SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

# Stanovisko k materiálu Pracovní skupiny pro ochranu dat dle čl. 29: vodítka pro výklad obsahu obecného nařízení o ochraně osobních údajů – téma Hodnocení dopadů na ochranu dat

## ÚVOD STANOVISKA

Mezi priority Svazu průmyslu a dopravy ČR (dále i „SP ČR“) patří mj. téma ochrany osobních údajů v digitálním prostředí: jde o jednu z priorit Expertního týmu pro digitální ekonomiku, v jehož rámci také funguje specializovaná Pracovní skupina pro ochranu dat, SP ČR je rovněž aktivním členem Pracovní skupiny Úřadu vlády pro legislativu v oblasti ochrany dat. K tématu připravenosti firem na zavedení novinek vyplývajících z nového evropského obecného nařízení o ochraně osobních údajů (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 – dále jen „GDPR“) realizoval SP ČR také na konci roku 2016 průzkum mezi českými podnikateli a ve I. čtvrtletí roku 2017 sérii regionálních diskusních setkání s podnikateli.

V návaznosti na publikaci vodítek pro výklad GDPR přijatých na jednání Pracovní skupiny pro ochranu dat dle čl. 29 jako poradního orgánu Evropské komise pro téma ochrany osobních údajů dne 4. dubna 2017 nyní SP ČR uplatňuje k publikovaným dokumentům následující komentáře:

## VODÍTKA K HODNOCENÍ DOPADŮ NA OCHRANU OSOBNÍCH ÚDAJŮ A HODNOCENÍ MÍRY RIZIKA

### Obecné poznámky SP ČR

- *V rámci své výkladové činnosti se WP29 zaměřuje spíše na technický a sémantický výklad textu GDPR, aniž by zohlednila praktické aspekty a nutnost dosáhnout za pomocí výkladových vodítek aplikovatelnosti GDPR v praxi. Projevuje se přílišná akademičnost přístupu WP29 s tím, že v některých ohledech jdou vodítka nad rámec WP29 a, ač po stránce sémantické dochází k vysvětlení obsahu WP29, pro praxi je ve výsledku obsah GDPR v kombinaci s vodítky ještě obtížněji aplikovatelný, než před jejich publikací.*
- *Co do formy vodítek, lze konstatovat, že oproti doposud publikovaným vodítkům (k právu na přenositelnost, pověřencům pro ochranu osobních údajů a identifikaci vedoucího dozorového orgánu) jsou nyní publikovaná vodítka více analyticky zpracovaná,*
- *Základem obsahu vodítek je správně jeden ze základních principů prolínajících se celým GDPR, tedy přístup založený na riziku – ten je základem nejen pojetí hodnocení dopadů, ale např. i bezpečnosti, ohlašovací a oznamovací povinnosti správců a zpracovatelů a řady dalších nových povinností vyplývajících z nařízení,*
- *SP ČR tedy v návaznosti na toto obecné hodnocení dále k nim formuluje svá doporučení směřující k revizi obsahu vydaných vodítek tak, aby zajistila vyšší míru aplikovatelnosti GDPR zejména ve firemní praxi. Současně využívá možnosti připomínkovat navržený text s cílem upozornit na některé nepřesnosti odstranit tak možné negativní dopady.*

TELEFON (+420) 225 279 111 | E-MAIL SPCR@SPCR.CZ
WEB WWW.SPCR.CZ | ADRESA FREYOVA 948/11, 190 00 PRAHA 9
ZAPSANÝ VE SPOLKOVÉM REJSTŘÍKU, VEDENÉM MĚSTSKÝM SOUDEM V PRAZE ODDÍL L, VLOŽKA 3148.
IČO: 00536211, DIČ: CZ00536211.

## Specificky

**Co zahrnuje proces hodnocení dopadů na ochranu údajů?**

- Dle WP29 pojem zahrnuje buď jednorázovou procesní operaci nebo soustavu procesních operací.
- WP29 na přehledném schématu (str. 6 vodítek) ilustruje procesy, které vedou ke zpracování hodnocení dopadů a které po něm následují.

**Které procesní operace jsou předmětem hodnocení dopadů?**

- DPIA je povinné tam, kde zpracování „pravděpodobně způsobí vysoké riziko“ pro zpracování údajů, přičemž za vysoce rizikové jsou považovány procesy:

    1. Evaluace nebo scoring vč. profilování a predikce
    2. Automatické rozhodování s právními nebo jinými zásadními důsledky
    3. Systematické monitorování
    4. Zpracování citlivých dat
    5. Velký rozsah zpracování dat
    6. Data týkající se zranitelných subjektů údajů:

        Z našeho pohledu je rizikové zahrnutí zaměstnanců mezi zranitelné skupiny – pro správce údajů je pak práce s jejich osobními údaji nesmírně ztížena. Zařazení zaměstnanců mezi zranitelné skupiny zvyšuje náklady na implementaci GDPR, zejména pro MSP. Tento požadavek pro zpracování DPIA by proto měl být upřesněn. Kromě zákonného důvodu v podobě pracovněprávních předpisů, které jsou titulem pro zpracování dat, by WP 29 měla identifikovat, u kterých zaměstnavatelů je tento požadavek obligatorní, např. ve spojení s určitým způsobem nakládání s daty (obdobně jako u zákazníků). Doporučujeme text vodítek doplnit v kontextu rec. 91. kdy se zdůrazňuje, že se jedná o operace, kdy je vzhledem k použití technologie pro subjekty údajů obtížnější uplatnit svá práva. Tento princip v pracovních vztazích platí jen částečně a povinnost DPIA by tak neměla na zaměstnavatele dopadat plošně.

    7. Propojování nebo kombinace datových souborů
    8. Inovativní využití nebo aplikace technologických či organizačních řešení
    9. Datové transfery mimo hranice EU:

        To, že datové transfery mimo EU jsou automaticky považovány za proces s vysokým rizikem, vnímáme jako znepokojující. WP29 zde vytváří dojem, že úroveň ochrany osobních údajů vně hranic EU je v principu nižší než v EU a že zde kvůli tomuto dochází k vysoce rizikovým operacím. Avšak mezi identifikací „vysokého rizika“ a „rizika“ obecně je rozdíl a

mezinárodní datové transfery jsou obvykle kryty alternativními metodami pro přenos dat jako např. standardní smluvní doložky, závazná vnitrofiremní pravidla nebo Privacy Shield. Zahrnutí mezinárodních datových transferů jako základního kritéria pro rizikovost operace proto nepovažujeme za správné a v nesouladu se záměrem zákonodárce.

10. Tam, kde zpracování znemožňuje subjektům údajů výkon práva nebo využití služby či smlouvy (jak vyplývá z čl. 22 a recitálu 91 GDPR).

Čím více výše popsaných kritérií je kumulativně splněno, tím pravděpodobnější je existence vysokého rizika pr o hodnocení dopadů údajů a tím spíše je pravděpodobná potřebnost DPIA.

- DPIA se nevyžaduje tam, kde zpracování „pravděpodobně nezpůsobí vysoké riziko“ nebo bylo již schváleno, nebo má právní základ,

- Pokud se týče již probíhajících zpracování, podmínky pro provedení DPIA se budou aplikovat na operace zpracování, které budou probíhat po nabytí účinnosti GDPR.

*Příklady (viz str. 10 vodítek):*

- *DPIA se vyžaduje v případech, kdy nemocnice zpracovávají genetická a zdravotní data svých pacientů v rámci informačního systému, správce monitoruje dopravu na dálnici prostřednictvím inteligentních videoanalytických systémů s automatickým rozpoznáváním SPZ, firma monitoruje aktivity svých zaměstnanců včetně monitoringu jejich pracovního místa, aktivity na internetu apod., shromažďování veřejně dostupných profilů osob na sociálních sítích a jejich další zpracování v rámci interních firemních systémů.*

- *DPIA se naopak nevyžaduje v případech, kdy je okruhu registrovaných uživatelů automaticky zasílán newsletter nebo tam, kde jsou uživatelům webu nabízejícího ojetá auta doporučovány nové odkazy v závislosti na jejich předchozím chování na webovém rozhraní.*

**Jak správně provádět DPIA?**

- DPIA má být prováděn před samotným zpracováním údajů

- Povinnost provést DPIA včetně odpovědnosti za způsob provedení nese vždy správce, spolupracuje přitom s DPO a svým zpracovatelem nebo zpracovateli

- Pro realizaci DPIA mohou být použity různé metodologie, ale DPIA by mělo vždy naplňovat společná základní kritéria

- Výsledek DPIA by měl být publikován – buď v plném nebo v částečném rozsahu (což je však výklad, který jde nad rámec GDPR), v případě předchozí konzultace navíc musí být komunikován dozorovému orgánu. Konzultace s dozorovým orgánem je přitom povinná tam, kde existuje vysoké „zbytkové riziko“. Zakotvením povinnosti publikace zde jde WP 29 nad rámec nařízení i ostatních právních předpisů EU o transparentnosti právnických osob atd. Publikace „slabých míst“ v podobě

DPIA pak může ohrozit správce, popř. zpracovatele. Doporučujeme, aby byla publikována informace o provedení DPIA, ale nikoliv celý DPIA, jak vyplývá z návrhu stanoviska na str. 17.

- Proces provádění DPIA by měl zahrnovat postup od prvotního popisu procesu přes následující vyhodnocení potřebnosti a proporcionality hodnocení dále přes volbu opatření, kterými bude zajištěn soulad s GDPR a dále před vyhodnocení rizik pro práva a svobody subjektů údajů a opatření zvolená k eliminaci těchto rizik až po dokumentaci celého procesu, jeho monitoring a vyhodnocení a následné eventuelní cyklické opakování celého postupu v situaci, kdy dojde ke změně nastavení systémů či procesů v organizaci správce či zpracovatele, které zahrnují zpracování osobních údajů

- Není však jasné, co je „where appropriate" – WP29 nepřináší výklad pojmu, ale naopak správcům ukládá nové povinnosti, které znamenají novou administrativní zátěž a nové výdaje.

**Závěry a doporučení WP29**

Dle výkladu WP29 je důležité, aby v případě existence vysokého rizika správce:

- Vybral si správně metodologický způsob provedení DPIA – v pojetí WP29 ovšem má správná metodologie mj. obsahovat i zahrnutí příslušných zainteresovaných stran s přesnou identifikací jejich zodpovědností (vč. např. subjektů údajů a jejich zástupců)

- Poskytl po provedení DPIA výstupy dozorovému orgánu

- Konzultoval s dozorovým orgánem případy, kdy nezvládá vymezit dostatečná opatření pro řešení vysokého rizika

- Periodicky revidoval provedené DPIA a současně i všechny hodnocené procesy, a to nejméně v případech, kdy nastává změna míry rizika

- Dokumentoval všechna přijatá rozhodnutí.

***<u>Připomínky SP ČR k publikovaným vodítkům:</u>***

***WP29 jde dle našeho názoru nad rámec GDPR v těchto oblastech:***

1. ***Výklad pojmu „zranitelné skupiny subjektů údajů"*** *– je nepřijatelné, aby byl pojem rozšířen i na zaměstnance, neboť to významně zkomplikuje práci se zaměstnaneckými daty.*

2. ***Mezinárodní datové transfery by neměly být a priori zahrnuty mezi vysoce rizikové operace vyžadující DPIA.*** *Rizikovost mezinárodních datových operací by měla být hodnocena ad hoc podle rozsahu a způsobu předávání dat včetně eventuálního využití některého z mechanismů pro zabezpečení datových toků náhradními mechanismy.*

3. ***Povinnost k provedení DPIA tam, kde je identifikováno „where appropriate"*** *– WP29 nepřináší výklad pojmu, ale naopak správcům ukládá nové povinnosti, které znamenají novou administrativní zátěž a nové výdaje pro správce údajů.*

4. ***Významné rozšíření povinností správců údajů k provedení DPIA nad rámec GDPR*** *tam, kde např. dochází k vytěžování dat z veřejných profilů, neboť jde o kombinaci velkého rozsahu a současně scoringu. V těchto případech tedy dle výkladu WP29 musejí být prováděny specifické a opakované DPIAs, což vytváří novou zátěž pro správce údajů.*

5. ***Periodické re-assessmenty „v rámci dobré praxe"*** *by dle doporučení WP29 měly být prováděny každé tři roky (viz str. 12 vodítek), což jde významně nad rámec GDPR, které vyžaduje periodický přezkum DPIA vždy pouze v případech, kdy dojde k meritorní změně (tj. kdy se změní míra rizika) a nikoli v časových periodách.*

6. ***Metodologie provádění DPIA musí mj. zahrnovat i zahrnutí celé řady stakeholderů včetně např. subjektů údajů a jejich zástupců,*** *což vnímáme jako výrazně kontraproduktivní. Je zcela nereálné, aby např. v případě bank byli jejich klienti a jejich zástupci zapojeni do procesu hodnocení dopadů rizik zpracování údajů.*

7. ***Publikace DPIA,*** *kterou WP29 doporučuje jako „particularly good practice" tam, kde je hodnocením dopadů dotčena veřejnost, je výrazně kontraproduktivní: správcům hrozí reputační riziko, ohrožení jejich obchodního tajemství a důvěrných informací, prostřednictvím publikace navíc de facto informují potenciální útočníky, kde jsou jejich zranitelná místa, publikují informace o vlastní zranitelnosti.*

8. *WP29 v poznámce (str. 4 vodítek) uvádí, že* ***DPIA může být kladeno na roveň v řadě právních řádů a firemních metodologií již známému PIA.*** *DPIA má však zvláštní pravidla, jde o jakýsi ekvivalent k „velké RIA", která má ustálená pravidla, strukturu, metodologii a obnáší vyšší míru zátěže pro jejího zpracovatele. Je pro nás nepřijatelné, aby „prosté" impact assessmenty byly podřízeny přísnějším pravidlům, která platí pro DPIA.*

***Naopak nedostatečná jsou vodítka WP29 ohledně otázky povinných konzultací s dozorovým orgánem v případech, kdy je identifikováno tzv. reziduální (zbytkové) riziko:***

- ***Není zřejmé, v jakých případech budou dozorové orgány vyžadovat předchozí konzultaci v případě reziduálních rizik*** *a ani vodítka WP29 se k této otázce nevyjadřují. Např. banky běžně akceptují 10-15 reziduálních rizik v měsíci, avšak pokud dle stanoviska dozorových orgánů bude třeba v těchto případech předchozích konzultací, může jít jak pro správce, tak i pro dozorový orgán o nepřiměřenou zátěž. Přijetí reziduálních rizik je nutnou procedurou pro řešení rizik rovněž i v souladu s mezinárodními standardy (např. ISO/IEC 27005). Pokud však dozorové orgány budou trvat na konzultaci skutečně všech reziduálních rizik, může tato administrativní zátěž být pro správce údajů až likvidační. WP 29 by dle našeho názoru měla povinnosti spojení s konzultací reziduálních rizik sjednotit, aby následně nedocházelo ke vzniku různorodých implementačních národních úprav a komplikacím na straně nadnárodních koncernů.*

- ***V této souvislosti není rovněž zřejmé, jak bude v této postupovat Sbor*** *při vydávání pokynů týkajících se operací zpracování, u nichž se má za to, že je nepravděpodobné, že by mohly představovat vysoké riziko pro práva a svobody fyzických osob, a stanovit, jaká opatření mohou být v takových případech k řešení podobného rizika postačující. (Rec. 77)*

- ***Příloha č. 2*** *– kritéria pro tvorbu přijatelného DPIA by měla být zásadně přepracována v tom směru, aby nebyla pouhým opisem a odkazy na příslušné články a recitály GDPR, ale blíže definovala, jak konkrétně provádět jednotlivé části DPIA.*

  ***Naše doporučení: vodítka doplnit o tuto otázku, inspirovat se přitom pozicí CIPL k tématu přístupu založeného na riziku.***