Svaz průmyslu a dopravy České republiky
Confederation of Industry of the Czech Republic

Stanovisko Svazu průmyslu a dopravy ČR
k zahájení trialogu ohledně
návrhu obecného nařízení o ochraně osobních údajů

a) Obecně:

1. Svaz průmyslu a dopravy dlouhodobě poukazuje na skutečnost, že data představují v 21. století stejný potenciál pro rozvoj hospodářství, jako například přírodní zdroje. Svaz průmyslu a dopravy ČR (dále jen „SP ČR"), proto vítá záměr Evropské komise vytvořit moderní pravidla pro regulaci ochrany osobních údajů v digitálním prostředí. Tento záměr je však splnitelný jen za podmínky, že požadavek na ochranu soukromí půjde ruku v ruce s posilováním schopnosti evropských podniků inovovat a být konkurenceschopnými na domácích i světových trzích. Evropská unie by měla využít této výjimečné příležitosti k tomu, aby ukázala, že je schopna přijmout moderní legislativu, která ochrání soukromí jejích občanů a současně podpoří inovace a hospodářský rozvoj. To se však Evropské komisi v jejím návrhu nepodařilo.

2. SP ČR oceňuje pokrok ve vyjednáváních, ke kterému došlo ohledně textu návrhu nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „GDPR") v Radě EU. Nicméně je přesvědčen, že je třeba vynaložit další úsilí při jednáních trialogu, aby byl návrh nařízení ucelený, konzistentní a schopný obstát i v realitě rychlého vývoje technologií a na datech založených inovací.

3. SP ČR tedy apeluje na všechny aktéry, aby nerezignovali na původní záměr zjednodušení právní úpravy ochrany osobních údajů, který byl (kromě ochrany osobních údajů) jedním ze základních důvodů pro přípravu GDPR. K tomu však zatím v žádné ze slibovaných oblastí nedošlo: nepodařilo se vytvořit funkční jednotné kontaktní místo, prosadit funkční přístup založený na riziku ani snížit administrativní zátěž, která na podniky dopadne. Rizikem také je, že se nařízení může v podstatě stát dvaceti osmi směrnicemi, kde mnoho oblastí bude ponecháno na rozhodnutí členských států.

4. SP ČR proto vyzývá strany zúčastněné jednání v trialogu, aby výsledná podoba GDPR:
    a. Uznala hodnotu pseudoanonymizovaných dat,
    b. Zachovala současný model legitimního zájmu,
    c. Vyhnula se jednoznačnému souhlasu s návrhem za všech podmínek,
    d. Zajistila zjednodušení administrativy a zavedla funkční a v praxi realizovatelný mechanismus jednotného kontaktního místa,
    e. Zachovala volný pohyb dat v přeshraničním styku,
    f. Zavedla dobře definovaný přístup založený na riziku,
    g. Odklonila se od paušální sdílené odpovědnosti zpracovatele a správce údajů,
    h. Zajistila omezení profilování na ty operace, které přinášejí významný negativní důsledek.
    i. Respektovala, že v praxi existují takové systémy zacházení s přístupy ke koncovým zařízením uživatelů, u kterých nedochází k bezprostřednímu ohrožení bezpečnosti jejich údajů (např. vzdálené přístupy podpory dodavatele či správce informačního systému).

Freyova 948/11, 190 00 Praha 9
Tel.: +420 225 279 111, Fax: +420 225 279 100
e-mail: spcr@spcr.cz, www.spcr.cz

5. SP ČR proto žádá, aby strany zúčastněné na jednání v trialogu vzaly v úvahu výše nastíněné argumenty a doporučení. Současně apeluje na jejich odpovědnost vůči firmám, které jsou správci i zpracovateli osobních údajů a žádá je, aby nevytvářely právní rámec, který je založen na nejhorším možném scénáři, ale aby naopak vytvořily takový režim ochrany osobních údajů, který bude schopen podporovat v příštích letech rozvoj inovací ve všech průmyslových odvětvích.

b) Ke konkrétním bodům návrhu nařízení:

1. **Zajištění harmonizace režimů ochrany osobních údajů, zjednodušení jejich administrativy a zavedení funkčního a v praxi realizovatelného mechanismu jednotného kontaktního místa**:
   Návrh GDPR dosáhl při jeho projednávání na půdě Evropského parlamentu v r. 2013 rekordního počtu pozměňovacích návrhů, což indikuje, že nalezení shody na textu dokumentu bude vyžadovat hledání kompromisů. Proto je na místě obava, že bude tendence některé sporné otázky ponechat úpravě prováděcích předpisů. Má-li však být evropská regulace dostatečně efektivní, harmonizovaná a má-li být schopna skutečně napomoci vytvoření jednotného digitálního trhu v rámci EU, měl by text GDPR minimalizovat počet odchylek a výjimek z aplikace v jednotlivých členských zemích.
   Doporučujeme také evropským institucím zapojeným do trialogu, aby se zaměřily na spolehlivé zavedení mechanismu jednotného kontaktního místa (one-stop-shopu) pro účely vymáhání implementace GDPR přímo do nařízení samotného a pokud možno se tak vyhnuly zbytečným komplikacím vedoucím ke zvyšování právní nejistoty firem i občanů.

2. **Odklon od paušální sdílené odpovědnosti zpracovatele a správce údajů nebo jasné oddělení odpovědnosti zpracovatelů a správců osobních údajů**:
   Aktuální text návrhu GDPR tento požadavek bohužel nenaplňuje, neboť Evropská komise v článku 77 (tak, jak je formulován) navrhla a Rada EU s jistými změnami přijala zavedení mechanismu sdílené odpovědnosti správce a zpracovatele osobních údajů. SP ČR varuje před implementací tohoto návrhu do výsledné podoby GDPR, protože dle našeho názoru povede k další právní nejistotě: nebude totiž jasné, kdo je při zpracování údajů v dodavatelsko-odběratelských řetězcích za kterou činnost přímo zodpovědný. Takový stav pak bude znamenat zdlouhavá a nákladná soudní řízení, ohrožení ochrany soukromí občanů a zvýšení finanční a byrokratické zátěže podniků. Nevidíme přitom důvod k tomu, aby se měnila současná osvědčená dobře fungující evropská právní úprava, která odděluje role správce a zpracovatele údajů a definuje jejich vzájemnou odpovědnost prostřednictvím smluvního vztahu.

3. **Nastavení jasné vazby sankcí na závažnost a subjektivní stránku jednání, jímž došlo k porušení stanovených povinností stanovených:**
   Dalším sporným bodem GDPR je úprava sankcí za porušení povinností stanovených nařízením. Navrhované sankce GDPR se svou výší blíží sankcím ukládaným za porušení pravidel soutěžního práva. Mechanismus jejich ukládání a stanovení výše ze strany dozorujících orgánů v případě porušení povinností stanovených GDPR byl však měl být

stanoven jasně a transparentně. Výše sankce by měla být závislá na závažnosti zásahu do soukromí subjektu údajů a na formě jednání, délce trvání protiprávního jednání, a především potom na posouzení otázky, zda porušovatel jednal úmyslně či z pouhé nedbalosti. Také by se mělo vždy zohlednit, zda protiprávním jednáním došlo ke vzniku faktické škody v důsledku zásahu do soukromí u subjektů s chráněnými osobními údaji.

4. **Vynětí specifických přístupů ke koncovým zařízením uživatelů, u kterých nedochází k bezprostřednímu ohrožení bezpečnosti jejich údajů, z působnosti nařízení**:
   Návrh GDPR také nezohledňuje nejnovější trendy v oblasti poskytování cloudových služeb a technologických řešení, zejména tzv. vzdálených přístupů podpory (jedná se o přístup dodavatele případně správce IT systému). V dnešní době stále častěji nastává situace, kdy dodavatel IT řešení či větších IT celků poskytuje odběratelům, resp. správcům osobních údajů, servisní služby ve formě vzdálené podpory systémů, kontroly funkce systému, opravy chyb, apod. Účelem takovýchto služeb (nebo subdodávek služeb) není systematické zpracovávání osobních údajů (osobní údaje většinou ani neopouštějí systém nebo příslušné datové centrum), ale pouze vzdálená správa systému datového centra, pročež by mělo být dle našeho názoru jasně stanoveno, že tato aktivita není zpracováním osobních údajů ve smyslu GDPR.

5. **Uznání hodnoty pseudoanonymizovaných dat a jejich vynětí z působnosti nařízení:**
   Návrh GDPR nově rozšiřuje aplikaci právního rámce ochrany osobních údajů i na kategorii tzv. psedoanonymizovaných údajů, ačkoliv právní povaha těchto údajů není jasně definována. Bylo by velmi přínosné, pokud by GDPR pojem pseudoanonymizace jasně definovalo a charakterizovalo. Nakládání s řádně pseudoanonymizovanými údaji by pak mělo být vyňato z režimu GDPR, neboť jejich zpracováním nedochází k zásahu ani ohrožení soukromí subjektů údajů. Např. údaje uchovávané v datových centrech mají velikou vypovídající hodnotu a jejich zpracování v rámci technologií big data mohou poskytnout řadu statistických závěrů, avšak tato data by neměla být směšována s cíleným profilováním či sledováním osob. Za pseudoanonymizaci dat by měl primárně odpovídat správce, resp. měl by zajistit, že díky přijatým technickým a organizačním opatřením nemůže dojít k identifikaci subjektu údajů, tedy neoprávněnému zásahu do soukromí.