobních údajů, nebrání nám už nic k tomu, abychom subjektům údajů poskytli transparentní a pravdivé informace o zacházení s osobními údaji. A sem celou dobu směřuji.

Závěr

Pokud jsem se ptal v úvodu, zda popsané zpracování představuje problém z hlediska ochrany osobních údajů, pak odpověď je: nikoli. Propojené NIS nejsou z pohledu GDPR apriori zakázané nebo zásadně problematické.

Problematickými se tyto komplexní zpracovatelské procesy stávají v momentě, kdy jednotliví aktéři nesprávně posoudí své role při zapojení do zpracování osobních údajů nebo nedokáží adekvátně vyhodnotit odpovídající právní základ pro dané zpracování. V takovém případě pak pacient nejenže dostává neúplné informace o tom, co se s jeho osobními údaji děje (neví, že k osobním údajům může přistupovat více poskytovatelů zdravotních služeb), ale je mu také eventuálně znemožněno řádně uplatnit své nároky vůči všem odpovědným správcům.

A takových situací by se měl férový správce údajů vyvarovat.

Ondřej Fiala
Autor je advokát v advokátní kanceláři Specialis, s. r. o.

Francouzský dozorový úřad radí náborářům

Francouzský dozorový úřad (Commission Nationale de l'Informatique et des Libertés, dále CNIL) vydal letos 30. ledna návod pro náboráře a personalisty zaměřený na standardy ochrany osobních údajů v souvislosti s výběrem a najímáním nových zaměstnanců. [1)]

Při náborech dochází ke zpracování velkého množství údajů více osob

Nábor zaměstnanců je proces, při kterém dochází ke zpracování velkého množství údajů více osob. Nepřekvapí proto, že se tímto tématem CNIL zabýval už dříve, konkrétně v roce 2002.[2)] Technologický posun a další změny v následujících 20 letech vedly k silnému zájmu odborné veřejnosti o nová vodítka k ochraně osobních údajů. Není snad ani třeba připomínat změnu právního prostředí díky nové evropské úpravě. Nové technologie přinesly nové možnosti náboru např. prostřednictvím sociálních sítí, personalizované reklamy a specializovaných vyhledávacích programů. Běžně se využívají nové formy komunikace. Kromě videokonferenčních hovorů jde o chatboty, různé mobilní aplikace a další nástroje. Mnohem snáze lze vytvořit velkou databázi údajů. Tu pak může zpracovat umělá inteligence nebo jiný nástroj, který na základě dostupných informací vyhodnotí „umění žít" či tzv. měkké dovednosti kandidátů. Všechny tyto nové prvky s sebou nesou rizika narušení soukromí uchazečů o práci.

Příručka CNIL se zaměřila na všechny fáze náboru

Příručka je rozdělena na dvě poloviny. První připomíná základy právní úpravy ochrany osobních údajů. Druhá polovina potom metodou otázek a odpovědí poskytuje návody v konkrétních situacích, zejména když se během náborového procesu využívají nové technologie.

První část se věnuje samotnému obsahu pojmu zpracování osobních údajů a základním variantám uspořádání vztahů a odpovědností při náboru (přímý kontakt mezi společností a uchazečem, nábor prostřednictvím inzerce, nábor prostřednictvím třetí osoby, např. pracovní agentury), otázce stanovení legitimního účelu zpracování, rozsahu osobních údajů, které lze zpracovávat (CNIL opakovaně zdůrazňuje zásadu minimalizace údajů), nebo otázce, kdo může mít k těmto údajům přístup. Příručka připomíná i základní práva uchazečů ve vztahu k jejich osobním údajům.

Druhá část se soustředí na konkrétní aspekty náboru a podává návod, na co se soustředit, případně čeho se vyvarovat. Právní rámec přitom netvoří pouze Obecné nařízení o ochraně osobních údajů (GDPR), ale také francouzský

zákoník práce. V něm je velmi podstatné, že umožňuje pouze dva možné cíle zpracování osobních údajů uchazeče ze strany zaměstnavatele, a to vyhodnocení schopnosti uchazeče vykonávat práci na pozici, o kterou se uchází, a zhodnocení jeho odborných schopností.[3)] Francouzský pracovněprávní předpis tak přistupuje k ochraně osobních údajů odlišně než česká právní úprava, která spočívá především ve výčtu informací, jež zaměstnavatel nesmí vyžadovat.[4)] V tomto považuji francouzskou úpravu za explicitnější a zároveň obecněji platnou, než je česká úprava. „Nesmí vyžadovat" alespoň gramaticky nepokrývá situace, kdy si zaměstnavatel opatřuje informace o uchazeči vlastními silami. Ustanovení francouzského zákoníku práce o souvislosti s pracovní pozicí, na kterou se uchazeč přihlásil, se uplatňuje průřezově na jakékoliv zpracování. Jím je třeba poměřovat i opatřování informací na internetu a z profilů uchazeče na sociálních sítích, nebo i případné požadavky na informaci o tom, zda a jaké má uchazeč záznamy v rejstříku trestů. Informace o trestu za způsobení dopravní nehody není relevantní u pozic, v jejichž náplni práce nefiguruje řízení motorových vozidel. Francouzské právo tak případný požadavek bezúhonnosti striktně omezuje na netrestání v oblastech, které souvisí s vykonávanou prací.[5)]

Uchazeč musí být předem informován o všech postupech a metodách

Francouzský zákoník práce navíc požaduje, aby byl uchazeč předem výslovně informován o postupech a metodách, kterými si zaměstnavatel při náboru vypomůže. Bez toho, aby o tom uchazeč předem věděl, se nesmí získávat žádné údaje, které se jej osobně týkají.

Základním právním základem zpracování osobních údajů při náboru je souhlas subjektu údajů (uchazeče) se zpracováním. Zde CNIL upozorňuje na to, že by náborový proces měl být nastaven tak, aby případné neudělení souhlasu se zpracováním nemělo vliv na šanci obsadit volnou pozici. Souhlas udělený v situaci, kdy jím je podmíněn např. postup do dalšího kola výběrového řízení, nelze považovat za svobodný. Provedení testu či zkoušek, které mají vliv na rozhodnutí o přijetí, by proto v žádném případě nemělo být podmíněno udělením souhlasu se zpracováním osobních údajů (tj. mělo by být postaveno na jiném právním základě).

Při výběru se uplatní účel oprávněného zájmu zpracovatele

U výběru uchazečů se kromě souhlasu ponejvíce uplatní účel oprávněného zájmu zpracovatele. Francouzský dozorový úřad ale v této souvislosti opakovaně upozorňuje na obecné omezení zpracování takovým způsobem, aby nezasáhlo do základních práv a svobod uchazeče. Typickým překročením této hranice je zpracování údajů, na jehož základě dojde k diskriminaci uchazeče. Vyšší riziko se pojí zejména se zpracováním osobních údajů získaných díky novým technologiím, například prostřednictvím sociálních sítí, nebo také pořízením videozáznamu pohovoru.

Jiná situace nastává při uzavření pracovní smlouvy, kde se z velké části zpracování zakládá na splnění právní povinnosti.

1) https://www.cnil.fr/sites/default/files/atoms/files/guide_-_recrutement.pdf (přístup 1. 5. 2023).
2) https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000017653561/ (přístup 1. 5. 2023).
3) Ustanovení L.1221-6 až L.1221-9 francouzského zákoníku práce, text ustanovení dostupný zde: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072050/LEGISCTA000006177850/#LEGISCTA000006177850 (přístup 3. 9. 2023).
4) V ČR jde zejm. o ustanovení § 316 zákoníku práce (zákon č. 262/2006 Sb.), popř. také § 12 odst. 2 zákona o zaměstnanosti (zákon č. 435/2004 Sb.).
5) Již za tehdejší české právní úpravy v roce 2011 k podobným závěrům dospěl Veřejný ochránce práv ve svém stanovisku, zveřejněném zde: https://www.ochrance.cz/uploads-import/ESO/30-2010-DIS-LO-doporu%C4%8Den%C3%AD.pdf (přístup 5. 9. 2023).

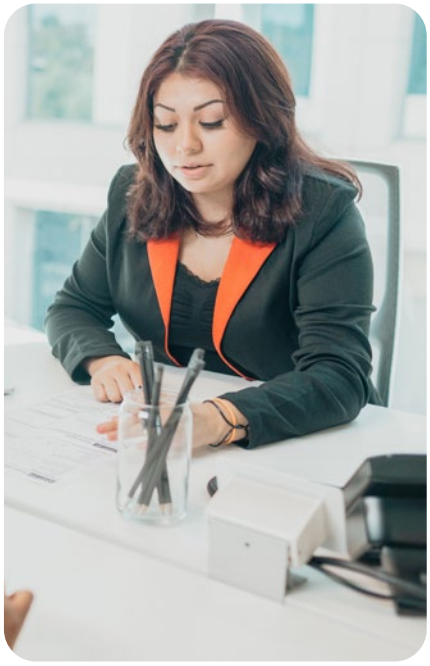
Délka uchovávání osobních údajů

Co se týče délky uchovávání osobních údajů, příručka uvádí tři etapy. První je výběr uchazeče, po němž by měla být většina údajů o neúspěšných uchazečích vymazána. Druhá je dána lhůtami, po které je legitimní některé údaje i o neúspěšných uchazečích uchovávat z důvodu možného sporu, například pro případ, že některý z odmítnutých uchazečů napadne výsledek výběrového řízení kvůli možné diskriminaci své osoby.[6] A třetí se vztahuje k tomu, že si zaměstnavatel pro případ uvolnění další pracovní pozice ponechá údaje neúspěšného uchazeče, aby mu tuto mohl nabídnout. V tomto posledním případě CNIL dovozuje, že údaje by měly být uchovávány se souhlasem uchazeče, a to po dobu nejdéle dvou let. Prodloužení této doby je možné se souhlasem uchazeče.

Analýza dopadů zpracování v některých situacích

Za velmi užitečné považuji upozornění náborářů na požadavek provádění analýzy dopadů zpracování v některých situacích. Tu CNIL považuje za povinnou u zpracování, u kterých je vysoká pravděpodobnost dopadů na práva a svobody subjektů údajů. V oblasti náboru toto naplňuje například selekce uchazečů prostřednictvím algoritmu, například při analýze videozáznamu pohovoru s cílem posoudit i osobnost uchazeče (neverbální projevy, emoce atd.). Ostatně na posuzování povahových rysů uchazečů se zaměřuje jedna z kapitol příručky. K povinnosti provést analýzu dopadů stačí, aby zpracování splnilo alespoň dvě z devíti kritérií ve výčtu zveřejněném ve směrnici Pracovní skupiny č. 20 z roku 2017[7]:

- hodnocení nebo bodování osoby, včetně profilování a předpovídání,
- automatizované rozhodování, které má právní nebo podobně závažný dopad,
- systematické monitorování,
- zpracování citlivých údajů nebo údajů vysoce osobní povahy (zvláštní kategorie osobních údajů),
- údaje zpracovávané v rozsáhlém měřítku,
- přiřazování nebo slučování datových souborů pocházejících z různých zpracování pro různé účely anebo zpracované různými správci,
- údaje týkající se zranitelných subjektů údajů,
- nové použití nebo využití nových technologických nebo organizačních řešení,
- zpracování, které subjektům brání uplatnit svá práva nebo využít novou službu nebo smlouvu.



Již zmíněné posuzování osobnosti uchazeče se musí pohybovat v mantinelech vymezených francouzským zákoníkem práce, tedy k posouzení předpokladů a schopností ve vztahu k dané pracovní pozici. Zkoumané měkké dovednosti či další rysy musí mít prokazatelnou souvislost s tímto pracovním místem. Platí opět, že o použitých metodách a postupech musí být uchazeč informován předem.

Použití videokonferenční platformy

Specifickou kapitolu CNIL věnoval použití videa, včetně jednání formou videokonference. Použití videokonferenční platformy může vést k nezamýšleným důsledkům. Některé aplikace totiž získají další osobní údaje například tím, že mají přístup do databáze kontaktů v zařízení. Příručka proto klade velký důraz na doporučení, aby zaměstnavatel zvolil takové řešení, při kterém nedochází k předávání osobních údajů uchazečů do třetích zemí.

Konečné rozhodnutí o člověku může učinit pouze člověk

Tenkým ledem mohou být rovněž automatizované procesy. Právo a ani CNIL jejich použití nevylučuje, ale upozorňuje na to, že konečné rozhodnutí o člověku může učinit pouze člověk. Navíc zde je velká pravděpodobnost, že získané údaje budou nepřesné. Hrozí rovněž riziko, že nastavení algoritmu může být diskriminační. Příručka tak dovozuje, že pouze automatizované rozhodování je takovým, které má závažný dopad na práva subjektu údajů. Totéž platí i o profilování uchazečů.

Pozor na blacklisty…

Velmi opatrný by zaměstnavatel měl být, jestliže si sestavuje seznam („blacklist“) potenciálních uchazečů, jejichž přihlášky by rovnou odmítl. V určitých situacích tak lze činit na základě oprávněného zájmu a za dodržení zásad transparentnosti a proporcionality. Příkladem může být, že zaměstnavatel na seznam zařadí své bývalé zaměstnance, kteří při svém předchozím zaměstnání u zaměstnavatele porušili právní předpisy zvláště závažným způsobem. Důvodem pro vedení na seznamu však nemůže být pozdní příchod k pohovoru. Obecně nesmí být důvody pro zařazení na seznam diskriminační, např. náboženské přesvědčení či politické názory, sexuální orientace nebo členství v odborech.

Jde o přehledný a podrobný návod pro personalisty

Příručka jako taková nepřináší zásadně nové informace, její přínos je v tom, že jde o přehledný a podrobný návod pro personalisty. V každém oddíle shrnuje v několika málo odrážkách základní kroky a principy, které vedou k souladu s platnou legislativou. Různé situace strukturuje a ke každé možnosti dává stručnou informaci, jak má být ochrana osobních údajů odstupňována. V barevně zvýrazněných boxech pak CNIL upozorňuje na obvyklé problémy či pochybení, ke kterým dochází. Francouzský dozorový úřad touto příručkou pokračuje ve své osvětové činnosti, které dlouhodobě věnuje velkou pozornost.

Pavel Janeček
Autor je odborník
na mezinárodní vztahy

6) Jak uvádí samotná příručka, francouzský zákoník práce v ustanovení L.1134-5 v případech možné diskriminace stanovuje promlčecí lhůtu pěti let. Viz https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033461494 (přístup 3. 9. 2023).

7) https://ec.europa.eu/newsroom/article29/items/611236 (přístup 3. 9. 2023).

8) Jde tedy o právo nebýt předmětem pouze automatizovaného rozhodování obsažené např. v čl. 22 GDPR.

DPO PRO. Ročník III, číslo 9. 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. 9. 2023. Autorská práva vykonává vydavatel.