Doporučení CCBE ohledně klíčových nových opatření pro advokáty k dosažení souladu s předpisy v souvislosti s obecným nařízením o ochraně osobních údajů (GDPR)

Prostřednictvím tohoto dokumentu by Rada evropských advokátních komor (CCBE)[1] chtěla uvést přehled základních nových opatření k dosažení souladu s předpisy, která mohou advokátní komory doporučovat za účelem souladu s požadavky stanovenými GDPR.

V následujících částech jsou zdůrazněny ty aspekty GDPR, které zejména pro advokáty nebo advokátní kanceláře (dále jen jako „advokátní praxe“) přinášejí nutnost nového nebo zvýšeného dodržování povinností plynoucích z předpisů. Účelem tohoto zdůraznění těchto záležitostí je, aby mohly advokátní praxe snadno identifikovat problémy, jimiž by se měly zabývat v první řadě. Vzhledem k tomu, že drtivá většina evropských advokátních praxí spadá pod hranici 250 zaměstnanců, níže uvedené záležitosti se netýkají ustanovení, která se vztahují pouze na větší advokátní kanceláře (například požadavek mít pověřence pro ochranu osobních údajů). Rovněž je třeba věnovat pozornost skutečnosti, že mnoho advokátních kanceláří zpracovává osobní údaje, které lze označit za „zvláštní kategorie osobních údajů“.

A. <u>Ohlašování porušení zabezpečení</u>

Podle článku 33 je právní praxe působící jako správce údajů povinna oznámit porušení zabezpečení příslušnému dozorovému úřadu bez zbytečného odkladu, v žádném případě ne později než 72 hodin od okamžiku, kdy se o něm dozvěděla. V případě pozdějšího ohlášení je nutno uvést důvody pro zpoždění. Existuje výjimka v případě, kdy porušení zabezpečení osobních údajů pravděpodobně nezpůsobí žádnou újmu subjektu (subjektům) údajů.

Pokud advokátní praxe působí jako zpracovatel a zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu správci.

Toto oznámení musí mimo jiné obsahovat specifikaci povahy porušení údajů (kategorie a přibližný počet dotčených subjektů údajů a záznamů osobních údajů), pravděpodobné následky porušení zabezpečení a opatření, která byla přijata nebo budou přijata ke zmírnění možných nepříznivých účinků. Oznámení lze provést v různých fázích.

Kromě toho je správce povinen tato porušení dostatečně podrobně zdokumentovat, aby dozorový úřad mohl ověřit soulad s oznámením porušení. Advokátní praxe jsou také povinny stanovit interní postupy pro řešení porušení zabezpečení údajů a zavést mechanismus pro oznamování dozorovému úřadu.

V určitých případech s vysokým rizikem je advokátní praxe rovněž povinna přímo informovat klienta (článek 34), i když existují zvláštní výjimky.

Samotný formát oznámení, definice „zbytečného odkladu“, požadavky na obsah dokumentace a výklad limitů a výjimek dozorovými orgány se přirozeně mohou mezi jednotlivými členskými státy lišit.

[1] CCBE (Rada evropských advokátních komor) zastupuje advokátní komory 32 členských států a dalších 13 přidružených a pozorovatelských států a jejich prostřednictvím více než 1 milion evropských advokátů.

Advokátní praxe by tudíž měly být informovány o již existujících a možných budoucích vnitrostátních pokynech v těchto oblastech.

I když některé členské státy již do vnitrostátního práva zavedly požadavky na ohlašování porušení zabezpečení údajů, směrnice 95/46/ES neukládala, aby správci hlásili porušení zabezpečení údajů dozorovému úřadu. Tento požadavek ale již existuje v odvětví telekomunikací (viz směrnice 2002/58/ES a nařízení Komise (EU) 611/2013, jež se obě vztahují na poskytovatele služeb elektronických komunikací). Výše uvedené prováděcí nařízení bylo definováno způsobem nezávislým na odvětví a v některých členských státech mohou dozorové úřady v oblasti telekomunikací nebo ochrany osobních údajů vydat podrobnější pokyny. Co je ještě důležitější, na základě této legislativy vydala pracovní skupina dozorových úřadů EU v oblasti ochrany osobních údajů zřízená podle článku 29 podrobné pokyny o provádění nařízení o porušení zabezpečení údajů (stanovisko WP 213 č. 03/2014 o oznámení k narušení bezpečnosti osobních údajů, 25. března 2014[2]), které stanoví doporučené postupy v této oblasti pro všechny správce údajů.

Pokud jde o budoucí předpisy v této oblasti, dle čl. 70 odst. 1 písm. g) a h) GDPR vydá Evropská rada pro ochranu údajů pravděpodobně pokyny, doporučení a osvědčené postupy pro a) to, jak zjistit případy porušení zabezpečení osobních údajů, b) to, jak určit „zbytečný odklad", a c) okolnosti, za nichž jsou správce a zpracovatel povinni porušení ohlásit dozorovému úřad nebo klientům.

B. Právo být zapomenut

Článek 17 obsahuje právo na výmaz („právo být zapomenut"), což znamená, že subjekty údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daných subjektů údajů týkají. Tentýž článek ukládá správci povinnost vymazat bez zbytečného odkladu osobní údaje, nastane-li některý z důvodů uvedených v odst. 1 písm. a) až f). Toto ustanovení má původ v případu Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos, Mario Costeja González[3], v němž soud uvedl, že jednotlivci mají právo (za určitých podmínek a záruk) požádat, aby vyhledávače odstranily odkazy s jejich osobními údaji. Jak již ale bylo uvedeno v části I.B výše, odst. 3 písm. e) článku 17 obsahuje významné omezení, kterého by se mohly dovolávat advokátní praxe v souvislosti s činnostmi při zpracovávání, které jsou nezbytné „pro určení, výkon nebo obhajobu právních nároků".

Je důležité si uvědomit, že toto ustanovení samozřejmě nemá přednost před určitými vnitrostátními předpisy, které stanoví povinnost uchovávat údaje po určitou dobu (např. pro splnění daňových povinností).

C. Pověřenec pro ochranu osobních údajů (DPO)

Povinnost advokátních kanceláří jmenovat DPO

Další novinkou je povinnost jmenovat DPO, pokud činnosti zpracování údajů určité organizace zahrnují rozsáhlé pravidelné a systematické monitorování subjektů údajů nebo rozsáhlé zpracování zvláštních kategorií osobních údajů (článek 37). Pracovní skupina zřízená podle článku 29 (WP29), která se skládá

[2] Dostupné z : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_cs.pdf

[3] http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d57637cb18820e4ceb913ecf71af33028d.e34KaxiLc3qMb40Rch0SaxuTahn0?text=&docid=152065&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=1115616

ze zástupců orgánů pro ochranu osobních údajů členských států, vydala pokyny ohledně DPO, v nichž objasňuje jejich úlohu a uvádí doporučené postupy.

Je-li jmenován DPO, organizace musí zveřejnit jeho údaje a musí tyto údaje sdělit příslušnému dozorovému úřadu.

V článku 9 GDPR jsou definovány zvláštní kategorie osobních údajů[4], jejichž zpracování je zakázáno, ale s určitými výjimkami: dle čl. 9 odst. 2 písm. f) se tento zákaz nevztahuje na zpracování nezbytné „pro určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednají v rámci svých soudních pravomocí". Toto ustanovení tedy povoluje zpracování zvláštních kategorií osobních údajů v kontextu práce advokátních praxí ve sporných řízení?.

Na správce a zpracovatele zvláštních kategorií údajů se ale stále vztahuje článek 37 (a rovněž článek 35, viz níže). Tato ustanovení vyžadují v případě, kdy hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9, *jmenování pověřence pro ochranu osobních údajů.* Podle pokynů ohledně DPO lze hlavní činnosti považovat za klíčové operace k dosažení cílů správce nebo zpracovatele. Toto také zahrnuje všechny činnosti, při nichž zpracování údajů tvoří neoddělitelnou součást činnosti správce nebo zpracovatele.

Význam „rozsáhlosti" je důležité téma, protože i malá advokátní kancelář může mít případy s velkým množstvím údajů. Lze ale snadno tvrdit, na základě bodu odůvodnění 91, že se tento požadavek nebude vztahovat na advokáty vykonávající advokacii samostatně. (Viz níže v části D týkající se posouzení vlivu.)

Povinnosti a úkoly DPO

GDPR ukládá DPO významné povinnosti, například monitorování souladu s tímto nařízením, dalšími ustanoveními Unie nebo členských států v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele, dále rozsah odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a provádění souvisejících auditů. DPO rovněž působí jako kontaktní místo pro orgány pro ochranu údajů.

Určený DPO, ať už jde o zaměstnance dané advokátní praxe nebo ne, by měl mít odborné znalosti předpisů v oblasti ochrany osobních údajů a být schopen plnit všechny úkoly na základě článku 39 GDPR, například uchovávání dokumentace veškerých operací zpracování, sledování jejich provádění a školení pracovníků, provádění auditů apod. Osoba působící jako DPO tedy bude mít na starost důležité a těžké úkoly.

Advokáti působící jako DPO

Mohlo by se zdát, že nejvhodnější osobou pro jmenování DPO by měl být advokát, ale je třeba mít na paměti, že s ohledem na rozmanitost povinností vyžadovaných tímto nařízením bude osoba jmenovaná jako DPO vyžadovat více než samotnou právní kvalifikaci.

Asimilace těchto dvou funkcí (advokát/DPO) a riziko záměny mezi těmito funkcemi jsou klíčovým bodem pro jakéhokoli advokáta, který by mohl být jmenován DPO na žádost klienta. Advokát v této pozici může zjistit, že bude muset alternovat mezi funkcí DPO a funkcí advokáta vykonávajícího regulované povolání. Advokát v postavení DPO bude muset zajistit nezávislost a zabránit střetu zájmů,

[4] Tj. „[...] údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby".

zejména střetům, které mohou plynout z toho, že je zároveň kontaktní osobou pro orgán pro ochranu údajů (což je role, která zahrnuje ohlašovací povinnost úřadu, i když je to proti zájmů správce nebo zpracovatele), zatímco má rovněž povinnost zastupovat zájmy klienta v plném rozsahu povoleném zákonem. Vzhledem k tomuto možnému střetu zájmů mohou advokátní komory advokátům doporučit, aby tuto odpovědnost DPO pro externího klienta na sebe vzali, pouze pokud nepůsobili jako advokát v záležitostech, které mohou spadat do oblasti působnosti DPO, ani nebudou po dobu výkonu funkce DPO působit jako advokáti v záležitostech, jichž se účastnili jako DPO.

D. Posouzení vlivu

Pokud je, dle článku 35, pravděpodobné, že určitý druh zpracování (zejména při využití nových technologií, s přihlédnutím k účelům zpracování atd.) bude mít za následek vysoké riziko pro práva a svobody fyzických osob, včetně jakéhokoli rozsáhlého zpracování zvláštních kategorií údajů, správce je před zpracováním povinen provést posouzení vlivu.

Je důležité si uvědomit, že v bodu odůvodnění 91 je vysvětleno, že zpracování osobních údajů by nemělo být považováno za zpracování velkého rozsahu, pokud se jedná o zpracování osobních údajů klientů jednotlivými právníky. Toto je výjimka, která jednoznačně platí pro advokáty vykonávající profesi samostatně, ale i u malé advokátní praxe může být vyžadováno, aby příležitostně tato posouzení prováděla.

Problém je, že podle stávajících standardů (jež nejsou stanoveny pro konkrétní odvětví) mohou být standardy rámců posouzení vlivu na ochranu osobních údajů, například posouzení vlivu, pro malé praxe neúnosné. Například i pouhý požadavek, aby správci údajů identifikovali software a hardware používané pro zpracování osobních údajů, může být určitými úřady vykládán jako požadavek na zavedení systému řízení konfigurací a změn. Obecně nejsou malé praxe s několika zaměstnanci (které jsou ale nad hranicí „samostatného advokáta“) v pozici, aby ve všech případech dodržely tyto požadavky v úzkém slova smyslu. Systém řízení změn by vyžadoval kontrolovaný a rozvinutý systém provozu jejich IT systému, což obvykle není pro praxe této velikosti charakteristické. (Je velmi rozdílné mít hrubý přehled o IT komponentách, které daná praxe má, a mezi fungující a kontrolovanou správou konfigurací a změn.)

Pokyny WP29 ohledně pověřenců pro ochranu osobních údajů (DPO) přijaté 13. prosince 2016 ani aktuálně dostupný návrh pokynů WP29 ohledně posouzení vlivu na ochranu osobních údajů (DPIA) bohužel v tomto ohledu další informace neposkytují. Pokud jde o bod odůvodnění 91, poznámka pod čarou č. 14 pokynů ohledně DPO poukazuje na to, že vše mezi zpracováním samostatným advokátem a zpracováním údajů celé země je šedá zóna. Tato vágnost bude nevyhnutelně vést k různým výkladům.[5]

I když jde o novou zátěž pro advokátní praxe, od provádění posouzení vlivu si nařízení slibuje to, že advokátní praxe budou moci identifikovat a řešit rizika, která by jinak nebyla zjištěna, a zabránit porušení zabezpečení, k nimž by jinak došlo.

[5] Vzhledem k tomu, že v době psaní tohoto dokumentu pracovní skupina zřízená podle článku 29 stále shromažďuje komentáře zúčastněných subjektů k pokynům ohledně posouzení vlivu na ochranu osobních údajů (DPIA), revidovaná a konečná verze by mohla být publikována v průběhu roku 2017 a mohla by obsahovat objasnění toho, co je u činností zpracování „rozsáhlé“.

V porovnání s oznámením o porušení zabezpečení osobních údajů neexistuje jasná regulatorní historie ani pokyny, jak by v advokátních kancelářích nebo u jiných podobných profesionálů měla být posouzení vlivu prováděna.

V současné době jsou posouzení vlivu na ochranu osobních údajů rozmanitá co do obsahu i metod a jsou většinou populární v zemích s tradicí angloamerického práva.[6] V Evropě vydal v roce 2014 úřad informačního komisaře Spojeného království dokument *„Privacy Impact Assessment Code of Practice" (Kodex posuzování vlivu na soukromí)* [7] (po dokumentu *„Privacy impact assessment manual", Návod k posuzování vlivu na soukromí*, který byl vydán již v roce 2007) a francouzský orgán pro ochranu údajů (CNIL) vydal návod k posuzování vlivu na soukromí v roce 2015[8]. Rovněž Evropská komise vydala doporučení vyzývající k posuzování vlivu v souvislosti s čipy RFID[9] (radio frequency identifier chips), které vyústilo v dohodu v daném odvětví ze dne 12. ledna 2011, *„Privacy and Data Protection Impact Assessment Framework for RFID Applications" (Rámec pro posuzování vlivů na soukromí a ochranu údajů u aplikací RFID).* Tento rámec byl schválen WP29 a sloužil rovněž jako vzor pro podobnou „vzorovou" iniciativu u inteligentních měřičů.[10]

Tato doporučení jsou bohužel konkrétní pro oblast, jíž se týkají, a pravděpodobně je nebude možno použít jako zdroj praktických pokynů pro posuzování vlivu advokáty nebo podobnými profesionály v kontextu oznamování porušení zabezpečení osobních údajů. Další podrobnosti lze očekávat od vnitrostátních pravidel pro konkrétní odvětví, pokud budou stanovena.

Advokátům, které zajímá obecné pozadí posouzení vlivu na soukromí, mohou pomoci výsledky studie posuzování vlivu na soukromí financované Komisí (Rámec posouzení vlivu na soukromí u ochrany osobních údajů a práv na soukromí).[11]

Souhrnně lze říci, že i když se samo nařízení zabývá některými aspekty posouzením vlivu detailně, samotné praktické požadavky nejsou dosud známy. Očekává se, že dozorové úřady a výše uvedená Rada poskytnou další pokyny u chybějících detailů, například ve vztahu k druhu operací zpracování, v nichž mohou být tato posouzení vlivu vyžadována.

E. Přenositelnost údajů

Subjekty údajů mají právo od správce obdržet kopii osobních údajů, které se na ně vztahují a které jsou nebo byly zpracovány. Článek 20 nařízení vyžaduje, aby byly tyto údaje předány ve strukturovaném, běžně používaném a strojově čitelném formátu, ale toto jsou pouze velmi obecné požadavky.

Podle pokynů WP29 ohledně práva na „přenositelnost údajů" jsou pojmy „strukturovaný", „běžně používaný" a „strojově čitelný" souborem minimálních požadavků, které by měly usnadnit interoperabilitu formátu údajů poskytovaných správcem údajů. Pokyny WP29 rovněž uvádějí, že vzhledem k široké škále možných typů údajů, které může správce údajů zpracovávat, GDPR neukládá konkrétní doporučení pro formát těchto osobních údajů, jež mají být poskytnuty.

---

[6] Za základy posouzení vlivu na soukromí se považují posouzení dopadu na životní prostředí původně z USA, viz část D1 dokumentu PIAF na http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf.

[7] Viz https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

[8] Viz https://www.cnil.fr/fr/node/15798.

[9] Viz doporučení Komise 2009/387/ES na http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:CS:PDF.

[10] Viz doporučení Komise 2012/148/EU a jeho schválení WP29 na http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_cs.pdf

[11] http://www.piafproject.eu/About%20PIAF.html

I když je požadavek na běžně používaný a strojově čitelný formát snadno splnitelný, otázka „strukturovanosti“ může být značným problémem. Dokumenty, které advokáti používají, mají obvykle nestrukturovaný obsah (například formáty Microsoft Word nebo PDF). Pro předávání úplných soudních spisů nebo případů ve strukturovaném formátu neexistuje všeobecně přijímaný formát.

Všichni advokáti vědí, jak předávat spisy advokátním kancelářím nově určeným bývalými klienty, ale někdy je přesný formát a struktura tohoto předání již v oblasti, kde mohou mezi advokáty vzniknout spory. V budoucnosti tento problém může vyžadovat další regulaci advokátními komorami.

F. Schopnost sledovat příjemce osobních údajů

Správci údajů mají povinnost být schopni sledovat příjemce osobních údajů patřících konkrétní osobě (přinejmenším jméno a kontaktní údaje pro elektronickou komunikaci). Toto je opět povinnost, kterou by řada advokátních praxí splnila, pouze pokud by ve svých IT systémech provedla určité změny (například konfigurace systému tak, aby měl spolehlivě vysledovatelné záznamy příjemců osobních údajů).