PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29

17/CS

WP 248 rev.01

Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679

Přijaté dne 4. dubna 2017

Přijaté dne 4. října 2017 v aktualizovaném znění

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán pro otázky ochrany údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Sekretariát poskytlo ředitelství C (Základní práva a občanství Unie) Evropské komise, Generální ředitelství pro spravedlnost, 1049 Brusel, Belgie, kancelář č. MO-59 03/075.

Webové stránky: http://ec.europa.eu/justice/data-protection/index_en.htm

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995,

s ohledem na články 29 a 30 uvedené směrnice,

s ohledem na svůj jednací řád,

PŘIJALA TYTO POKYNY:

Obsah

I. Úvod

Nařízení 2016/679[1] (obecné nařízení o ochraně osobních údajů) se použije ode dne 25. května 2018. V článku 35 obecného nařízení o ochraně osobních údajů se zavádí posouzení vlivu na ochranu osobních údajů[2]; stejný nástroj se zavádí i ve směrnici 2016/680[3].

Posouzení vlivu na ochranu osobních údajů je postup, jehož záměrem je popis zpracování údajů, posouzení jeho nezbytnosti a přiměřenosti a řízení rizik pro práva a svobody fyzických osob plynoucích ze zpracování osobních údajů[4], a to prostřednictvím jejich posouzení a stanovení opatření k jejich řešení. Posouzení vlivu na ochranu osobních údajů jsou důležitým nástrojem zajištění odpovědnosti, protože pomáhají správcům nejen plnit příslušné povinnosti obecného nařízení o ochraně osobních údajů, ale také doložit, že byla přijata příslušná opatření s cílem zajistit soulad s tímto nařízením (viz též článek 24)[5]. Jinými slovy **posouzení vlivu na ochranu osobních údajů je postup určený k zajištění a doložení souladu**.

Podle obecného nařízení o ochraně osobních údajů mohou za nesoulad s požadavky posouzení vlivu na ochranu osobních údajů ukládat příslušné dozorové úřady pokuty. Pokud v případech, kdy se na zpracování vztahuje povinnost provést posouzení vlivu na ochranu osobních údajů, není toto posouzení vlivu na ochranu osobních údajů provedeno (čl. 35 odst. 1 a 3–4), je provedeno nesprávně (čl. 35 odst. 2 a 7 až 9), nebo není předloženo příslušnému dozorovému úřadu ke konzultaci, přestože

---

[1] Nařízení Evropského parlamentu a Rady (EU) č. 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).

[2] V jiné souvislosti bývá často používán pojem „posouzení vlivu na soukromí“ (Privacy Impact Assessment), kterým se označuje totožný nástroj.

[3] V článku 27 směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů se rovněž uvádí, že posouzení vlivu na ochranu osobních údajů je třeba provést, „*[p]okud je pravděpodobné, že […] zpracování […] bude […] mít za následek vysoké riziko pro práva a svobody fyzických osob“*.

[4] V obecném nařízení o ochraně osobních údajů není pojem „posouzení vlivu na ochranu osobních údajů“ přímo definován, ale

- v čl. 35 odst. 7 se stanoví, jaké náležitosti musí přinejmenším splňovat:
  - „*a) systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce;*
  - *b) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;*
  - *c) posouzení rizik pro práva a svobody subjektů údajů uvedených v odstavci 1; a*
  - *d) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob*“;
- jeho význam a úloha jsou upřesněny v 84. bodě odůvodnění takto: „*S cílem přispět k zajištění souladu s tímto nařízením v případech, kdy je pravděpodobné, že operace zpracování budou představovat vysoké riziko pro práva a svobody fyzických osob, by měl být správce odpovědný za provedení posouzení vlivu na ochranu osobních údajů, aby vyhodnotil zejména původ, povahu, zvláštnost a závažnost tohoto rizika“*.

[5] Viz též 84. bod odůvodnění: „*Výsledek posouzení by měl být zohledněn při rozhodování o vhodných opatřeních, která by měla být přijata s cílem prokázat, že zpracování osobních údajů je v souladu s tímto nařízením*“.

to příslušná ustanovení (čl. 36 odst. 3 písm. e)) vyžadují, může být uložena správní pokuta do výše 10 milionů EUR, nebo jedná-li se o podnik, až do výše 2 % celkového ročního obratu celosvětově za předchozí rozpočtový rok, podle toho, co je vyšší.

II. Oblast působnosti pokynů

Tyto pokyny přihlíží k:

- prohlášení pracovní skupiny pro ochranu údajů zřízené podle článku 29 č. 14/EN WP 218[6],
- pokynům pracovní skupiny zřízené podle článku 29 č. 16/EN WP 243 týkajícím se pověřence pro ochranu osobních údajů[7],
- stanovisku pracovní skupiny zřízené podle článku 29 č. 13/EN WP 203 k účelu omezení[8],
- mezinárodním normám[9].

V souladu s přístupem založeným na rizicích obsaženém v obecném nařízení o ochraně osobních údajů není posouzení vlivu na ochranu osobních údajů nutné provádět při každém zpracování. Posouzení vlivu na ochranu osobních údajů se vyžaduje, pouze „[*p*]*okud je pravděpodobné, že […] zpracování […] bude […] mít za následek vysoké riziko pro práva a svobody fyzických osob“ (čl. 35 odst. 1). Aby byl* zajištěn soudržný výklad okolností, za nichž je provádění posouzení vlivu na ochranu osobních údajů povinné (čl. 35 odst. 3), stávající pokyny se nejprve snaží tento nástroj vyjasnit a stanovit kritéria pro seznamy, které má přijmout úřad pro ochranu osobních údajů podle čl. 35 odst. 4.

Podle čl. 70 odst. 1 písm. e) bude Evropský sbor pro ochranu osobních údajů moci vydávat pokyny, doporučení a osvědčené postupy, aby podporoval soudržné uplatňování obecného nařízení o ochraně osobních údajů. Účelem tohoto dokumentu je připravit se na budoucí činnost Evropského sboru pro ochranu osobních údajů a vyjasnit příslušná ustanovení obecného nařízení o ochraně osobních údajů, a tím pomoci správcům zajistit soulad s právními předpisy a poskytnout právní jistotu správcům, kteří musejí provádět posouzení vlivu na ochranu osobních údajů.

Tyto pokyny mají rovněž za cíl podpořit přípravu:

- společného seznamu operací zpracování Evropské unie, které podléhají požadavku na posouzení vlivu na ochranu osobních údajů (čl. 35 odst. 4),
- společného seznamu operací zpracování Evropské unie, u nichž se posouzení vlivu na ochranu osobních údajů nevyžaduje (čl. 35 odst. 5),

---

[6] Prohlášení pracovní skupiny zřízené podle článku 29 č. 14/EN WP 218 k úloze přístupu založeného na rizicích k právním rámcům pro ochranu údajů přijaté dne 30. května 2014.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] Pokyny pracovní skupiny zřízené podle článku 29 č. 16/EN WP 243 týkající se pověřence pro ochranu osobních údajů přijaté dne 13. prosince 2016.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] Stanovisko pracovní skupiny zřízené podle článku 29 č. 13/EN WP 203 k účelu omezení přijaté dne 2. dubna 2013.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] Např. ISO 31000:2009, *Řízení rizika – zásady a pokyny*, Mezinárodní organizace pro normalizaci (ISO); ISO/IEC 29134 (projekt), *Informační technologie – techniky zabezpečení – posouzení vlivu na soukromí – pokyny*, Mezinárodní organizace pro normalizaci (ISO).

- společných kritérií k metodice provádění posouzení vlivu na ochranu osobních údajů (čl. 35 odst. 5),
- společných kritérií, jež stanoví, kdy je třeba konzultovat dozorový úřad (čl. 36 odst. 1),
- doporučení, která budou případně vycházet ze zkušeností získaných v členských státech EU.

III. Posouzení vlivu na ochranu osobních údajů: výklad nařízení

Obecné nařízení o ochraně údajů ukládá správci povinnost zavést odpovídající opatření, aby zajistil a byl schopen doložit soulad s obecným nařízením o ochraně osobních údajů, přičemž přihlíží mimo jiné „k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob“ (čl. 24 odst. 1). Povinnost správců provést za určitých okolností posouzení vlivu na ochranu osobních údajů je třeba vnímat v rámci jejich obecné povinnosti vhodným způsobem řídit rizika[10] spojená se zpracováním osobních údajů.

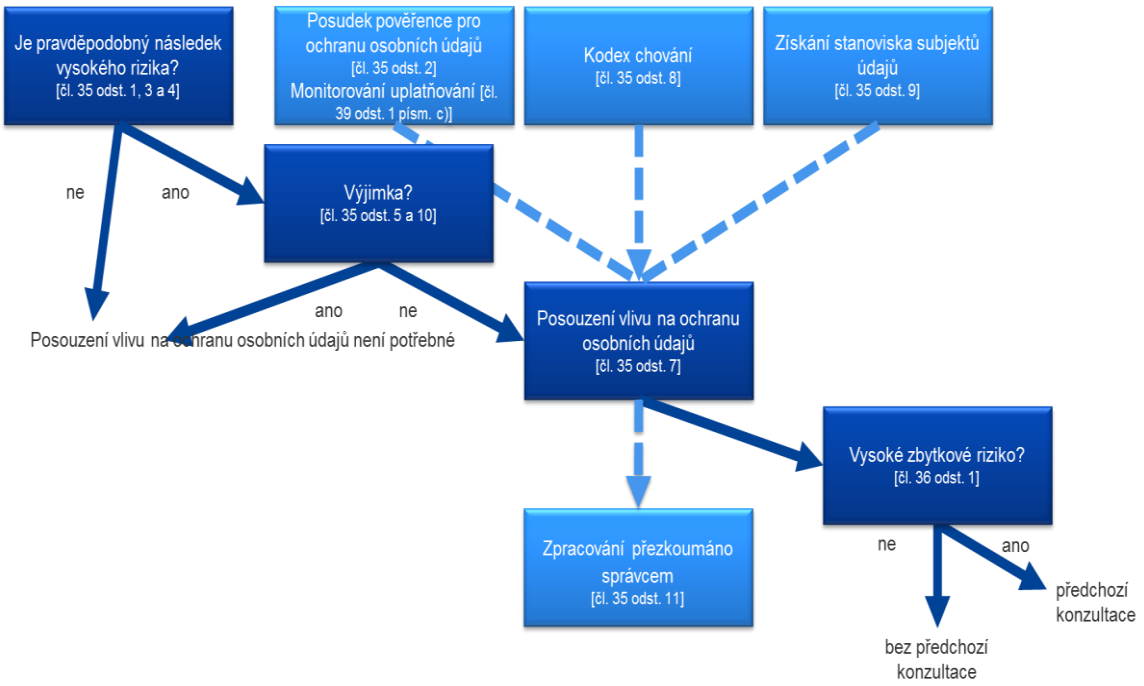
„Rizikem“ se rozumí scénář, v němž je uveden popis určité události a jejích důsledků společně s odhadem její závažnosti a pravděpodobnosti. „Řízení rizik“ je naproti tomu možné definovat jako soubor koordinovaných činností určených k řízení a omezení rizika v určité organizaci.

V článku 35 je odkaz na pravděpodobnost vysokého rizika „pro práva a svobody fyzických osob“. Jak je uvedeno v prohlášení pracovní skupiny pro ochranu údajů zřízené podle článku 29 k úloze přístupu založeného na rizicích k právním rámcům pro ochranu údajů, odkaz na „práva a svobody“ subjektů údajů se především týká práv na ochranu údajů a soukromí, může však také zahrnovat jiná základní práva, jako např. svobodu projevu, svobodu myšlení, svobodu pohybu, zákaz diskriminace, právo na svobodu, svědomí a náboženské vyznání.

V souladu s přístupem založeným na rizicích obsaženém v obecném nařízení o ochraně osobních údajů není posouzení vlivu na ochranu osobních údajů nutné provádět při každém zpracování. Namísto toho se posouzení vlivu na ochranu osobních údajů vyžaduje jen tehdy, je-li u určitého druhu zpracování „pravděpodobné, že […] bude mít za následek vysoké riziko pro práva a svobody fyzických osob“ (čl. 35 odst. 1). Pouhá skutečnost, že nebyly naplněny podmínky zakládající povinnost provádět posouzení vlivu na ochranu osobních údajů, však nesnižuje obecnou povinnost správců vhodným způsobem zvládat rizika pro práva a svobody subjektů údajů. V praxi to znamená, že správci musí soustavně vyhodnocovat rizika vznikající při činnostech zpracování, aby mohli stanovit, kdy je u určitého druhu zpracování „pravděpodobné, že [...] bude mít za následek vysoké riziko pro práva a svobody fyzických osob“.

[10] Je třeba zdůraznit, že řízení rizik pro práva a svobody fyzických osob vyžaduje, aby byl nejprve vypracován jejich výčet, proveden jejich rozbor, odhad, posouzení a aby byla řešena (např. snižována…) a pravidelně přezkoumávána. Správci nemohou uniknout své odpovědnosti tím, že pokryjí rizika pojistnými smlouvami.

Na následujícím obrázku jsou znázorněny základní principy související s posouzením vlivu na ochranu osobních údajů v obecném nařízení o ochraně osobních údajů:



A. <u>K čemu se posouzení vlivu na ochranu osobních údajů vztahuje? K jedné operaci zpracování údajů nebo k určitému souboru podobných operací zpracování.</u>

Posouzení vlivu na ochranu osobních údajů se může týkat jedné operace zpracování údajů. V čl. 35 odst. 1 se uvádí, že „*[p]ro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení*“. V 92. bodě odůvodnění se dodává, že „*[z]a určitých okolností může být přiměřené a účelné, aby byl předmět posouzení vlivu na ochranu osobních údajů širší a nevztahoval se pouze na jeden projekt, například když orgány veřejné moci nebo veřejné subjekty mají v úmyslu vytvořit společnou aplikaci nebo platformu zpracování, nebo když několik správců hodlá zavést společnou aplikaci nebo zpracovatelské prostředí pro celé průmyslové odvětví nebo pro určitý segment nebo pro široce užívanou horizontální činnost*“.

Jedno posouzení vlivu na ochranu osobních údajů může být použito k posouzení více operací zpracování, které jsou podobné, pokud jde o povahu, rozsah, kontext, účel zpracování a rizika. Posouzení vlivu na ochranu osobních údajů se zaměřují na systematické zkoumání nových situací, které mohou mít za následek vysoká rizika pro práva a svobody fyzických osob, a není třeba provádět posouzení vlivu na ochranu osobních údajů v případech (tj. operacích zpracování provedených v konkrétním kontextu za určitým účelem), které byly již studovány. Tak tomu může být v případech, kdy jsou použity podobné technologie ke sběru stejného druhu údajů za stejným účelem. Například skupina obecních orgánů, z nichž každý zavádí podobný uzavřený televizní okruh (CCTV), by mohla provést jediné posouzení vlivu na ochranu osobních údajů zahrnující zpracování těmito samostatnými správci, nebo provozovatel železnice (jediný správce) by mohl provést jediné posouzení vlivu na ochranu osobních údajů pro dohled pomocí videokamer na všech vlakových nádražích. To se může vztahovat i na podobné operace zpracování prováděné různými správci údajů. V těchto případech by mělo být posouzení vlivu na ochranu osobních údajů sdíleno nebo by mělo být veřejně přístupné,

opatření popsaná v posouzení vlivu na ochranu osobních údajů musí být provedena a je třeba uvést odůvodnění pro jediné posouzení vlivu na ochranu osobních údajů.

Pokud jsou pro operace zpracování stanoveni společní správci, je třeba, aby byly jejich příslušné povinnosti přesně vymezeny. Jejich posouzení vlivu na ochranu osobních údajů by měla uvádět, která ze stran je odpovědná za jednotlivá opatření určená k řešení rizik a k ochraně práv a svobod subjektů údajů. Každý správce údajů by měl vyjádřit své potřeby a sdílet důležité informace, aniž by vyzradil tajné informace (jako je např.: ochrana obchodního tajemství, duševního vlastnictví, důvěrné obchodní informace) nebo zveřejnil slabá místa.

Posouzení vlivu na ochranu osobních údajů lze rovněž použít pro hodnocení vlivu technologického produktu na ochranu údajů, například určitého hardwaru nebo softwaru, pokud je pravděpodobné, že tento produkt budou používat různí správci údajů pro různé operace zpracování. Správce údajů, který zavádí určitý produkt, má ovšem i nadále povinnost provést vlastní posouzení vlivu na ochranu osobních údajů, může však případně čerpat informace z posouzení vlivu na ochranu osobních údajů vypracovaného poskytovatelem produktu. Jako příklad může sloužit vztah mezi výrobcem inteligentních měřicích přístrojů a společnostmi veřejných služeb. Každý poskytovatel produktu nebo zpracovatel by měl sdílet užitečné informace, aniž by vyzradil tajné informace nebo způsobil riziko pro zabezpečení tím, že by zveřejnil slabá místa.

B. Které operace zpracování podléhají posouzení vlivu na ochranu osobních údajů? Kromě výjimek, kdy je „*pravděpodobné, že budou mít za následek vysoké riziko*“.

V tomto oddíle je popsáno, kdy je posouzení vlivu na ochranu osobních údajů povinné, a kdy povinnost provést posouzení vlivu na ochranu osobních údajů nevzniká.

Pokud se na operaci zpracování nevztahuje některá z výjimek (III.B.a), je nutné provést posouzení vlivu na ochranu osobních údajů, pokud je u operace zpracování „*pravděpodobné, že* bude *mít za následek vysoké riziko*“ (III.B.b).

a) Kdy je posouzení vlivu na ochranu osobních údajů povinné? Pokud je u určitého zpracování „*pravděpodobné, že bude mít za následek vysoké riziko*“.

Obecné nařízení o ochraně osobních údajů nestanoví, aby bylo posouzení vlivu na ochranu osobních údajů prováděno pro každou operaci zpracování, která by mohla mít za následek rizika pro práva a svobody fyzických osob. Povinnost provést posouzení vlivu na ochranu osobních údajů vzniká, pouze „*[p]okud je pravděpodobné, že […] zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob“ (čl. 35 odst. 1, názorně vysvětleno v čl. 35 odst. 3 a doplněno v čl. 35 odst. 4). To je zvlášť důležité, pokud se zavádí nové technologie na zpracování údajů*[11].

V případech, kdy není zřejmé, zda vzniká povinnost provést posouzení vlivu na ochranu osobních údajů, pracovní skupina zřízená podle článku 29 doporučuje, aby bylo přesto posouzení vlivu na ochranu osobních údajů provedeno, protože posouzení vlivu na ochranu osobních údajů je užitečný nástroj, který pomůže správcům zajistit soulad s právními předpisy v oblasti ochrany údajů.

[11] Pro další příklady viz body odůvodnění 89, 91 a čl. 35 odst. 1 a 3.

I když povinnost provést posouzení vlivu na ochranu osobních údajů může vzniknout i za jiných okolností, v čl. 35 odst. 3 jsou uvedeny některé příklady, kdy je pravděpodobné, že operace zpracování „*bude … mít za následek vysoké riziko*“:

- „*a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad*[12]*;*
- *b) rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10*[13]*; nebo*
- *c) rozsáhlé systematické monitorování veřejně přístupných prostorů*“.

Jak vyplývá ze slova „*zejména*“ v návětí čl. 35 odst. 3 obecného nařízení o ochraně osobních údajů, jedná se o demonstrativní seznam. Může existovat „vysoké riziko“ operací zpracování, které nejsou v tomto výčtu uvedeny, a přesto mohou představovat podobně vysoká rizika. Na tyto operace zpracování by se rovněž měla vztahovat povinnost provádět posouzení vlivu na ochranu osobních údajů. Z tohoto důvodu níže uvedená kritéria občas přesahují pouhé vysvětlení toho, co by tři příklady uvedené v čl. 35 odst. 3 obecného nařízení o ochraně osobních údajů měly znamenat.

Aby byl stanoven konkrétnější soubor operací zpracování, u nichž je uložena povinnost posouzení vlivu na ochranu osobních údajů kvůli jejich vysokému riziku, s přihlédnutím ke zvláštním prvkům čl. 35 odst. 1 a čl. 35 odst. 3 písm. a) až c), seznamu, který má být přijat na vnitrostátní úrovni podle čl. 35 odst. 4) a podle bodů odůvodnění 71, 75 a 91, a k dalším odkazům v obecném nařízení o ochraně osobních údajů na operace zpracování, u nichž „*je pravděpodobné, že [...] [budou] mít za následek vysoké riziko*“[14]*, je třeba zvážit těchto devět kritérií.*

1. Hodnocení nebo bodování, včetně profilování a předpovídání, zejména z *„aspektů souvisejících s pracovním výkonem subjektu údajů, jeho ekonomickou situací, zdravotním stavem, osobními preferencemi nebo zájmy, spolehlivostí nebo chováním, místem pobytu či pohybu“* (71. a 91. bod odůvodnění). Může se jednat například o finanční instituci, která prověřuje svého zákazníka v databázi úvěrových referencí nebo v databázi pro boj proti praní peněz a financování terorismu či podvodům, nebo biotechnologickou společnost, která nabízí genetické testování přímo spotřebitelům za účelem posouzení nebo předpovězení rizika nemoci / zdravotních rizik, nebo společnost, která vytváří behaviorální nebo marketingové profily na základě používání webových stránek nebo pohybu na nich.
2. Automatizované rozhodování, které má právní nebo podobně závažný dopad: zpracování, jehož cílem je rozhodování o subjektech údajů, jež má „*ve vztahu k fyzickým osobám právní účinky*“ nebo má „*na fyzické osoby podobně závažný dopad*“ (čl. 35 odst. 3 písm. a)). Např. zpracování může mít za následek vyloučení nebo diskriminaci jednotlivců. Na zpracování,

[12] Viz 71. bod odůvodnění: „*kdy jsou za účelem vytvoření či využití osobních profilů vyhodnocovány osobní aspekty, zejména prostřednictvím analýzy a odhadu aspektů týkajících se pracovních výsledků, ekonomické situace, zdravotního stavu, osobních preferencí nebo zájmů, spolehlivosti nebo chování, místa pobytu nebo pohybu“*.

[13] Viz 75. bod odůvodnění: „*kdy jsou zpracovávány osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filosofickém přesvědčení nebo členství v odborech, kdy jsou zpracovávány genetické údaje či údaje o zdravotním stavu či sexuálním životě nebo odsouzení v trestních věcech a trestných činů či souvisejících bezpečnostních opatřeních*“.

[14] Viz např. 75., 76., 92., 116. bod odůvodnění.

které má jen nepatrný nebo žádný dopad na jednotlivce, se toto konkrétní kritérium nevztahuje. Další vysvětlení těchto pojmů bude obsahem připravovaných pokynů pracovní skupiny zřízené podle článku 29 k profilování.

3. Systematické monitorování: zpracování, které je používáno k pozorování, monitorování nebo kontrole subjektů údajů, včetně údajů shromážděných prostřednictvím sítí nebo „*rozsáhlé systematické monitorování veřejně přístupných prostorů*“ (čl. 35 odst. 3 písm. c))[15]. Tento druh monitorování je jedním z kritérií, protože osobní údaje mohou být shromažďovány za okolností, za nichž nemusí subjekty údajů vědět, kým jsou jejich údaje shromažďovány a jak budou použity. Navíc nemusí být v silách jednotlivců zabránit tomu, aby se stali subjektem tohoto zpracování na veřejných (nebo veřejně přístupných) místech.
4. Citlivé údaje nebo údaje vysoce osobní povahy: sem spadají i zvláštní kategorie osobních údajů ve smyslu článku 9 (např. údaje týkající se politických názorů jedince), stejně jako osobní údaje týkající se rozsudků v trestních věcech a trestných činů ve smyslu článku 10. Jako příklad může sloužit zdravotnická dokumentace uchovávaná ve všeobecné nemocnici nebo podrobné údaje vedené soukromým vyšetřovatelem vůči pachateli. Kromě těchto ustanovení obecného nařízení o ochraně osobních údajů mohou zvyšovat možné riziko pro práva a svobody jednotlivců některé další kategorie údajů. Tyto osobní údaje jsou považovány za citlivé (v běžném smyslu toho slova), protože mají vazbu na domácnosti a soukromé činnosti (jako např. elektronické komunikace, jejichž důvěrný charakter by měl být chráněn) nebo protože mají dopad na výkon základních práv (např. lokalizační údaje, jejichž shromažďování zpochybňuje svobodu pohybu) nebo proto, že jejich porušení má jednoznačně závažný vliv na každodenní život subjektu údajů (např. finanční údaje, které by mohly vést k podvodům s platbami). V tomto ohledu může být důležité, zda subjekt údajů nebo třetí osoby údaje už zveřejnily. Skutečnost, že osobní údaje jsou veřejně dostupné, může být považována za jeden z faktorů při posouzení, zda se počítalo s dalším využitím údajů. Toto kritérium může zahrnovat také údaje, jako jsou např. osobní dokumenty, e-maily, osobní deníky, elektronická čtecí zařízení vybavená funkcemi poznámek a informace velmi osobní povahy obsažené v aplikacích zaznamenávajících průběh denních aktivit subjektu údajů (tzv. „lifelog“).
5. Údaje zpracovávané v rozsáhlém měřítku: obecné nařízení o ochraně osobních údajů přesně nevymezuje, co znamená rozsáhlé, i když 91. bod odůvodnění určité vodítko poskytuje. Pracovní skupina zřízená podle článku 29 v každém případě doporučuje, aby při určování, zda je zpracování rozsáhlé, byly zvažovány zejména tyto faktory[16]:
    a. počet dotčených subjektů údajů vyjádřený konkrétním číslem, nebo jako podíl příslušné populace;
    b. objem údajů a/nebo rozsah jednotlivých zpracovávaných údajů;

[15] Podle výkladu pracovní skupiny zřízené podle článku 29 se za „*systematickou*“ označuje činnost, která splňuje jeden nebo více z těchto předpokladů (viz Pokyny pracovní skupiny zřízené podle článku 29 č. 16/EN WP 243 týkající se pověřence pro ochranu osobních údajů):

- řídí se určitým systémem,
- je předem naplánovaná, organizovaná nebo metodická,
- probíhá v rámci obecného plánu pro sběr údajů,
- je prováděna v rámci strategie.

Podle výkladu pracovní skupiny zřízené podle článku 29 se za „*veřejně přístupné prostory“ považuje jak*ékoli místo přístupné široké veřejnosti, jako např. náměstí, nákupní středisko, ulice, tržiště, vlakové nádraží nebo veřejná knihovna.

[16] Viz Pokyny pracovní skupiny zřízené podle článku 29 č. 16/EN WP 243 týkající se pověřence pro ochranu osobních údajů.

c. délka nebo trvání činnosti zpracování údajů;
d. zeměpisný rozsah činnosti zpracování.

6. Přiřazování nebo slučování datových souborů, pokud například pocházejí ze dvou nebo více operací zpracování údajů prováděných pro různé účely a/nebo různými správci údajů způsobem, který by přesahoval přiměřené očekávání subjektu údajů[17].
7. Údaje týkající se zranitelných subjektů údajů (75. bod odůvodnění): zpracování tohoto druhu údajů je jedním z kritérií kvůli větší nerovnováze moci mezi subjekty údajů a správcem údajů, což znamená, že pro jednotlivce může být nemožné snadno vyslovit souhlas případně nesouhlas se zpracováním svých údajů, nebo vykonávat svá práva. Mezi zranitelné subjekty mohou patřit děti (u nichž lze mít za to, že nejsou schopny vědomě nebo promyšleně vyslovit nesouhlas popřípadě souhlas se zpracováním svých údajů), zaměstnanci, zranitelnější skupiny obyvatelstva, které vyžadují zvláštní ochranu (osoby s duševní chorobou, žadatelé o azyl nebo starší osoby, pacienti atd.) a všichni ti, v jejichž případech je možné stanovit nerovnováhu ve vztahu mezi postavením subjektu údajů a správce.
8. Nové použití nebo využití nových technologických nebo organizačních řešení, jako např. kombinace použití otisků prstů a rozpoznávání obličejů pro zlepšení omezení fyzického přístupu atd. Obecné nařízení o ochraně osobních údajů upřesňuje (čl. 35 odst. 1 a 89. a 91. bod odůvodnění), že použití nové technologie, definované v „*souladu s dosaženou úrovní technických znalostí*“ (91. bod odůvodnění), může zakládat potřebu provést posouzení vlivu na ochranu osobních údajů. Použití této technologie totiž může zahrnovat nové formy sběru a použití údajů s potenciálně vysokým rizikem pro práva a svobody fyzických osob. Osobní a sociální důsledky zavedení nové technologie mohou být nepředvídatelné. Posouzení vlivu na ochranu osobních údajů pomůže správci údajů porozumět těmto rizikům a řešit je. Například některé aplikace „internetu věcí“ mohou mít významný vliv na každodenní život a soukromí jednotlivců; a proto je třeba provést posouzení vlivu na ochranu osobních údajů.
9. Pokud samotné zpracování *„brání subjektům údajů v uplatňování některého z jejich práv nebo v používání některé služby či smlouvy“* (článek 22 a 91. bod odůvodnění). Sem se řadí operace zpracování, které mají za cíl umožnit, změnit nebo zamezit subjektu údajů přístup ke službě nebo uzavření smlouvy. Může se jednat například o banku, která prověřuje svého zákazníka v databázi úvěrových referencí, aby rozhodla, zda mu udělí úvěr, či nikoli.

Ve většině případů může správce údajů zpracování, které splňuje dvě kritéria, považovat za zpracování, pro něž se vyžaduje posouzení vlivu na ochranu osobních údajů. Pracovní skupina zřízená podle článku 29 se obecně domnívá, že čím více kritérií zpracování splňuje, tím větší je pravděpodobnost, že bude představovat vysoké riziko pro práva a svobody subjektů údajů, a bude proto vyžadovat posouzení vlivu na ochranu osobních údajů, a to bez ohledu na opatření, která hodlá správce přijmout.

Avšak v některých případech **správce údajů může mít za to, že posouzení vlivu na ochranu osobních údajů vyžaduje i zpracování, které splňuje jen jedno z těchto kritérií.**

Příklady uvedené v tabulce ukazují, jak by měla být používána kritéria k posouzení, zda určitá operace zpracování vyžaduje posouzení vlivu na ochranu osobních údajů:

[17] Viz vysvětlení ve stanovisku pracovní skupiny zřízené podle článku 29 č. 13/EN WP 203 k účelu omezení, s. 24.

Příklady zpracování	Případná důležitá kritéria	Je pravděpodobné, že bude zapotřebí provést posouzení vlivu na ochranu osobních údajů?
Nemocnice zpracovávající zdravotnické a genetické údaje svého pacienta (nemocniční informační systém).	- Citlivé údaje nebo údaje vysoce osobní povahy. - Údaje týkající se zranitelných subjektů údajů. - Údaje zpracovávané v rozsáhlém měřítku.	ano
Použití kamerového systému pro monitorování chování řidičů na silnicích. Správce hodlá použít inteligentní systém analýzy obrazového záznamu k identifikaci vozidel a automatickému rozpoznávání státních poznávacích značek.	- Systematické monitorování. - Nové použití nebo využití technologických nebo organizačních řešení.	
Společnost systematicky monitoruje činnost svých zaměstnanců, včetně monitorování pracovních stanic zaměstnanců, jejich činnosti na internetu atd.	- Systematické monitorování. - Údaje týkající se zranitelných subjektů údajů.	
Shromažďování veřejně dostupných údajů ze sociálních médií pro vytváření profilů.	- Hodnocení nebo bodování. - Údaje zpracovávané v rozsáhlém měřítku. - Přiřazování nebo slučování datových souborů. - Citlivé údaje nebo údaje vysoce osobní povahy	
Instituce vytvářející databázi úvěrového hodnocení nebo podvodů na vnitrostátní úrovni.	- Hodnocení nebo bodování. - Automatizované rozhodování, které má právní nebo podobně závažný dopad. - Zabraňuje subjektu údajů ve výkonu práva nebo využívání služby či uzavření smlouvy. - Citlivé údaje nebo údaje vysoce osobní povahy	
Uložení pseudonymizovaných osobních citlivých údajů týkajících se zranitelných subjektů údajů získaných v rámci výzkumných projektů nebo klinických hodnocení za účelem archivování.	- Citlivé údaje. - Údaje týkající se zranitelných subjektů údajů. - Zabraňuje subjektu údajů ve výkonu práva nebo využívání služby či uzavření smlouvy.	
Zpracování „osobních údajů pacientů nebo klientů jednotlivými lékaři, zdravotníky nebo	- Citlivé údaje nebo údaje vysoce osobní povahy.	ne

Příklady zpracování	Případná důležitá kritéria	Je pravděpodobné, že bude zapotřebí provést posouzení vlivu na ochranu osobních údajů?
právníky" (91. bod odůvodnění).	- Údaje týkající se zranitelných subjektů údajů.	
Internetový časopis, který používá distribuční seznam pro zasílání obecného denního přehledu svým odběratelům.	- Údaje zpracovávané v rozsáhlém měřítku.	
Webové stránky elektronického obchodu zobrazující reklamy na náhradní díly do automobilových veteránů využívající omezené profilování na základě zboží zobrazovaného nebo zakoupeného na této webové stránce.	- Hodnocení nebo bodování.	

Naproti tomu operace zpracování může odpovídat některému z výše uvedených případů a správce přitom nemusí dospět k názoru, že „je pravděpodobné, že zpracování […] bude […] mít za následek vysoké riziko pro práva a svobody fyzických osob". V těchto případech by měl správce odůvodnit a zdokumentovat důvody, proč nebude provedeno posouzení vlivu na ochranu osobních údajů, a měl by připojit/zaznamenat názor pověřence pro ochranu osobních údajů.

Kromě toho v souladu se zásadou odpovědnosti každý správce údajů „*vede záznamy o činnostech zpracování, za něž odpovídá*", včetně mimo jiné účelu zpracování, popisu kategorií údajů a příjemců údajů a „*je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1*" (čl. 30 odst. 1), přičemž musí posoudit, zda v případě, že se rozhodne neprovést posouzení vlivu na ochranu osobních údajů, je pravděpodobnost vysokého rizika.

Pozn.: dozorové úřady mají povinnost sestavit a zveřejnit seznam druhů operací zpracování, které podléhají požadavku na posouzení vlivu na ochranu osobních údajů, a informovat o něm Evropský sbor pro ochranu osobních údajů (čl. 35 odst. 4)[18]. Výše stanovená kritéria mohou pomoci dozorovým úřadům při sestavení tohoto seznamu tím, že včas doplní případný konkrétnější obsah. Například jakékoli zpracování biometrických údajů nebo údajů dětí by také mohlo být považováno za významné z hlediska sestavení seznamu podle čl. 35 odst. 4.

b) Kdy se posouzení vlivu na ochranu osobních údajů nevyžaduje? Pokud není u daného zpracování „pravděpodobné, *že […] bude […] mít za následek vysoké riziko pro práva a svobody fyzických osob*", nebo pokud existuje podobné posouzení vlivu na ochranu

[18] V této souvislosti „*příslušný dozorový úřad [použije] mechanismus jednotnosti uvedený v článku 63, pokud tyto seznamy zahrnují činnosti zpracování související s nabídkou zboží či služeb subjektům údajů nebo s monitorováním jejich chování v několika členských státech, nebo jestliže dané seznamy mohou výrazně ovlivnit volný pohyb osobních údajů v rámci Unie*" (čl. 35 odst. 6).

osobních údajů, nebo pokud bylo schváleno před květnem 2018, nebo má právní základ, nebo je uvedeno na seznamu operací zpracování, které nepodléhají požadavku posouzení vlivu na ochranu osobních údajů.

Pracovní skupina zřízená podle článku 29 se domnívá se, že posouzení vlivu na ochranu osobních údajů není nutné v těchto případech:

- **pokud není u daného zpracování „*pravděpodobné, že [...] bude […] mít za následek vysoké riziko pro práva a svobody fyzických osob*"** (čl. 35 odst. 1),
- **pokud povaha, rozsah, kontext a účel zpracování jsou velmi podobné zpracování, pro které bylo posouzení vlivu na ochranu osobních údajů už provedeno**. V těchto případech je možné použít výsledky posouzení vlivu na ochranu osobních údajů pro podobné zpracování (čl. 35 odst. 1[19]),
- pokud operace zpracování zkontroloval dozorový úřad před květnem 2018 za konkrétních podmínek, které se nezměnily[20] (viz III.C),
- **pokud má zpracování** podle čl. 6 odst. 1 písm. c) nebo e) **právní základ** v právu EU nebo členského státu, pokud toto právo upravuje konkrétní operaci zpracování **a pokud bylo posouzení vlivu na ochranu osobních údajů již provedeno** v souvislosti s přijetím uvedeného právního základu (čl. 35 odst. 10)[21], ledaže by členský stát prohlásil, že považuje provedení tohoto posouzení vlivu na ochranu osobních údajů před činnostmi zpracování za nezbytné,
- **pokud je zpracování uvedeno na nepovinném seznamu operací zpracování (sestaveném dozorovým úřadem)**, u nichž není posouzení vlivu na ochranu osobních údajů nutné (čl. 35 odst. 5). Tento seznam může obsahovat činnosti zpracování, které splňují podmínky stanovené tímto úřadem, zejména prostřednictvím pokynů, konkrétních rozhodnutí nebo povolení, pravidel pro zajištění souladu atd. (např. ve Francii se jedná o povolení, výjimky, zjednodušená pravidla, soubory opatření pro zajištění souladu…). V takových případech, jež podléhají přezkoumání příslušným dozorovým úřadem, se posouzení vlivu na ochranu osobních údajů nevyžaduje, avšak jen za předpokladu, že zpracování spadá důsledně do rozsahu příslušných postupů uvedených v seznamu a že nadále splňuje veškeré příslušné požadavky obecného nařízení o ochraně osobních údajů.

C. Jak je tomu v případě už existujících operací zpracování? Posouzení vlivu na ochranu osobních údajů jsou za určitých okolností vyžadována.

Požadavek na provedení posouzení vlivu na ochranu osobních údajů se vztahuje na stávající operace zpracování, u nichž je pravděpodobné, že zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, a u kterých došlo ke změně rizik s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování.

---

[19] „*Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení*".

[20] „*Přijatá rozhodnutí Komise a schválení dozorových úřadů vycházející ze směrnice 95/46/ES by měla zůstat v platnosti, dokud nebudou změněna, nahrazena nebo zrušena*" (171. bod odůvodnění).

[21] Pokud se posouzení vlivu na ochranu osobních údajů provádí ve fázi přípravy právních předpisů, jež tvoří právní základ zpracování, bude pravděpodobně třeba před zahájením operací provést přezkum, protože přijaté právní předpisy se mohou lišit od návrhů způsobem, který může mít vliv na oblast ochrany soukromí a údajů. Kromě toho technické podrobnosti o skutečném zpracování, které byly k dispozici v době přijetí právních předpisů, nemusí být dostatečné, třebaže ke zpracování bylo vypracováno posouzení vlivu na ochranu osobních údajů. V těchto případech může být před provedením vlastních činností zpracování třeba provést konkrétní posouzení vlivu na ochranu osobních údajů.

Posouzení vlivu na ochranu osobních údajů se nevyžaduje u operací zpracování, které prošly kontrolou dozorového úřadu nebo osoby pověřené ochranou údajů podle článku 20 směrnice 95/46/ES a které jsou prováděny způsobem, jenž se od předchozí kontroly nezměnil. V nařízení se totiž stanoví: „*[p]řijatá rozhodnutí Komise a schválení dozorových úřadů vycházející ze směrnice 95/46/ES by měla zůstat v platnosti, dokud nebudou změněna, nahrazena nebo zrušena"* (171. bod odůvodnění).

To analogicky znamená, že každé zpracování údajů, u něhož dojde ke změně podmínek provádění (rozsahu, účelu, shromážděných osobních údajů, totožnosti správce údajů nebo příjemců, období uchovávání dat, technických a organizačních opatření atd.) od předchozí kontroly provedené dozorovým úřadem nebo osobou pověřenou ochranou údajů a u něhož je pravděpodobné, že bude mít za následek vysoké riziko, by mělo podléhat posouzení vlivu na ochranu osobních údajů.

Kromě toho posouzení vlivu na ochranu osobních údajů může být vyžadováno, jakmile dojde ke změně rizik, která jsou důsledkem operací zpracování[22], například z důvodu zahájení využívání nové technologie, nebo proto, že došlo ke změně účelu využívání osobních údajů. Operace zpracování údajů se mohou vyvíjet rychle a mohou vznikat nová slabá místa. Proto je třeba konstatovat, že revize posouzení vlivu na ochranu osobních údajů není užitečná jen s ohledem na soustavné zlepšování, ale má rovněž zásadní význam pro udržení úrovně ochrany údajů v postupně se měnícím prostředí. Posouzení vlivu na ochranu osobních údajů může být rovněž potřebné z důvodu změny organizačního nebo společenského kontextu činnosti zpracování, např. protože účinky některých automatizovaných rozhodnutí nabyly na významu nebo protože dojde k ohrožení nových kategorií subjektů údajů diskriminací. Každý z těchto příkladů může být jedním z činitelů, který má za následek změnu rizika vyplývající z příslušné činnosti zpracování.

Naproti tomu určité změny mohou rovněž riziko snižovat. Například operace zpracování se mohou změnit tak, že rozhodnutí už nejsou automatizovaná nebo monitorování už není systematické. V tomto případě může z provedeného přezkumu analýzy rizika vyplynout závěr, že provedení posouzení vlivu na ochranu osobních údajů už není potřebné.

V rámci osvědčených postupů **by mělo být posouzení vlivu na ochranu osobních údajů soustavně přezkoumáváno a mělo by se pravidelně přehodnocovat**. Takže i když se ke dni 25. května 2018 posouzení vlivu na ochranu osobních údajů nevyžaduje, správce bude ve vhodnou dobu nucen toto posouzení vlivu na ochranu osobních údajů provést v rámci svých povinností obecné odpovědnosti.

D. Jak provést posouzení vlivu na ochranu osobních údajů?

a) Kdy by mělo být posouzení vlivu na ochranu osobních údajů provedeno? Před zpracováním.

Posouzení vlivu na ochranu osobních údajů by mělo být prováděno „*před zpracováním*" (čl. 35 odst. 1 a čl. 35 odst. 10, 90. a 93. bod odůvodnění)[23]. Je to v souladu se zásadami záměrné a

[22] A to s ohledem na kontext, shromážděné údaje, účel, funkce, zpracovávané osobní údaje, příjemce, slučování údajů, rizika (podpůrný kapitál, zdroje rizik, možné dopady, hrozby atd.), bezpečnostní opatření a mezinárodní převody.

[23] Kromě případů, kdy se jedná o již probíhající zpracování, které bylo předmětem předchozí kontroly dozorového úřadu – v tomto případě se posouzení vlivu na ochranu osobních údajů provádí předtím, než dojde k nějaké významné změně v procesu zpracování.

standardní ochrany osobních údajů (článek 25 a 78. bod odůvodnění). Posouzení vlivu na ochranu osobních údajů by mělo být vnímáno jako nástroj usnadňující rozhodování v oblasti zpracování.

Posouzení vlivu na ochranu osobních údajů by mělo být zahájeno, co nejdříve je to možné, v rámci přípravy koncepce operací zpracování, třebaže zatím nejsou všechny operace zpracování známé. Projekt průběžného aktualizování posouzení vlivu na ochranu osobních údajů během životního cyklu zajistí, že bude zohledňována ochrana údajů a soukromí a že budu podporována taková řešení, která budou příznivá pro zajištění souladu s nařízením. Může být rovněž nutné v průběhu vývoje procesu jednotlivé kroky hodnocení opakovat, protože volba určitých technických nebo organizačních opatření může mít vliv na závažnost nebo pravděpodobnost rizik, která ze zpracování vyplývají.

Skutečnost, že posouzení vlivu na ochranu osobních údajů může vyžadovat aktualizaci, jakmile je zahájeno vlastní zpracování, není platný důvod pro odklad nebo neprovedení posouzení vlivu na ochranu osobních údajů. Posouzení vlivu na ochranu osobních údajů je trvalý proces, zejména v případě dynamických operací zpracování, které se soustavně mění. **Provedení posouzení vlivu na ochranu osobních údajů je neustálý – a nikoli jednorázový – proces**.

b) Kdo je povinen provést posouzení vlivu na ochranu osobních údajů? Správce společně s pověřencem pro ochranu osobních údajů a zpracovateli.

Správce odpovídá za zajištění posouzení vlivu na ochranu osobních údajů (čl. 35 odst. 2). Posouzení vlivu na ochranu osobních údajů může provést někdo jiný – ať už někdo v rámci organizace, či vně organizace – konečnou odpovědnost za plnění úkolu však nese správce.

Správce si musí rovněž vyžádat posudek pověřence pro ochranu osobních údajů, byl-li jmenován (čl. 35 odst. 2), přičemž tyto posudky i rozhodnutí přijatá správcem by měly být zdokumentovány v posouzení vlivu na ochranu osobních údajů. Pověřenec pro ochranu osobních údajů by měl rovněž monitorovat uplatňování posouzení vlivu na ochranu osobních údajů (čl. 39 odst. 1 písm. c)). Podrobnější údaje jsou uvedeny v Pokynech pracovní skupiny zřízené podle článku 29 č. 16/EN WP 243 týkajících se pověřence pro ochranu osobních údajů.

Pokud zpracování provádí zcela nebo zčásti zpracovatel údajů, **zpracovatel by měl pomoci správci při provedení posouzení vlivu na ochranu osobních údajů** a poskytnout veškeré potřebné informace (podle čl. 28 odst. 3 písm. f)).

Správce musí „*ve vhodných případech [získat] […] stanovisko subjektů údajů nebo jejich zástupců*“ *(čl. 35 odst. 9)*. Pracovní skupina zřízená podle článku 29 se domnívá, že:

- tato stanoviska lze v závislosti na kontextu získat různými prostředky (např. prostřednictvím obecné studie související s účelem a prostředky operace zpracování, otázky položené zástupcům zaměstnanců nebo obvyklého průzkumu zaslaného budoucím zákazníkům správce údajů), přičemž je třeba mít jistotu, že správce se při zpracování veškerých osobních údajů v souvislosti se získáním tohoto stanoviska opírá o právní základ. I když je třeba poznamenat, že souhlas se zpracováním není samozřejmě způsob, jak získat stanovisko subjektů údajů,
- jestliže se konečné rozhodnutí správce údajů liší od stanoviska subjektů údajů, je třeba důvody dalšího postupu zdokumentovat,
- správce by měl rovněž zdokumentovat své odůvodnění, proč nezískal stanovisko subjektů údajů, jestliže se rozhodne, že získání stanoviska není vhodné, např. pokud by tím byla

ohrožena důvěrná povaha podnikatelských plánů společnosti nebo pokud by to bylo nepřiměřené či neproveditelné.

Ostatně představuje správnou praxi definovat a zdokumentovat další konkrétní úlohy a odpovědnosti v závislosti na vnitřních zásadách, procesech a pravidlech, např.:

- pokud konkrétní podnikatelské jednotky mohou navrhnout, že provedou posouzení vlivu na ochranu osobních údajů, tyto jednotky by pak měly poskytnout podklady pro posouzení vlivu na ochranu osobních údajů a měly by se podílet na procesu ověřování posouzení vlivu na ochranu osobních údajů,
- ve vhodných případech se doporučuje získat stanovisko nezávislých odborníků z různých oborů[24] (právníků, odborníků na informační technologie, bezpečnostních odborníků, sociologů, odborníků na etiku atd.),
- úlohy a povinnosti zpracovatelů musí být smluvně stanoveny a posouzení vlivu na ochranu osobních údajů se provádí s pomocí zpracovatele, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici (čl. 28 odst. 3 písm. f)),
- hlavní pověřenec pro bezpečnost informačních systémů, pokud je jmenován, a pověřenec pro ochranu osobních údajů mohou navrhnout, aby správce provedl posouzení vlivu na ochranu osobních údajů pro konkrétní operaci zpracování, měli by pomáhat zúčastněným stranám při přípravě metodiky, pomáhat vyhodnotit kvalitu posouzení rizika a přijatelnost zbytkového rizika a rozvíjet znalosti v kontextu správce údajů,
- hlavní pověřenec pro bezpečnost informačních systémů, pokud je jmenován, a/nebo oddělení IT, by měli poskytovat pomoc správci a mohou navrhnout provedení posouzení vlivu na ochranu osobních údajů pro konkrétní operaci zpracování v závislosti na bezpečnostních nebo provozních potřebách.

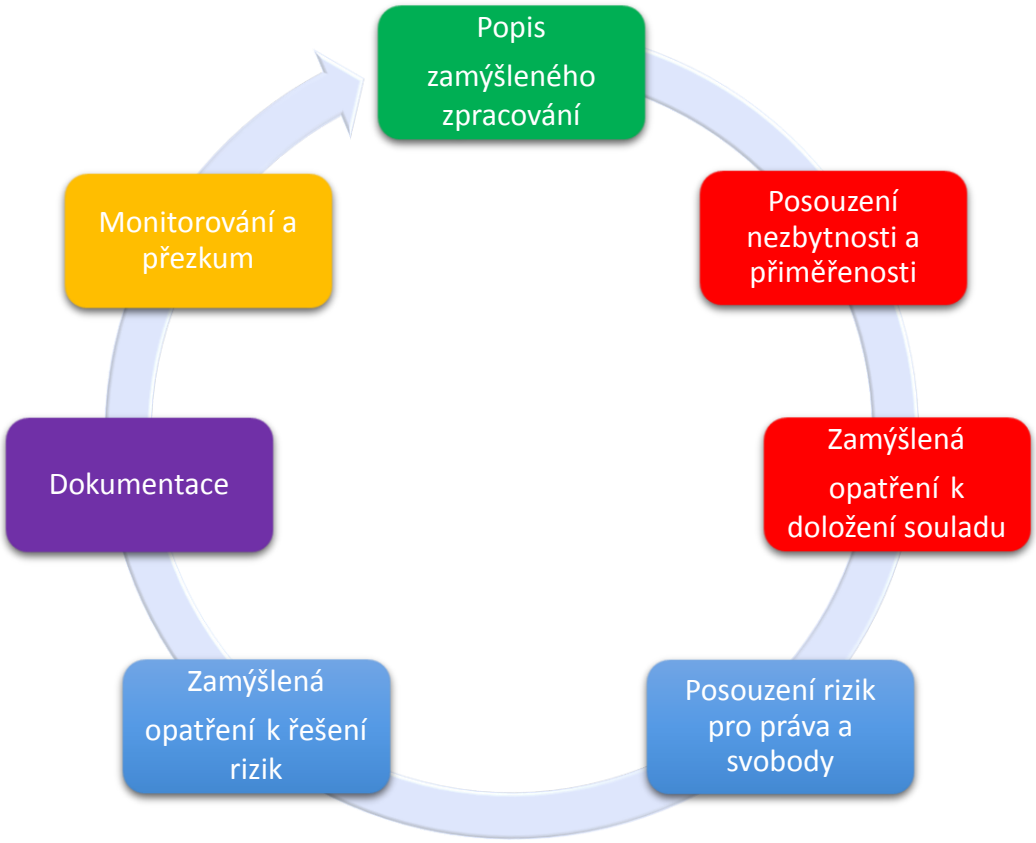
c) Jaká metodika se použije pro provedení posouzení vlivu na ochranu osobních údajů? Metodiky jsou různé, ale jsou společná kritéria.

[24] *Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (Doporučení pro rámec posouzení vlivu na soukromí pro Evropskou unii, cíl D3):* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

Obecné nařízení o ochraně osobních údajů stanoví minimální náležitosti posouzení vlivu na ochranu osobních údajů (čl. 35 odst. 7 a 84. a 90. bod odůvodnění):

- „*popis zamýšlených operací zpracování a účely zpracování*“,
- „*posouzení nezbytnosti a přiměřenosti operací zpracování*“,
- „*posouzení rizik pro práva a svobody subjektů údajů*“,
- „*plánovaná opatření:*
  - „*k řešení těchto rizik*“,
  - „*k doložení souladu s tímto nařízením*“.

Tento obrázek znázorňuje obecný opakující se proces provádění posouzení vlivu na ochranu osobních údajů[25]:



Při posuzování dopadu operací zpracování údajů je třeba zohlednit dodržování kodexu chování podle článku 40 (čl. 35 odst. 8). To může být užitečné při prokázání, že byla zvolena nebo zavedena odpovídající opatření, pokud je kodex chování pro operaci zpracování vhodný. Je třeba rovněž zohlednit osvědčení, pečeti a známky pro účely doložení souladu s obecným nařízením o ochraně osobních údajů v případě operací zpracování prováděných správci a zpracovateli (článek 42), stejně jako závazná podniková pravidla.

Všechny příslušné požadavky stanovené v obecném nařízení o ochraně osobních údajů tvoří široký obecný rámec pro navrhování a provádění posouzení vlivu na ochranu osobních údajů. Praktické

[25] Je třeba zdůraznit, že zobrazený proces je opakovaný: v praxi to znamená, že je pravděpodobné, že před dokončením posouzení vlivu na ochranu osobních údajů bude třeba se k jednotlivým etapám opakovaně vracet.

provedení posouzení vlivu na ochranu osobních údajů bude záviset na požadavcích stanovených v obecném nařízení o ochraně osobních údajů, které mohou doplnit podrobnější praktické pokyny. Provádění posouzení vlivu na ochranu osobních údajů jsou škálovatelná. To znamená, že i malý správce údajů může navrhovat a provádět posouzení vlivu na ochranu osobních údajů vhodné pro jeho operace zpracování.

V 90. bodě odůvodnění obecného nařízení o ochraně osobních údajů je výčet řady prvků posouzení vlivu na ochranu osobních údajů, které se překrývají s přesně definovanými prvky řízení rizika (např. ISO 31000[26]). Z hlediska řízení rizik je záměrem posouzení vlivu na ochranu osobních údajů „řídit rizika" pro práva a svobody fyzických osob, a to prostřednictvím těchto postupů:

- stanovení kontextu: „*zohlednit […] povahu, rozsah, kontext a účely zpracování a zdroje rizika",*
- posouzení rizik: „*posoudit konkrétní pravděpodobnost a závažnost vysokého rizika*",
- řešení rizik: „*snížení tohoto rizika*" a „*zajištění ochrany osobních údajů*" a „*prokázání souladu s tímto nařízením*".

Pozn.: posouzení vlivu na ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů je nástrojem pro řízení rizik pro práva subjektů údajů, a proto vychází z jejich hlediska, jak je tomu v určitých oblastech (např. v oblasti ochrany společnosti). Naproti tomu řízení rizik v ostatních oblastech (např. bezpečnost informačních systémů) se zaměřuje na organizaci.

Obecné nařízení o ochraně osobních údajů poskytuje správcům údajů pružnost při stanovení přesné struktury a formy posouzení vlivu na ochranu osobních údajů, aby mohla být přizpůsobena stávajícím pracovním postupům. V EU a ve světě existuje řada různých zavedených postupů, které přihlížejí ke složkám uvedeným v 90. bodě odůvodnění. Ať už je ale jeho forma jakákoli, posouzení vlivu na ochranu osobních údajů musí být skutečným posouzením rizik, jež umožní správci přijmout opatření na jejich řešení.

Na podporu provádění základních požadavků stanovených v obecném nařízení o ochraně osobních údajů je možné použít různé metodiky (pro příklady metodik posouzení vlivu na ochranu osobních údajů a soukromí viz příloha 1). Byla stanovena společná kritéria, jejichž účelem je umožnit existenci těchto rozdílných přístupů a současně zajistit soulad s obecným nařízením o ochraně osobních údajů ze strany správců (viz příloha 2). Vyjasňují základní požadavky nařízení, ponechávají však dostatečný prostor pro různé formy provádění. Pomocí těchto kritérií je možné prokázat, že konkrétní metodika posouzení vlivu na ochranu osobních údajů splňuje potřebné normy, které ukládá obecné nařízení o ochraně osobních údajů. **Volba metodiky spočívá na správci údajů, tato metodika by však měla splňovat kritéria uvedená v příloze 2.**

Pracovní skupina zřízená podle článku 29 vybízí k vytváření odvětvových rámců posouzení vlivu na ochranu osobních údajů. Mohou tak využívat znalostí konkrétního odvětví a posouzení vlivu na ochranu osobních údajů tak může řešit specifická hlediska konkrétního druhu operace zpracování (např.: konkrétní druhy údajů, majetek podniků, možné dopady, hrozby, opatření). To znamená, že posouzení vlivu na ochranu osobních údajů může řešit problémy, které vznikají v konkrétním

[26] Postupy řízení rizik: sdělení a konzultace, stanovení kontextu, posouzení rizik, řešení rizik, monitorování a přezkum (viz pojmy a definice a obsah přehledu ISO 31000: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

hospodářském odvětví, nebo při použití konkrétních technologií nebo provádění konkrétního druhu operace zpracování.

Kromě toho v případě potřeby *„[s]právce […] provede přezkum s cílem posoudit, zda je zpracování prováděno v souladu s posouzením vlivu na ochranu osobních údajů alespoň v případech, kdy dojde ke změně rizika, jež představují operace zpracování“ (čl. 35 odst. 11*[27]*).*

d) Existuje povinnost zveřejnit posouzení vlivu na ochranu osobních údajů? Nikoli, ale zveřejnění souhrnu může podpořit důvěru, přičemž úplné posouzení vlivu na ochranu osobních údajů musí být zasláno dozorovému úřadu, pokud proběhly předchozí konzultace nebo pokud to požaduje úřad pro ochranu údajů.

Zveřejnění posouzení vlivu na ochranu osobních údajů není požadavek vyplývající z obecného nařízení o ochraně osobních údajů, záleží na rozhodnutí správce. Správci by však měli zvážit zveřejnění alespoň části, jako např. souhrnu nebo závěru svého posouzení vlivu na ochranu osobních údajů.

Účelem tohoto postupu by bylo podpořit důvěru v operace zpracování prováděné správcem a prokázat odpovědnost a transparentnost. Zveřejnění posouzení vlivu na ochranu osobních údajů v případech, kdy je veřejnost dotčena operací zpracování, je zvláště dobrou praxí. Tak by tomu mohlo být zejména v případě, kdy posouzení vlivu na ochranu osobních údajů provádí orgán veřejné správy.

Zveřejněné posouzení vlivu na ochranu osobních údajů nemusí obsahovat celé posouzení, zejména pokud by posouzení vlivu na ochranu osobních údajů mohlo obsahovat konkrétní informace týkající se bezpečnostních rizik pro správce údajů nebo vyzradit obchodní tajemství nebo obchodně citlivé informace. Za těchto okolností by zveřejněná verze mohla obsahovat pouze souhrn hlavních zjištění posouzení vlivu na ochranu osobních údajů, případně jen prohlášení, že bylo posouzení vlivu na ochranu osobních údajů provedeno.

Kromě toho pokud posouzení vlivu na ochranu osobních údajů odhalí značné zbytkové riziko, správce údajů má uloženo, aby před zpracováním požádal o konzultaci dozorový úřad (čl. 36 odst. 1). Přitom je nutné poskytnout celé posouzení vlivu na ochranu osobních údajů (čl. 36 odst. 3 písm. e)). Dozorový úřad může poskytnout své stanovisko[28], aniž by vyzradil obchodní tajemství nebo odhalil slabá místa v zabezpečení, a to v souladu se zásadami platnými v každém členském státě o přístupu veřejnosti k úředním dokumentům.

E. <u>Kdy je konzultován dozorový úřad? Když je vysoké zbytkové riziko.</u>

Jak je vysvětleno výše:

- posouzení vlivu na ochranu osobních údajů se vyžaduje, pouze pokud je u dané operace zpracování *„pravděpodobné, že [...] bude [...] mít za následek vysoké riziko pro práva a svobody fyzických osob“ (čl. 35 odst. 1, viz III.B.a). Jedná se například o rozsáhlé zpracovávání zdravotnických údajů, u něhož je pravděpodobné, že bude mít za následek vysoké riziko, a u něhož se vyžaduje posouzení vlivu na ochranu osobních údajů,*

[27] Čl. 35 odst. 10 výslovně vylučuje pouze použití čl. 35 odst. 1 až 7.

[28] Správce je povinen vyžádat si písemné stanovisko, pouze pokud se dozorový úřad domnívá, že zamýšlené zpracování by porušovalo nařízení, jak je uvedeno v čl. 36 odst. 2.

- dále je odpovědností správce údajů, aby posoudil rizika pro práva a svobody subjektů údajů a stanovil opatření[29] určená ke snížení těchto rizik na přijatelnou míru a prokázání souladu s obecným nařízením o ochraně osobních údajů (čl. 35 odst. 7, viz III.C.c). Jako příklad lze uvést používání vhodných technických a organizačních bezpečnostních opatření při uchovávání osobních údajů v přenosných počítačích (účinné šifrování celého disku, silná správa klíčů, dostatečná kontrola přístupu, bezpečné zálohování atd.) kromě existujících opatření (oznámení, souhlasu, práva na přístup, práva vznést námitku atd.).

Pokud ve výše uvedeném příkladu s přenosným počítačem správce údajů považuje riziko za dostatečně snížené a ve smyslu ustanovení čl. 36 odst. 1 a 84. a 94. bodu odůvodnění, může zpracování pokračovat bez konzultace s dozorovým úřadem. V případech, kdy správce údajů nedokáže zjištěná rizika dostatečně řešit (tj. zbytkové riziko zůstává vysoké), musí správce údajů konzultovat dozorový úřad.

Za nepřijatelně vysoké zbytkové riziko lze například považovat, pokud subjektům údajů hrozí závažné nebo dokonce nevratné důsledky, které nelze překonat (např. neoprávněný přístup k údajům, který má za následek ohrožení života subjektu údajů, propuštění ze zaměstnání, finanční ohrožení) a/nebo pokud je zřejmé, že riziko nastane (např. tím, že nebude možné omezit počet osob, které mají přístup k údajům, kvůli způsobu jejich sdílení, použití nebo distribuce, nebo pokud není u některé známé zranitelnosti opraveno zabezpečení).

Pokud správce údajů nemá k dispozici dostatečná opatření ke snížení rizika na přijatelnou míru (to znamená, že zbytková rizika jsou nadále vysoká), je nutná konzultace s dozorovým úřadem[30].

Kromě toho správce bude muset konzultovat dozorový úřad vždy, když právo členského státu ukládá správci povinnost konzultovat s dozorovým úřadem anebo získat od něj předchozí povolení, pokud jde o zpracování správcem za účelem vykonání úkolu ve veřejném zájmu, včetně zpracování v souvislosti se sociální ochranou a veřejným zdravím (čl. 36 odst. 5).

Je však třeba konstatovat, že bez ohledu na to, zda jsou konzultace s dozorovým úřadem povinné, či nikoli – což záleží na míře zbytkového rizika, stále zůstává povinnost uchovat záznam o posouzení vlivu na ochranu osobních údajů a aktualizovat posouzení vlivu na ochranu osobních údajů v přiměřené době.

IV. Závěry a doporučení

Posouzení vlivu na ochranu osobních údajů jsou užitečným nástrojem, jímž mohou správci údajů provádět systémy zpracování údajů, které jsou v souladu s obecným nařízením o ochraně osobních údajů, a mohou být pro některé typy operací zpracování povinná. Jsou škálovatelná a mohou mít různou formu, obecné nařízení o ochraně osobních údajů však stanoví základní požadavky pro účinné posouzení vlivu na ochranu osobních údajů. Správci údajů by měli vnímat posouzení vlivu na ochranu

[29] Rovněž je třeba zohlednit stávající pokyny Evropského sboru pro ochranu osobních údajů a dozorových úřadů a zohlednit stav a náklady provádění, jak je stanoveno v čl. 35 odst. 1.

[30] Pozn.: opatření „*pseudonymizace a šifrování osobních údajů*“ (stejně jako minimalizace údajů, mechanismy dohledu *atd*.) nemusejí být vhodná za všech okolností. Jedná se jen o příklady. Stanovení vhodných opatření záleží na kontextu a rizicích konkrétních operací zpracování.

osobních údajů jako užitečnou a prospěšnou činnost, která pomáhá zajištění souladu s právními předpisy.

V čl. 24 odst. 1 je stanoven výčet základních odpovědností správce z hlediska souladu s obecným nařízením o ochraně osobních údajů: „*[s] přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována*“.

Posouzení vlivu na ochranu osobních údajů je jedním z hlavních nástrojů pro zajištění souladu s nařízením v případech, kdy je plánováno nebo se počítá s vysoce rizikovým zpracováním údajů. To znamená, že správci údajů by měli stanovit, zda má být posouzení vlivu na ochranu osobních údajů provedeno, či nikoli, a to za pomoci kritérií stanovených v tomto dokumentu. Správce údajů by měl rozšířit tento seznam prostřednictvím interních zásad o další požadavky doplňující právní požadavky obecného nařízení o ochraně osobních údajů. To by mělo posílit důvěru a jistotu subjektů údajů i dalších správců údajů.

Pokud se počítá s pravděpodobným vysokým rizikem zpracování, správce údajů musí:

- zvolit metodiku posouzení vlivu na ochranu osobních údajů (příklady jsou uvedeny v příloze 1), která splňuje kritéria uvedená v příloze 2, nebo stanovit a zavést postup systematického posouzení vlivu na ochranu osobních údajů, který:
  - splňuje kritéria uvedená v příloze 2,
  - je začleněn do stávajících postupů návrhu, vývoje, změn, rizik a operačního přezkumu, a to v souladu s vnitřními postupy, kontextem a kulturou,
  - zahrnuje příslušné zúčastněné strany a jednoznačně vymezuje jejich odpovědnosti (správce, pověřenec pro ochranu osobních údajů, subjekty údajů nebo jejich zástupci, podniky, technické služby, zpracovatelé, pověřenec pro bezpečnost informačních systémů atd.),
- předkládat zprávu o posouzení vlivu na ochranu osobních údajů příslušnému dozorovému úřadu, pokud je mu tato povinnost uložena,
- konzultovat dozorový úřad, pokud se nepodařilo stanovit dostatečná opatření na snížení vysokého rizika,
- pravidelně provádět přezkum posouzení vlivu na ochranu osobních údajů a zpracování, které posuzuje, alespoň pokud existuje určitá pravděpodobnost, že zpracování operace bude spojeno s určitým rizikem,
- zdokumentovat přijatá rozhodnutí.

Příloha 1 – Příklady stávajících rámců EU pro posouzení vlivu na ochranu osobních údajů

Obecné nařízení o ochraně osobních údajů nestanoví přesně postup posouzení vlivu na ochranu osobních údajů, umožňuje však správcům údajů zavést rámec, který doplní jejich stávající pracovní postupy, jestliže zohledňuje prvky popsané v čl. 35 odst. 7. Tento rámec může nechat vypracovat správce údajů nebo se může jednat o společný rámec pro konkrétní odvětví. Existující rámce vypracované úřady pro ochranu údajů členských států EU a odvětvové rámce EU zahrnují (mimo jiné):

Příklady obecných rámců EU:

- DE: Standardní model pro ochranu údajů, V.1.0 – zkušební verze, 2016[31].
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/node/15798
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Příklady odvětvových rámců EU:

- Rámec pro posuzování dopadů aplikací radiofrekvenční identifikace (RFID) na soukromí a ochranu údajů[32].
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Šablona pro posouzení vlivu inteligentních sítí a inteligentních měřicích systémů na ochranu osobních údajů[33]
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

---

[31] Jednomyslně přijatý 92 hlasy (Bavorsko se zdrželo hlasování). Konference nezávislých úřadů pro ochranu údajů na spolkové a zemské úrovni v Kühlungsbornu ve dnech 9.–10. listopadu 2016.

[32] Viz též:

- Doporučení Komise ze dne 12. května 2009 o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence.
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ%3AL%3A2009%3A122%3A0047%3A0051%3Acs%3APDF
- Stanovisko 9/2011 k revidovanému návrhu odvětví na rámec pro posuzování dopadů aplikací RFID na soukromí a ochranu údajů.
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_cs.pdf

[33] Viz též stanovisko 7/2013 k šabloně pro posouzení dopadů inteligentních sítí a inteligentních měřicích systémů na ochranu údajů, kterou vypracovala odborná skupina 2 pracovní skupiny Komise pro inteligentní sítě.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_cs.pdf

Mezinárodní norma je rovněž zdrojem obecných zásad pro metodiky používané při provádění posouzení vlivu na ochranu osobních údajů (ISO/IEC 29134[34]).

[34] ISO/IEC 29134 (projekt), *Informační technologie – techniky zabezpečení – posouzení vlivu na soukromí – pokyny*, Mezinárodní organizace pro normalizaci (ISO).

Příloha 2 – Kritéria přijatelného posouzení vlivu na ochranu osobních údajů

Pracovní skupina zřízená podle článku 29 navrhuje tato kritéria, na základě kterých mohou správci údajů určit, zda je třeba provést posouzení vlivu na ochranu osobních údajů, či nikoli, nebo zda je zvolená metodika posouzení vlivu na ochranu osobních údajů dostatečně komplexní, aby zajišťovala soulad s obecným nařízením o ochraně osobních údajů:

- ☐ je uveden systematický popis zpracování (čl. 35 odst. 7 písm. a)):
  - ☐ přihlíží se k povaze, rozsahu, kontextu a účelům zpracování (90. bod odůvodnění),
  - ☐ jsou zaznamenány osobní údaje, příjemci a doba, po kterou budou osobní údaje uloženy,
  - ☐ je uveden funkční popis operace zpracování,
  - ☐ jsou stanoveny prostředky, na nichž jsou osobní údaje závislé (hardware, software, sítě, lidé, tištěné dokumenty a kanály pro přenos tištěných dokumentů),
  - ☐ je zohledněn soulad se schválenými kodexy chování (čl. 35 odst. 8);
- ☐ je posouzena nezbytnost a přiměřenost operací zpracování (čl. 35 odst. 7 písm. b)):
  - ☐ jsou stanovena opatření určená k zajištění souladu s nařízením (čl. 35 odst. 7 písm. d) a 90. bodem odůvodnění, přičemž se přihlíží k:
    - ☐ opatřením za účelem přiměřenosti a nezbytnosti zpracování na základě:
      - ☐ stanovených, výslovně vyjádřených a legitimních účelů (čl. 5 odst. 1 písm. b)),
      - ☐ zákonnosti zpracování (článek 6),
      - ☐ údajů, které jsou přiměřené, relevantní a omezené na nezbytný rozsah (čl. 5 odst. 1 písm. c)),
      - ☐ omezené doby uložení (čl. 5 odst. 1 písm. e)),
    - ☐ opatřením za účelem podpory práv subjektů údajů:
      - ☐ informace poskytnuté subjektu údajů (článek 12, 13 a 14),
      - ☐ právo na přístup a přenositelnost údajů (články 15 a 20),
      - ☐ právo na opravu a výmaz údajů (články 16, 17 a 19),
      - ☐ právo na námitku a na omezení zpracování (články 18, 19 a 21),
      - ☐ vztahy se zpracovatelem (článek 28),
      - ☐ ochrany týkající se předávání údajů mezinárodním subjektům (kapitola V)
      - ☐ před konzultací (článek 36);
- ☐ jsou řízena rizika pro práva a svobody subjektů údajů (čl. 35 odst. 7 písm. c)):
  - ☐ je zhodnocen původ, povaha, zvláštnost a závažnost rizika (srov. 84. bod odůvodnění) nebo přesněji pro každé riziko (neoprávněný přístup, nežádoucí úpravy a zánik dat) z hlediska subjektu údajů:
    - ☐ jsou zohledněny zdroje rizik (90. bod odůvodnění),
    - ☐ jsou určeny možné vlivy na práva a svobody subjektů údajů v případě událostí, jako např. neoprávněný přístup, nežádoucí úpravy či zánik dat,
    - ☐ hrozby, které by mohly mít za následek neoprávněný přístup, nežádoucí úpravy či zánik dat,
    - ☐ je proveden odhad pravděpodobnosti a závažnosti (90. bod odůvodnění),
  - ☐ jsou stanovena opatření určená k řešení těchto rizik (čl. 35 odst. 7 písm. d) a 90. bod odůvodnění);
- ☐ jsou zapojeny zúčastněné strany:
  - ☐ je vyžádán posudek pověřence pro ochranu osobních údajů (čl. 35 odst. 2);
  - ☐ je případně získáno stanovisko subjektů údajů nebo jejich zástupců (čl. 35 odst. 9).