Spolek pro ochranu osobních údajů

Připomínky k návrhu Metodiky obecného posouzení vlivu na ochranu osobních údajů (DPIA)

V Praze, dne 15.12.2019

Spolek pro ochranu osobních údajů („Spolek“) považuje předložený materiál za velmi kvalitně zpracovaný. V rámci pracovního setkání členů Spolku jsme předložený materiál prodiskutovali, a to zejména z pohledu nejasností, které by mohly vyvstat především při jeho praktické aplikaci.

Z tohoto pohledu si proto dovolujeme předložit několik připomínek a návrhů upřesnění, popř. doplnění, které vzešly z této interní diskuze.

Z obecných bodů jsme diskutovali otázku charakteru dokumentu „K povinnosti správců provádět posouzení vlivu na ochranu osobních údajů (DPIA)“ ve smyslu čl. 35 odst. 4 GDPR dostupného z https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38349 (dále jen „pozitivní seznam“). Z našeho pohledu vychází nařízení z toho, že tento pozitivní seznam vydaný dozorovým orgánem zahrnuje případy, kdy je nutné vždy provést posouzení vlivu, aniž je potřeba dalšího zhodnocení vlivu. Vedle toho je možné vydat „negativní“ seznam podle čl. 35 odst. 5. Podle našeho názoru znění nařízení počítá s tím, že vedle operací identifikovaných v těchto seznamech budou existovat i další operace zpracování - nezařazené ani do jednoho seznamu - u nichž tedy bude třeba provést předběžné zhodnocení, aby správce určil, zda má provést DPIA či nikoliv (tedy v zásadě „šedá zóna“ mezi pozitivním a negativním seznamem operací zpracování). Z textu předloženého materiálu (popis 2. etapy na str. 8) nám není zřejmé, zda úřad vychází z toho, že pokud nejsou naplněna hlediska požadovaná pozitivním seznamem, vždy se jedná o zpracování, které povinnosti DPIA nepodléhá, nebo zda v tom případě musí být provedeno další – předběžné – zhodnocení zamýšleného zpracování (ledaže by byla naplněna kritéria negativního seznamu podle čl. 35 odst. 5 Nařízení) s cílem identifikovat, zda má být DPIA provedena, či nikoliv. Zejména vzhledem k tomu, že pozitivní seznam je založen na principu kriteriální analýzy, přichází do úvahy obě varianty. Otázkou pak zůstává, jaká další kritéria nad rámec 10 kritérií identifikovaných v pozitivním seznamu, by měl v případě dalšího hodnocení správce brát v potaz a hodnotit. Domníváme se, že by bylo velmi vhodné tuto otázku vyjasnit.

Samotné požadavky posouzení rizik podle 3. části (str. 9) podle našeho názoru poněkud ponechávají stranou zhodnocení rizik, která mohou vyplývat ze samotného charakteru zpracovávaných údajů anebo prováděných operací, přičemž se zaměřují pouze na aspekty bezpečnostních (kybernetických) rizik a souvisejících technických a organizačních opatření. Zjevné je to zejména v rámci požadavků uvedených v kroku 2 na str. 9, kde již samotná operace zpracování může představovat zvýšené riziko,

a to i v případě, kdy veškerá zde uvedená opatření budou na úrovni *state of art* – a tedy podle návrhu metodiky by nevznikala žádná rizika. Vyhodnocení rizik spojených s údaji a operacemi zpracování může v určitých případech vést k nutnosti návratu do 2. části DPIA (předběžné hodnocení) a přehodnocení závěrů o nezbytnosti zpracování jako takového (právě s ohledem na rizika plynoucí z kombinace charakteru údajů a možných aplikovatelných bezpečnostních opatření). V některých případech může být ovšem riziko spočívající v charakteru údajů anebo zpracovatelských operací zcela primární, bez ohledu na kybernetické aspekty daného zpracování. Doporučujeme proto zvážit vyšší integraci i tohoto pohledu do metodiky. Detailněji se k tomuto aspektu vyjadřujeme v druhé části našeho stanoviska.

Ačkoliv vysoce hodnotíme kvalitu a komplexnost připraveného materiálu, požadavky v něm stanovené mohou být obzvláště pro menší správce příliš náročné, doporučujeme proto zdůraznit, že se jedná o doporučení a správci dostojí zákonným požadavkům na zpracování DPIA vždy, kdy jimi provedená DPIA splňuje podmínky čl. 35 odst. 7 nařízení. Z hlediska přehlednosti pro menší správce by možná bylo vhodné zvážit, zda některý text uvedený v závorkách přesunout do samostatné více vysvětlující věty.

K jednotlivým dílčím problémům:

Str. 4 - *Posouzení vlivu se zpravidla připravuje pro (operace) zpracování osobních údajů (jeho hranice definuje správce –například to může být účetnictví, ale i celý provozní/ekonomický systém správce).*

Doporučujeme zvážit tyto příklady. Předně se jedná o velmi široce vymezené druhy zpracování, jež by vyžadovaly velmi komplexní a rozsáhlou DPIA. Vedle toho se příklad účetnictví nejeví jako zcela vhodný, protože pro vedení účetnictví nebude třeba DPIA obvykle provádět. Ani provozní systém správce nemusí nutně naplnit kritéria vysoce rizikového zpracování, zejména pokud neobsahuje zvláštní kategorie údajů.

Vedle toho v praxi správci volí provádění DPIA buď z pohledu jednotlivých operací (popř. jejich souboru) zpracování, nebo z pohledu systému používaného ke zpracování osobních údajů. Doporučujeme ponechat správcům v tomto směru volnost, aby mohli v určit, jaké kritérium pro provedení DPIA zvolí. To by jim mělo také umožnit, aby nemuseli vždy znovu provádět DPIA v rozsahu systémů, které slouží jako podpůrné pro samotné potenciálně rizikové zpracování, které jsou ale obecně vyhodnoceny jako dostatečně zabezpečené (vedlo by to ke zjednodušení rozsahu kroků nutných podle kroků 1, 2 a 3 v třetí části DPIA (viz str. 9).

Str. 8 – prosíme o vyjasnění tohoto požadavku: *seznam zpracovávaných údajů (zde asi nepostačují pro provedení analýzy kategorie osobních údajů),*

Domníváme se, že postačí uvedení kategorií údajů (např. „jméno“, „příjmení“, „adresa“, „rodné číslo“ apod.). Uvést přímo seznam zpracovávaných údajů by bylo nejen velmi náročné, ale obvykle i nemožné, protože DPIA se provádí standardně před započetím zpracování. Pro vyloučení pochybností by bylo vhodnější přímo ve výčtu náležitostí uvést výslovně „**kategori**e subjektů údajů“, „**kategorie** příjemců údajů“ namísto „**popisu**“ subjektů údajů či příjemců. Obecné nařízení rovněž tak pracuje s pojmem „kategorie“.[1]

[1] Viz např. čl. 30 odst. 1 písm. c) Obecného nařízení

Str.8 – požadavek na *diagram (workflow) popisující zpracování (tok) osobních údajů* by měl být volitelný a bylo by vhodné vyjasnit, zda se má týkat pohybů údajů v systémech správce (případně zpracovatelů) anebo i z hlediska příjemců.

Str. 9 – požadavek na synchronizaci s analýzou rizik má smysl v případě, že je analýza rizik prováděná v oblasti kyberbezpečnosti. Méně vhodným se jeví v případě, kdy jde o analýzu rizik prováděnou v rámci business/compliance procesů, které jsou obvykle v jiném rozsahu a s jiným zaměřením.

Str. 9 – 3. část – postup je relevantní pro hodnocení kybernetických rizik, což nebude relevantní v případě mnoha prováděných hodnocení dopadů „běžných", byť vysoce rizikových, zpracovatelských aktivit, které dokonce nutně nemusí mít elektronickou podobu. Metodika postrádá pohled na hodnocení rizik a dopadů procesu do práv a svobod jednotlivce ve smyslu čl. 35 Obecného nařízení. Možná je v tomto ohledu návrh Metodiky příliš preskriptivní a neponechává dostatečnou flexibilitu správci při zohlednění specifik hodnocené zpracovatelské aktivity.

3. krok – domníváme se, že relevantní je nejenom určení hrozeb, ale i jejich následků, např. jaká hrozba (riziko) vzniká pro subjekty údajů v případě narušení integrity nebo dostupnosti jejich údajů.

Str. 12, text: *V případě, že je posouzení rizik prováděno pro více zpracování osobních údajů (například předkladatel právního předpisu, který upravuje totožné zpracování osobních údajů prováděné řadou subjektů např. obcí), budou navržená opatření obecnějšího charakteru (posouzení totiž nemůže zohledňovat například začlenění zpracování osobních údajů do informačních systémů spravovaných týmž subjektem např. společné užití podpůrných aktiv). V těchto případech je nutno posouzení vlivu přizpůsobit konkrétním podmínkám správce.* Ačkoliv jsme si vědomi textu § 10 zákona č. 110/2019 Sb., doporučujeme přesto v tomto dokumentu zdůraznit (v souladu s čl. 35 odst. 10 nařízení), že v daném právním předpisu musí být uvedeny *konkrétní operaci nebo soubor operací zpracování.* Jen v takovém případě totiž podle nás může být obecné v souvislosti s přijímaným zákonem provedené posouzení dostatečnou zárukou pro práva subjektů údajů, neboť může zohlednit všechny aspekty a rizika zamýšleného zpracování. V opačném případě je nezbytné provést standardní DPIA.

Str. 12, 4. část: *Monitorování a přezkoumávání rizik pro práva a svobody subjektů údajů probíhá nepřetržitě (nová aktiva, nové (dosud neuvažované) hrozby, nové synergické efekty působení hrozeb, identifikace nových zranitelností, po porušení zabezpečení osobních údajů).* Doporučuje zdůraznit, že kontroly postačuje provádět v souladu s plánem mitigačních či pouze monitorovacích kroků obsaženým v DPIA podle aktuální potřeby. Tento se bude logicky lišit podle komplexnosti plánovaných opatření mitigujících rizika či pouze potřeby jejich efektivitu v přiměřeném časovém intervalu kontrolovat. Plošný požadavek *nepřetržitého* monitorování je opět příliš preskriptivní a neponechává správci potřebnou flexibilitu zohledňující specifika posuzované aktivity.

Str. 12: text: *Monitorování uplatnění posouzení vlivu zajišťuje nezávislá osoba s odbornými znalostmi a praxí jmenovaná správcem.* Domníváme se, že požadavek na nezávislost takové osoby bude obvykle nepřiměřený. Často naopak bude výhodné, aby monitorování prováděla osoba obeznámená dobře s chodem správce (např. interní zaměstnanec, pověřenec apod.).

Str. 13 – získání stanoviska uživatelů. Domníváme se, že stanovisko uživatelů by mělo být získáno spíše k samotnému zpracování (nikoliv až posouzení) a následně sloužit jako jeden z podkladů pro zpracování DPIA (viz i čl. 35 odst. 9 Nařízení).

PŘÍKLAD TABULKY PRO POSOUZENÍ RIZIK

Někteří z našich členů přistoupili k praktickému využití navržené tabulky posouzení rizik. Protože tato je dimenzovaná především pro hodnocení kybernetických rizik, je její praktická aplikace na řadu zpracovatelských aktivit velmi obtížná. V této souvislosti bychom považovali za velmi přínosné uspořádání schůzky zástupců Spolku se zástupci Úřadu za účelem vyjasnění práce s touto tabulkou, případně rovněž zvážili její možné úpravy, aby mohla efektivně sloužit svému účelu.