PRACOVNÁ SKUPINA PRE OCHRANU ÚDAJOV ZRIADENÁ PODĽA ČLÁNKU 29

SN 4654/17

17/SK

WP 248 rev.01

# Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“

**Prijaté 4. apríla 2017**

**V znení naposledy revidovanom a prijatom 4. októbra 2017**

Táto pracovná skupina sa zriadila podľa článku 29 smernice 95/46/ES. Je to nezávislý európsky poradný orgán pre ochranu údajov a súkromie. Jeho úlohy sú opísané v článku 30 smernice 95/46/EHS a v článku 15 smernice 2002/58/ES.

Sekretariát zabezpečuje Riaditeľstvo C (Základné práva a občianstvo Únie) Európskej komisie, Generálne riaditeľstvo pre spravodlivosť, B-1049 Brusel, Belgicko, kancelária č. MO-59 03/075.

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

**PRACOVNÁ SKUPINA PRE OCHRANU JEDNOTLIVCOV SO ZRETEĽOM NA SPRACOVANIE OSOBNÝCH ÚDAJOV,**

ktorá bola zriadená smernicou Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995,

so zreteľom na články 29 a 30 uvedenej smernice,

so zreteľom na svoj rokovací poriadok,

**PRIJALA TIETO USMERNENIA:**

# Obsah

## I. Úvod

Nariadenie 2016/679[1] (všeobecné nariadenie o ochrane údajov) sa bude uplatňovať od 25. mája 2018. V článku 35 všeobecného nariadenia o ochrane údajov sa zavádza pojem posúdenie vplyvu na ochranu údajov (Data Protection Impact Assessment – DPIA[2]), podobne ako sa zavádza v smernici 2016/680[3].

Posúdenie vplyvu na ochranu údajov je proces určený na opis spracúvania, posúdenie jeho nutnosti a primeranosti, ako aj na to, aby pomohol riadiť riziká pre práva a slobody fyzických osôb vyplývajúce zo spracúvania osobných údajov[4] tým, že sa tieto riziká posúdia a určia sa opatrenia na vysporiadanie sa s nimi. Posúdenia vplyvu na ochranu údajov sú dôležitými nástrojmi na to, aby príslušné subjekty prevzali zodpovednosť, keďže prevádzkovateľom pomáhajú nielen dodržiavať požiadavky všeobecného nariadenia o ochrane údajov, ale aj preukázať, že sa prijali primerané opatrenia na zabezpečenie súladu s nariadením (pozri aj článok 24)[5]. Inými slovami, **posúdenie vplyvu na ochranu údajov je proces budovania a preukazovania súladu**.

Podľa všeobecného nariadenia o ochrane údajov môže nedodržiavanie požiadaviek týkajúcich sa posúdenia vplyvu na ochranu údajov viesť k uloženiu pokút zo strany príslušného dozorného orgánu. Ak sa posúdenie vplyvu na ochranu údajov nevykoná, keď mu spracúvanie podlieha (článok 35 ods. 1) a ods. 3 – 4, ak sa posúdenie vplyvu na ochranu údajov vykoná nesprávne (článok 35 ods. 2 a ods. 7 až 9) alebo ak sa podľa potreby nekonzultuje s príslušným dozorným orgánom [článok 36 ods. 3 písm. e)], môže to viesť k správnej pokute vo výške do 10 miliónov EUR, alebo v prípade podniku do 2 %

---

[1] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracovávaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

[2] V iných kontextoch sa často používa anglický termín „*Privacy Impact Assessment*“ (PIA – posúdenie vplyvu na súkromie), pričom sa ním odkazuje na ten istý pojem.

[3] V článku 27 smernice Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov sa tiež uvádza, že posúdenie vplyvu na ochranu údajov je potrebné, pretože „*spracúvanie pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb*“.

[4] Vo všeobecnom nariadení o ochrane údajov sa pojem posúdenie vplyvu na ochranu údajov formálne nevymedzuje, ale

- jeho minimálny obsah je upresnený v článku 35 ods. 7 takto:
  - *„a) systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ;*
  - *b) posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu;*
  - *c) posúdenie rizika pre práva a slobody dotknutých osôb uvedených v odseku 1 a*
  - *d) opatrenia na riešenie rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením s ohľadom na práva a oprávnené záujmy dotknutých osôb a ďalších osôb, ktorých sa to týka“;*
- jeho význam a úloha je objasnená v odôvodnení 84 takto: *„S cieľom posilniť súlad s týmto nariadením, ak je pravdepodobné, že spracovateľské operácie povedú k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ by mal byť zodpovedný za vykonanie posúdenia vplyvu na ochranu údajov s cieľom zhodnotiť najmä pôvod, povahu, osobitosť a závažnosť tohto rizika“*.

[5] Pozri aj odôvodnenie 84. *„Výsledok posúdenia by sa mal zohľadniť pri stanovení primeraných opatrení, ktoré sa majú prijať s cieľom preukázať, že spracúvanie osobných údajov je v súlade s týmto nariadením“*.

celkového celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho ktorá suma je vyššia.

## II. Rozsah pôsobnosti usmernení

V týchto usmerneniach sa zohľadňuje:

- Vyhlásenie 14/EN WP 218[6], ktoré vydala pracovná skupina pre ochranu údajov zriadená podľa článku 29 (WP29);
- Usmernenia WP29 týkajúce sa zodpovednej osoby 16/EN WP 243[7];
- Stanovisko WP29 k obmedzeniu účelu 13/EN WP 203[8];
- medzinárodné normy[9];

V súlade s prístupom založeným na riziku, ktorý zosobňuje všeobecné nariadenie o ochrane údajov, vykonanie posúdenia vplyvu na ochranu údajov nie je povinné pre každú spracovateľskú operáciu. Posúdenie vplyvu na ochranu údajov sa vyžaduje len vtedy, keď spracúvanie „*pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb*“ (článok 35 ods. 1). S cieľom zabezpečiť jednotný výklad podmienok, za ktorých je posúdenie vplyvu na ochranu údajov povinné [článok 35 ods. 3)], je cieľom týchto usmernení najprv objasniť tento pojem a poskytnúť kritériá pre zoznamy, ktoré majú vypracovať orgány na ochranu údajov podľa článku 35 ods. 4).

Podľa článku 70 ods. 1 písm. e) bude Európsky výbor pre ochranu údajov môcť vydávať usmernenia, odporúčania a najlepšie postupy s cieľom podnietiť konzistentné uplatňovanie všeobecného nariadenia o ochrane údajov. Cieľom tohto dokumentu je predvídať takúto budúcu prácu Európskeho výboru pre ochranu údajov, a preto objasniť príslušné ustanovenia všeobecného nariadenia o ochrane údajov s cieľom pomôcť prevádzkovateľom dodržať zákon a poskytnúť právnu istotu tým prevádzkovateľom, ktorí musia vykonať posúdenie vplyvu na ochranu údajov.

Cieľom týchto usmernení je tiež podporiť vypracovanie:

- spoločného zoznamu Európskej únie týkajúceho sa spracovateľských operácií, v prípade ktorých je posúdenie vplyvu na ochranu údajov povinné (článok 35 ods. 4);
- spoločného zoznamu EÚ týkajúceho sa spracovateľských operácií, v prípade ktorých posúdenie vplyvu na ochranu údajov nie je potrebné (článok 35 ods. 5);
- spoločných kritérií týkajúcich sa metodiky vykonávania posúdenia vplyvu na ochranu údajov (článok 35 ods. 5);

---

[6] Vyhlásenie 14/EN WP 218, ktoré vydala WP29 v súvislosti s úlohou prístupu k právnym rámcom na ochranu údajov založeného na riziku, ktoré sa prijalo 30. mája 2014.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] Usmernenia WP29 týkajúce sa zodpovednej osoby 16/EN WP 243 prijaté 13. decembra 2016.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] Stanovisko WP29 k obmedzeniu účelu 13/EN WP 203 prijaté 2. apríla 2013.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] napr. ISO 31000:2009, *Riadenie rizík – Zásady a usmernenia*, Medzinárodná organizácia pre normalizáciu (ISO); ISO/IEC 29134 (projekt), *Informačné technológie – Bezpečnostné techniky – Posúdenie vplyvu na súkromie – Usmernenia*, Medzinárodná organizácia pre normalizáciu (ISO).

- spoločných kritérií určujúcich, kedy sa majú uskutočniť konzultácie s dozorným orgánom (článok 36 ods. 1);
- odporúčaní, pri ktorých by sa podľa možností malo vychádzať zo skúseností získaných v členských štátoch EÚ.

## III. Posúdenie vplyvu na ochranu údajov: vysvetlenie nariadenia

Vo všeobecnom nariadení o ochrane údajov sa od prevádzkovateľov vyžaduje, aby vykonali primerané opatrenia na zabezpečenie a preukázanie súladu s uvedeným nariadením, pričom okrem iného majú zohľadniť „riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb“ (článok 24 ods. 1). Povinnosť prevádzkovateľov vykonávať za určitých okolností posúdenie vplyvu na ochranu údajov je potrebné vnímať v kontexte ich všeobecnej povinnosti primerane riadiť riziká[10], ktoré prináša spracúvanie osobných údajov.

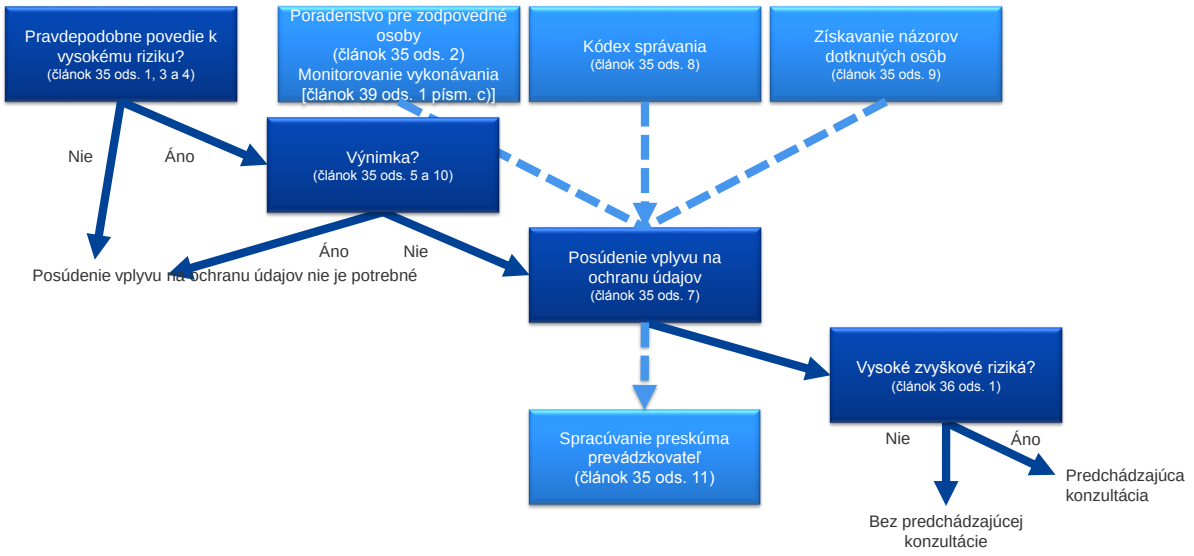
„Riziko“ je scenár, ktorý opisuje udalosť a jej následky odhadované v kategóriách závažnosti a pravdepodobnosti. „Riadenie rizika“ na druhej strane možno vymedziť ako koordinované činnosti s cieľom usmerniť a kontrolovať organizáciu, pokiaľ ide o riziko.

V článku 35 sa odkazuje na pravdepodobné „vysoké riziko pre práva a slobody jednotlivcov“. Ako sa uvádza vo vyhlásení pracovnej skupiny pre ochranu údajov zriadenej podľa článku 29, ktoré sa týka úlohy prístupu založeného na riziku k právnym rámcom na ochranu údajov, odkaz na „práva a slobody“ dotknutých osôb sa predovšetkým týka práv na ochranu údajov a súkromie, ale môže tiež zahŕňať iné základné práva, ako je sloboda prejavu, sloboda myslenia, sloboda pohybu, zákaz diskriminácie, právo na slobodu svedomia a náboženského vyznania.

V súlade s prístupom založeným na riziku, ktorý zosobňuje všeobecné nariadenie o ochrane údajov, vykonanie posúdenia vplyvu na ochranu údajov nie je povinné pre každú spracovateľskú operáciu. Namiesto toho sa posúdenie vplyvu na ochranu údajov sa vyžaduje len vtedy, keď spracúvanie „*pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb*“ (článok 35 ods. 1). Samotná skutočnosť, že neboli splnené podmienky pre vznik povinnosti vykonať posúdenie vplyvu na ochranu údajov, však neznižuje všeobecnú povinnosť prevádzkovateľa vykonávať opatrenia na primerané riadenie rizík pre práva a slobody dotknutých osôb. V praxi to znamená, že prevádzkovatelia musia neustále posudzovať riziká, ktoré vznikajú v dôsledku ich spracovateľských činností, aby mohli identifikovať, keď určitý druh spracúvania „pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb“.

[10] Je potrebné zdôrazniť, že na riadenie rizík pre práva a slobody fyzických osôb sa tieto riziká musia pravidelne identifikovať, analyzovať, odhadovať, hodnotiť, riešiť (napr. zmierňovať...) a skúmať. Prevádzkovatelia nemôžu uniknúť svojej zodpovednosti tým, že riziká pokryjú v rámci poistných zmlúv.

Základné zásady vzťahujúce sa na posúdenie vplyvu na ochranu údajov v rámci všeobecného nariadenia o ochrane údajov možno ilustrovať nasledovne:




A. Čo sa rieši v rámci posúdenia vplyvu na ochranu údajov? Jedna spracovateľská operácia alebo súbor podobných spracovateľských operácií.

**Posúdenie vplyvu na ochranu údajov sa môže týkať jednej operácie spracúvania údajov**. V článku 35 ods. 1 sa však uvádza, že „*pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziká, môže byť dostatočné jedno posúdenie*“. V odôvodnení 92 sa dopĺňa, že „*existujú okolnosti, za ktorých môže byť vhodné a hospodárne, aby sa predmet posúdenia vplyvu na ochranu údajov nevzťahoval len na jeden projekt, ale bol širší, napríklad ak orgány verejnej moci alebo verejnoprávne subjekty zamýšľajú vytvoriť spoločnú aplikáciu či spracovateľskú platformu alebo ak niekoľko prevádzkovateľov zamýšľa zaviesť spoločnú aplikáciu či spracovateľské prostredie v rámci odvetvia alebo segmentu priemyslu alebo na široko rozvetvenú horizontálnu činnosť*“.

**Jedno posúdenie vplyvu na ochranu údajov by sa mohlo použiť na posúdenie viacerých spracovateľských operácií, ktoré sú podobné** z hľadiska povahy, rozsahu, kontextu, účelu a rizík. Cieľom posúdení vplyvu na ochranu údajov je systematické skúmanie nových situácií, ktoré by mohli viesť k vysokým rizikám pre práva a slobody fyzických osôb, a posúdenie vplyvu na ochranu údajov nie je potrebné vykonávať v prípadoch (t.j. v spracovateľských operáciách uskutočňovaných v špecifickom kontexte a na špecifický účel), ktoré už boli predmetom skúmania. Mohlo by ísť o situáciu, keď sa podobná technológia používa na získavanie rovnakých údajov na tie isté účely. Napríklad skupina orgánov miestnej samosprávy, z ktorých každý zriaďuje podobný systém CCTV, by mohla vykonať jedno posúdenie vplyvu na ochranu údajov, ktoré by pokrylo spracúvanie týmito samostatnými prevádzkovateľmi, alebo prevádzkovateľ železnice (jeden prevádzkovateľ) by mohol jedným posúdením vplyvu na ochranu údajov pokryť monitorovanie kamerovým systémom vo všetkých svojich vlakoch. Môže sa to uplatniť aj na podobné spracovateľské operácie vykonávané rôznymi prevádzkovateľmi. V takých prípadoch by sa malo zdieľať alebo verejne sprístupniť referenčné posúdenie vplyvu na ochranu údajov, opatrenia opísané v posúdení vplyvu na ochranu údajov sa musia vykonať a musí sa poskytnúť zdôvodnenie vykonania jedného posúdenia vplyvu na ochranu údajov.

Keď spracovateľská operácia zahŕňa spoločných prevádzkovateľov, musia si presne vymedziť svoje povinnosti. V ich posúdení vplyvu na ochranu údajov by sa malo určiť, ktorá strana je zodpovedná za jednotlivé opatrenia navrhované na riešenie rizík a na ochranu práv a slobôd dotknutých osôb. Každý prevádzkovateľ by mal vyjadriť svoje potreby a vymeniť si užitočné informácie bez toho, aby vyzradil tajomstvá (napr. ochranu obchodných tajomstiev, duševné vlastníctvo, dôverné obchodné informácie) alebo zverejnil zraniteľné miesta.

**Posúdenie vplyvu na ochranu údajov môže byť užitočné aj pre posúdenie vplyvu technologického produktu na ochranu údajov**, napr. určitého hardvéru alebo softvéru, ak je pravdepodobné, že ho budú používať rôzni prevádzkovatelia na rôzne spracovateľské operácie. Prevádzkovateľ zavádzajúci určitý produkt je samozrejme naďalej povinný v súvislosti so špecifickým vykonávaním uskutočniť svoje vlastné posúdenie vplyvu na ochranu údajov, ako jeho základ však môže poslúžiť posúdenie vplyvu na ochranu údajov, ktoré vypracuje poskytovateľ produktu. Príkladom by mohol byť vzťah medzi výrobcami inteligentných meračov a spoločnosťami poskytujúcimi verejné služby. Každý poskytovateľ alebo sprostredkovateľ produktu by mal poskytovať užitočné informácie bez toho, aby vyzradil tajomstvá alebo aby jeho konanie viedlo k bezpečnostným rizikám tým, že sa zverejnia zraniteľné miesta.

B. Ktoré spracovateľské operácie podliehajú posúdeniu vplyvu na ochranu údajov? Okrem výnimiek, v ktorých „*pravdepodobne povedú k vysokému riziku*“.

V tejto časti sa uvádza, v ktorých prípadoch je posúdenie vplyvu na ochranu údajov povinné a v ktorých sa nemusí vykonať.

**Pokiaľ spracovateľská operácia nespĺňa výnimku (časť III.B.a), posúdenie vplyvu na ochranu údajov sa musí vykonať, keď spracovateľská operácia „*pravdepodobne povedie k vysokému riziku*“ (časť III.B.b).**

a) Kedy je posúdenie vplyvu na ochranu údajov povinné? Keď spracúvanie „*pravdepodobne povedie k vysokému riziku*“.

Vo všeobecnom nariadení o ochrane údajov sa nevyžaduje, aby sa posúdenie vplyvu na ochranu údajov vykonalo pre každú spracovateľskú operáciu, ktorá môže viesť k rizikám pre práva a slobody fyzických osôb. Vykonanie posúdenia vplyvu na ochranu údajov je povinné len vtedy, keď spracúvanie „*pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb*“ (článok 35 ods. 1, čo preukazuje článok 35. ods. 3 a dopĺňa článok 35 ods. 4). Je to osobitne dôležité, keď sa zavádza[11] nová technológia spracúvania údajov.

Keď nie je jasné, či sa má vyžadovať posúdenie vplyvu na ochranu údajov, WP29 odporúča, aby sa napriek tomu vykonalo, keďže je to užitočný nástroj, ako pomôcť prevádzkovateľom dodržiavať právne predpisy o ochrane údajov.

Hoci by sa posúdenie vplyvu mohlo požadovať aj za iných okolností, v článku 35 ods. 3 sa uvádza niekoľko príkladov, keď spracovateľská operácia „*pravdepodobne povedie k vysokému riziku*“:

- a) systematické a rozsiahle hodnotenie osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania a z ktorého vychádzajú

[11] Ďalšie príklady sa uvádzajú v odôvodneniach 89 a 91 a v článku 35 ods. 1 a 3.

rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu[12];

- *b) spracúvanie vo veľkom rozsahu osobitných kategórií údajov podľa článku 9 ods. 1 alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky podľa článku 10[13]; alebo*
- c) s*ystematické monitorovanie verejne prístupných priestorov vo veľkom rozsahu.*

Ako naznačuje slovo „*najmä*" v úvodnej vete článku 35 ods. 3 všeobecného nariadenia o ochrane údajov, v tomto zozname nie sú uvedené všetky možnosti. Môžu existovať spracovateľské operácie s vysokým rizikom, ktoré nie sú v tomto zozname uvedené, ale predstavujú podobne vysoké riziko. Takéto spracovateľské operácie by tiež mali podliehať posúdeniu vplyvu na ochranu údajov. Preto sú kritériá rozpracované nižšie niekedy podrobnejšie ako len jednoduché vysvetlenie, čo by sa malo chápať tromi príkladmi, ktoré sa uviedli v článku 35 ods. 3 všeobecného nariadenia o ochrane údajov.

S cieľom poskytnúť konkrétnejší súbor spracovateľských operácií, ktoré si vyžadujú posúdenie vplyvu na ochranu údajov z dôvodu vysokého rizika, ktoré je im vlastné, pričom sa zohľadnia jednotlivé prvky článku 35 ods. 1 a článku 35 ods. 3 písm. a) až c), by sa v súvislosti so zoznamom, ktorý sa má prijať na vnútroštátnej úrovni podľa článku 35 ods. 4 a odôvodnení 71, 75 a 91 a iných odkazov vo všeobecnom nariadení o ochrane údajov na spracovateľské operácie[14], ktoré *„pravdepodobne povedú k vysokému riziku*", malo zvážiť týchto deväť kritérií.

1. <u>Hodnotenie alebo prideľovanie bodov</u> vrátane profilovania a predpovedania, najmä z *„aspektov súvisiacich s výkonnosťou dotknutej osoby v práci, jej majetkovými pomermi, zdravím, osobnými preferenciami alebo záujmami, spoľahlivosťou alebo správaním, polohou alebo pohybom*" (odôvodnenia 71 a 91). Príkladom tohto postupu by mohla byť finančná inštitúcia, ktorá preveruje svojich klientov prostredníctvom v databáze obsahujúcej informácie o úveroch alebo v databáze obsahujúcej informácie o praní špinavých peňazí a financovaní terorizmu alebo v databáze s informáciami o podvodoch, alebo v prípade biotechnologickej spoločnosti by mohlo ísť o ponuku genetických testov priamo spotrebiteľom s cieľom posúdiť a predvídať riziká ochorenia a zdravotné riziká, alebo by mohlo ísť o spoločnosť, ktorá vytvára behaviorálne alebo marketingové profily založené na používaní jej webovej stránky alebo navigácii na nej.
2. <u>Automatizované rozhodovanie s právnym alebo podobne závažným účinkom</u>: spracúvanie, ktorého cieľom je prijatie rozhodnutí o dotknutých osobách *„s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu*" [článok 35 ods. 3 písm. a)]. Spracúvanie môže napríklad viesť k vylúčeniu jednotlivcov alebo k diskriminácii voči nim. Spracúvanie s malým alebo žiadnym vplyvom na jednotlivcov

[12] Pozri odôvodnenie 71: „*ak sa posudzujú osobné aspekty, najmä ak sa analyzujú alebo predvídajú aspekty týkajúce sa výkonnosti v práci, majetkových pomerov, zdravia, osobných preferencií alebo záujmov, spoľahlivosti alebo správania, polohy alebo pohybu, s cieľom vytvoriť alebo používať osobné profily*".

[13] Pozri odôvodnenie 75: „*ak sa spracúvajú osobné údaje odhaľujúce rasový alebo etnický pôvod, politické názory, náboženstvo alebo filozofické názory a členstvo v odborových organizáciách, a ak sa spracúvajú genetické údaje, údaje týkajúce sa zdravia či údaje týkajúce sa sexuálneho života alebo uznania viny zo spáchania trestného činu a priestupku či súvisiacich bezpečnostných opatrení*".

[14] Pozri napr. odôvodnenia 75, 76, 92 a 116.

nespĺňa toto špecifické kritérium. Ďalšie vysvetlenia týkajúce sa týchto pojmov sa poskytnú v nadchádzajúcich usmerneniach WP29 o profilovaní.

3. Systematické monitorovanie: spracúvanie používané na pozorovanie, monitorovanie alebo kontrolu dotknutých osôb vrátane údajov získaných prostredníctvom sietí alebo „*systematického monitorovania verejne prístupných miest*“ [článok 35 ods. 3 písm. c)][15]. Tento typ monitorovania je kritériom, pretože osobné údaje sa môžu získavať za okolností, keď dotknuté osoby nemusia vedieť, kto zbiera ich údaje a ako sa budú používať. Okrem toho, pre jednotlivcov sa môže ukázať ako nemožné zabrániť tomu, aby sa stali predmetom takéhoto spracúvania na verejnom (alebo verejne prístupnom) mieste (-ach).
4. Citlivé údaje alebo údaje veľmi osobnej povahy: zahŕňa to osobitné kategórie osobných údajov vymedzené v článku 9 (napr. informácie o politických názoroch jednotlivcov), ako aj osobné údaje týkajúce sa uznania viny za trestné činy a priestupky vymedzené v článku 10. Príkladom by mohla byť všeobecná nemocnica, ktorá uchováva lekárske záznamy pacientov, alebo súkromný detektív uchovávajúci podrobné informácie o páchateľoch trestnej činnosti. Nad rámec ustanovení všeobecného nariadenia o ochrane údajov sa niektoré kategórie údajov môžu považovať za také, ktoré zvyšujú možné riziko pre práva a slobody jednotlivcov. Tieto osobné údaje sa považujú za citlivé (ako sa tento pojem bežne chápe), pretože sú prepojené na domácnosť a súkromné aktivity (napr. elektronická komunikácia, ktorej dôvernosť by mala byť chránená) alebo preto, že vplývajú na výkon určitého základného práva (napr. údaje o polohe, ktorých získavanie spochybňuje slobodu pohybu), alebo preto, že ich porušenie jednoznačne zahŕňa závažné dôsledky na každodenný život dotknutej osoby (napr. finančné údaje, ktoré by sa mohli použiť na platobné podvody). V tejto súvislosti môže byť relevantné, či už dotknutá osoba alebo tretie strany údaje zverejnili. Skutočnosť, že osobné údaje sú verejne prístupné, sa môže zohľadniť ako faktor pri posudzovaní, ak sa v súvislosti s týmito údajmi očakávalo, že sa budú ďalej používať na isté účely. Toto kritérium môže zahŕňať aj také údaje, ako sú osobné dokumenty, emaily, denníky, poznámky z elektronických čítačiek vybavených prvkami na zapisovanie poznámok a veľmi osobné informácie, ktoré sa nachádzajú v aplikáciách na zaznamenávanie udalostí v rôznych oblastiach života (life-logging applications).
5. Údaje spracúvané vo veľkom rozsahu: vo všeobecnom nariadení o ochrane údajov sa nevymedzuje, čo predstavuje veľký rozsah, hoci v odôvodnení 91 sa uvádza určité usmernenie. WP29 v každom prípade odporúča, aby sa pri posudzovaní toho, či sa spracúvanie vykonáva vo veľkom rozsahu, zvážili predovšetkým tieto faktory[16]:
    a. počet dotknutých osôb, ktorých sa to týka, buď ako konkrétne číslo alebo ako podiel relevantnej populácie;
    b. objem údajov a/alebo rozsah rôznych údajových položiek, ktoré sa spracúvajú;
    c. dĺžka trvania alebo nemennosť činnosti spracúvania údajov;

[15] WP29 vykladá slovo „*systematický*“ tak, že znamená jedno alebo viacero z nasledovných skutočností (pozri usmernenia WP29 týkajúce sa zodpovednej osoby 16/EN WP 243):

- vykonáva sa podľa systému;
- vopred pripravené, organizované alebo metodické;
- uskutočňuje sa ako súčasť všeobecného plánu na získavanie údajov;
- vykonáva sa ako súčasť stratégie.

WP29 vykladá slovo „*verejne prístupné miesto*“ ako akékoľvek miesto, ktoré je otvorené verejnosti, napr. námestie, nákupné centrum, ulica, trh, vlaková stanica alebo verejná knižnica.

[16] Pozri usmernenia WP29 týkajúce sa zodpovednej osoby 16/EN WP 243.

d. geografický rozsah činnosti spracúvania.

6. Spájanie alebo kombinovanie súborov údajov, napr. údajov pochádzajúcich z dvoch alebo viacerých operácií spracúvania údajov vykonaných na rozdielne účely a/alebo rozličnými prevádzkovateľmi údajov takým spôsobom, ktorý by prekročil rozumné očakávania dotknutej osoby[17].
7. Údaje týkajúce sa zraniteľných dotknutých osôb (odôvodnenie 75): spracúvanie tohto druhu údajov je kritériom z dôvodu zvýšenej nerovnováhy moci medzi dotknutými osobami a prevádzkovateľom, čo znamená, že jednotlivci sa môžu nachádzať v pozícii, že nemôžu jednoduchým spôsobom vyjadriť súhlas so spracúvaním svojich údajov, namietať voči nemu ani vykonávať svoje práva. Zraniteľné dotknuté osoby môžu zahŕňať deti (možno ich považovať osoby, ktoré nie sú schopné vedome a na základe uváženia namietať voči spracúvaniu svojich údajov alebo s ním súhlasiť), zamestnanci, zraniteľnejšie časti obyvateľstva vyžadujúce si osobitnú ochranu (mentálne postihnuté osoby, žiadatelia o azyl, staršie osoby, pacienti atď.) a v každom prípade také osoby, v súvislosti s ktorými možno identifikovať nerovnováhu vo vzťahu medzi postavením dotknutej osoby a prevádzkovateľa.
8. Inovačné využitie alebo uplatňovanie nových technologických alebo organizačných riešení, napr. kombinácia využitia odtlačkov prstov a rozpoznávania tvárí pre lepšiu kontrolu fyzického prístupu atď. Vo všeobecnom nariadení o ochrane údajov sa jednoznačne uvádza (v článku 35 ods. 1 a v odôvodneniach 89 a 91), že využitie novej technológie vymedzenej v „*súlade s dosiahnutým stavom technologických znalostí*“ (odôvodnenie 91), môže viesť k tomu, že bude potrebné vykonať posúdenie vplyvu na ochranu údajov. Je to z toho dôvodu, že využitie takejto technológie môže zahŕňať nové formy získavania a využívania údajov, ktoré môžu byť spojené s vysokým rizikom pre práva a slobody jednotlivcov. Osobné a sociálne dôsledky zavedenia novej technológie môžu byť naozaj neznáme. Posúdenie vplyvu na ochranu údajov pomôže prevádzkovateľovi pochopiť a riešiť tieto riziká. Napríklad určité aplikácie „internetu vecí“ by mohli mať výrazný vplyv na každodenné životy jednotlivcov a ich súkromie, a preto si vyžadujú posúdenie vplyvu na ochranu údajov.
9. Keď samotné spracúvanie *bráni dotknutým osobám uplatniť svoje právo alebo využiť službu alebo zmluvu* (článok 22 a odôvodnenie 91). Zahŕňa to spracovateľské operácie, ktorých cieľom je umožniť, upraviť alebo odmietnuť prístup dotknutých osôb k službe alebo uzavretiu zmluvy. Príkladom tohto postupu by mohla byť situácia, keď banka preveruje svojich klientov v databáze obsahujúcej informácie o úveroch s cieľom rozhodnúť o tom, či im poskytne úver.

Vo väčšine prípadov môže prevádzkovateľ predpokladať, že spracúvanie, ktoré spĺňa dve kritéria, by si vyžadovalo vykonanie posúdenia vplyvu na ochranu údajov. WP29 sa vo všeobecnosti domnieva, že čím viac kritérií spracúvanie spĺňa, tým je pravdepodobnejšie, že predstavuje vysoké riziko pre práva a slobody dotknutých osôb, a preto si vyžaduje posúdenie vplyvu na ochranu údajov, a to bez ohľadu na opatrenia, ktoré prevádzkovateľ plánuje prijať.

V niektorých prípadoch sa však **prevádzkovateľ môže domnievať, že posúdenie vplyvu na ochranu údajov je potrebné aj v prípade spracúvania, ktoré spĺňa len jedno z týchto kritérií.**

[17] Pozri vysvetlenie v stanovisku WP29 k obmedzeniu účelu 13/EN WP 203, s. 24.

Na základe nasledovných príkladov možno názorne ukázať, aké kritériá by sa mali použiť na posúdenie toho, či si konkrétna spracovateľská operácia vyžaduje posúdenie vplyvu na ochranu údajov:

| **Príklady spracúvania** | **Prípadné relevantné kritériá** | **Je pravdepodobné, že sa bude vyžadovať posúdenie vplyvu na ochranu údajov?** |
|---|---|---|
| Nemocnica spracúvajúca genetické a zdravotné údaje svojich pacientov (nemocničný informačný systém). | - citlivé údaje alebo údaje veľmi osobnej povahy<br>- údaje týkajúce sa zraniteľných dotknutých osôb<br>- údaje spracúvané vo veľkom rozsahu | Áno |
| Používanie kamerového systému na monitorovanie správania vodičov na diaľniciach. Prevádzkovateľ plánuje používať inteligentný systém na analýzu videozáznamov s cieľom identifikovať jednotlivé autá a automaticky rozpoznávať poznávacie značky. | - systematické monitorovanie<br>- inovačné použitie alebo uplatňovanie technologických alebo organizačných riešení | |
| Podnik systematicky monitorujúci činnosti svojich zamestnancov vrátane monitorovania ich počítačov, činností na internete atď.. | - systematické monitorovanie<br>- údaje týkajúce sa zraniteľných dotknutých osôb | |
| Zhromažďovanie údajov z verejných sociálnych médií na vytváranie profilov | - hodnotenie alebo prideľovanie bodov<br>- údaje spracúvané vo veľkom rozsahu<br>- spájanie alebo kombinovanie súborov údajov<br>- citlivé údaje alebo údaje veľmi osobnej povahy: | |
| Inštitúcia vytvárajúca celoštátnu databázu pre úverové hodnotenie alebo databázu na účely boja proti podvodom. | - hodnotenie alebo prideľovanie bodov<br>- automatizované rozhodovanie s právnym alebo podobne závažným účinkom<br>- dotknutým osobám sa bráni vo výkone práva alebo využitia služby alebo zmluvy<br>- citlivé údaje alebo údaje veľmi osobnej povahy: | |
| Uchovávanie na účely archivácie týkajúce sa pseudonymizovaných citlivých osobných údajov o zraniteľných dotknutých osobách vykonávané v rámci výskumných projektov alebo klinických skúšok. | - citlivé údaje<br>- údaje týkajúce sa zraniteľných dotknutých osôb<br>- dotknutým osobám sa bráni vo výkone práva alebo využitia služby alebo zmluvy | |

| Príklady spracúvania | Prípadné relevantné kritériá | Je pravdepodobné, že sa bude vyžadovať posúdenie vplyvu na ochranu údajov? |
|---|---|---|
| Spracúvanie „osobných údajov pacientov alebo klientov jednotlivým lekárom, iným zdravotníckym pracovníkom alebo právnikom“ (odôvodnenie 91). | - citlivé údaje alebo údaje veľmi osobnej povahy<br>- údaje týkajúce sa zraniteľných dotknutých osôb | Nie |
| Online časopis využívajúci zoznam mailových adries na zasielanie všeobecného denného prehľadu svojim predplatiteľom. | - údaje spracúvané vo veľkom rozsahu | |
| Webová stránka vykonávajúca elektronický obchod, ktorá zobrazuje inzeráty na súčiastky na automobilové veterány, čo zahŕňa obmedzené profilovanie na základe položiek, ktoré sa na jej vlastnej webovej stránke prezerali alebo kúpili. | - hodnotenie alebo prideľovanie bodov | |

**Naopak, spracovateľská operácia môže zodpovedať uvedeným prípadom a prevádzkovateľ ju stále nemusí považovať za takú, ktorá „pravdepodobne povedie k vysokému riziku“. V takýchto prípadoch by prevádzkovateľ mal zdôvodniť a zdokumentovať dôvody nevykonania posúdenia vplyvu na osobné údaje a zahrnúť/zaznamenať názory zodpovednej osoby.**

Okrem toho ako súčasť zásady zodpovednosti každý prevádzkovateľ „*vedie záznamy o spracovateľských činnostiach, za ktoré je zodpovedný,*“ ktoré okrem iného zahŕňajú účel spracúvania, opis kategórií údajov a príjemcov údajov a „*podľa možností všeobecný opis technických a organizačných bezpečnostných opatrení uvedených v článku 32 ods. 1*“ (článok 30 ods. 1), pričom musí posúdiť, či je vysoké riziko pravdepodobné, aj keď sa nakoniec nerozhodne vykonať posúdenie vplyvu na ochranu údajov.

Poznámka: od dozorných orgánov sa vyžaduje, aby stanovili a zverejnili zoznam spracovateľských operácií, ktoré si vyžadujú posúdenie vplyvu na ochranu údajov, a zaslali ho Európskemu výboru pre ochranu údajov (článok 35 ods. 4)[18]. Kritériá uvedené vyššie môžu dozorným orgánom pomôcť vypracovať takýto zoznam, pričom v prípade potreby môžu neskôr doplniť konkrétnejší obsah. Napríklad spracúvanie akéhokoľvek druhu biometrických údajov alebo údajov týkajúcich sa detí by sa tiež mohlo považovať za relevantné na účely vypracovania zoznamu podľa článku 35 ods. 4.

b) Kedy nie je potrebné posúdenie vplyvu na ochranu údajov? Keď spracúvanie pravdepodobne nepovedie k vysokému riziku alebo existuje podobné posúdenie vplyvu na ochranu údajov, alebo sa schválilo pred májom 2018, alebo má právny

[18] V uvedenom kontexte, „*príslušný dozorný orgán [...] uplatní mechanizmus konzistentnosti uvedený v článku 63, ak takéto zoznamy zahŕňajú spracovateľské činnosti, ktoré súvisia s ponukou tovaru alebo služieb dotknutým osobám alebo sledovaním ich správania vo viacerých členských štátoch, alebo ak môžu podstatne ovplyvniť voľný pohyb osobných údajov v rámci Únie*“ (článok 35 ods. 6).

základ, alebo je na zozname spracovateľských operácií, pre ktoré sa posúdenie vplyvu na ochranu údajov nevyžaduje.

WP29 sa domnieva, že posúdenie vplyvu na ochranu údajov sa nevyžaduje v týchto prípadoch:

- **ak nie je pravdepodobné, že spracúvanie povedie k vysokému riziku pre práva a slobody fyzických osôb** (podľa článku 35 ods. 1),
- **ak sú povaha, rozsah, kontext a účely spracúvania veľmi podobné spracúvaniu, pre ktoré sa už posúdenie vplyvu na ochranu údajov vykonalo**. V takých prípadoch možno použiť výsledky posúdenia vplyvu na ochranu údajov pre podobné spracúvania (článok 35 ods. 1[19]),
- keď spracovateľské operácie skontroloval dozorný orgán pred májom 2018 v osobitných podmienkach, ktoré sa nezmenili[20] (pozri časť III.C),
- **ak má spracovateľská operácia** podľa článku 6 ods. 1 písm. c) alebo e) **právny základ** v práve EÚ alebo v práve členského štátu, pričom v tomto práve sa upravuje konkrétna spracovateľská operácia a **už vykonalo posúdenie vplyvu na ochranu údajov** ako súčasť stanovenia tohto právneho základu (článok 35 ods. 10)[21], okrem prípadov, ak členský štát uviedol, že posúdenie vplyvu na ochranu údajov sa musí vykonať pred začatím spracovateľských činností,
- **ak je spracúvanie zahrnuté do dobrovoľného zoznamu spracovateľských operácií (vypracovaného dozorným orgánom)**, v prípade ktorých sa nevyžaduje posúdenie vplyvu na ochranu údajov (článok 35 ods. 5). V takomto zozname sa môžu uvádzať spracovateľské činnosti, ktoré spĺňajú podmienky upresnené týmto orgánom, najmä prostredníctvom usmernení, konkrétnych rozhodnutí alebo povolení, pravidiel na dosiahnutie súladu, atď. (napr. vo Francúzsku, povolenia, výnimky, zjednodušené pravidlá, balíky opatrení na dosiahnutie súladu...). V takýchto prípadoch a s výhradou opätovného posúdenia príslušným dozorným orgánom sa posúdenie vplyvu na ochranu údajov nevyžaduje, ale len vtedy, ak spracúvanie jednoznačne patrí do rozsahu pôsobnosti príslušného postupu uvedeného v zozname a naďalej spĺňa všetky príslušné podmienky všeobecného nariadenia o ochrane údajov.

C. Ako postupovať v prípade už existujúcich spracovateľských operácií? V niektorých prípadoch sú potrebné posúdenia vplyvu na ochranu údajov.

**Požiadavka na vykonanie posúdenia vplyvu na ochranu údajov sa vzťahuje na existujúce spracovateľské operácie, ktoré pravdepodobne povedú k vysokému riziku pre práva a slobody fyzických osôb a v prípade ktorých došlo k zmene rizík, pričom sa zohľadní povaha, rozsah, kontext a účely spracúvania.**

[19] „*Pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziká, sa môže vykonať jedno posúdenie*“.

[20] „*Rozhodnutia, ktoré Komisia prijala, a povolenia, ktoré dozorné orgány vydali na základe smernice 95/46/ES, zostávajú v platnosti až do ich zmeny, nahradenia alebo zrušenia*“ (odôvodnenie 171).

[21] Keď sa posúdenie vplyvu na ochranu údajov vykonáva v etape vypracovania právneho predpisu, ktorým sa zabezpečí právny základ pre spracúvanie, je pravdepodobné, že pred začiatkom uplatňovania bude potrebné preskúmanie, keďže prijatý právny predpis sa môže odlišovať od návrhu spôsobmi, ktoré majú vplyv na otázky v oblasti súkromia a ochrany údajov. Okrem toho v čase prijatia právneho predpisu nemusia byť k dispozícii dostatočné technické informácie týkajúce sa skutočného spracúvania, aj keby ho sprevádzalo posúdenie vplyvu na ochranu údajov. V takýchto prípadoch môže stále byť potrebné vykonať pred uskutočnením samotných spracovateľských činností konkrétne posúdenie vplyvu na ochranu údajov.

Posúdenie vplyvu na ochranu údajov nie je potrebné v prípade spracovateľských operácií, ktoré skontroloval dozorný orgán alebo zodpovedná osoba, v súlade s článkom 20 smernice 95/46/ES, a ktoré sa vykonávajú spôsobom, ktorý sa od ich predchádzajúcej kontroly nezmenil. Skutočne „*rozhodnutia, ktoré Komisia prijala, a povolenia, ktoré dozorné orgány vydali na základe smernice 95/46/ES, zostávajú v platnosti až do ich zmeny, nahradenia alebo zrušenia*“ (odôvodnenie 171).

Naopak to znamená, že akékoľvek spracúvanie údajov, ktorého podmienky vykonávania (rozsah, účel, získané osobné údaje, totožnosť prevádzkovateľov alebo príjemcov, obdobie uchovávania údajov, technické a organizačné opatrenia atď.) sa od predchádzajúcej kontroly uskutočnenej dozorným orgánom alebo zodpovednou osobou zmenili a ktoré pravdepodobne povedie k vysokému riziku, by malo podliehať posúdeniu vplyvu na ochranu údajov.

Posúdenie vplyvu na ochranu údajov by sa okrem toho mohlo vyžadovať aj po zmene rizík vyplývajúcich zo spracovateľských operácií[22], napríklad preto, že sa začala používať nová technológia alebo osobné údaje sa používajú na iný účel. Operácie spracúvania údajov sa môžu rýchlo vyvíjať a môžu sa objaviť nové zraniteľné miesta. Preto je potrebné poznamenať, že revízia posúdenia vplyvu na ochranu údajov je nielen užitočná na neustále zlepšovanie, ale aj kľúčová na zachovanie úrovne ochrany údajov v prostredí, ktoré sa v priebehu času mení. Posúdenie vplyvu na ochranu údajov môže byť potrebné aj preto, že sa zmenil organizačný alebo spoločenský kontext pre spracovateľskú činnosť, napríklad z dôvodu, že účinky určitých automatizovaných rozhodnutí sa stali závažnejšie alebo nové kategórie dotknutých osôb sa stali zraniteľnejšie voči diskriminácii. Každý z týchto príkladov môže byť prvkom, ktorý vedie k zmene rizika vyplývajúceho z príslušnej spracovateľskej činnosti.

Naopak, riziko by mohli znížiť aj určité zmeny. Spracovateľská operácia by sa napr. mohla vyvinúť tak, že rozhodnutia už nie sú automatizované alebo monitorovacia činnosť už nie je systematická. V takom prípade sa na základe preskúmania vykonanej analýzy rizík môže ukázať, že uskutočnenie posúdenia vplyvu na ochranu údajov sa už nevyžaduje.

V duchu dobrej praxe by sa **posúdenie vplyvu na ochranu údajov malo neustále preskúmavať a pravidelne prehodnocovať.** Preto, aj keď sa posúdenie vplyvu na ochranu údajov nebude vyžadovať 25. mája 2018, prevádzkovateľ bude takéto posúdenie vo vhodnom čase musieť vykonať ako súčasť jeho všeobecných povinností týkajúcich sa zodpovednosti.

D. Ako sa má vykonať posúdenie vplyvu na ochranu údajov?

a) V ktorom okamihu sa má vykonať posúdenie vplyvu na ochranu údajov? Pred spracúvaním.

**Posúdenie vplyvu by sa malo vykonať „*pred spracúvaním*“ (článok 35 ods. 1 a článok 35 ods. 10, odôvodnenia 90 a 93)[23]. Je to v súlade so zásadami týkajúcimi sa špecificky navrhnutej**

[22] Pokiaľ ide o kontext, získané údaje, účely, funkcie, spracované osobné údaje, príjemcovia, kombinácie údajov, riziká (podporné aktíva, zdroje rizík, prípadné dôsledky, hrozby atď.), bezpečnostné opatrenia a medzinárodné prenosy.

[23] Okrem prípadov, keď ide už o existujúce spracúvanie, ktoré vopred skontroloval dozorný orgán, pričom v takomto prípade by sa posúdenie vplyvu na ochranu údajov malo vykonať pred uskutočnením závažných zmien.

**a štandardnej ochrany údajov (článok 25 odôvodnenie 78). Posúdenie vplyvu na ochranu údajov by sa malo vnímať ako pomocný nástroj pri rozhodovaní o spracúvaní.**

S posudzovaním vplyvu na ochranu údajov by sa malo začať čo najskôr pri navrhovaní spracovateľskej operácie, aj keď niektoré spracovateľské operácie ešte nie sú známe. Aktualizáciou posúdenia vplyvu na ochranu údajov prostredníctvom projektu životného cyklu sa zabezpečí zohľadnenie ochrany údajov a súkromia a podnieti to vytvorenie riešení, ktorými sa podporuje dodržiavanie predpisov. V priebehu procesu vývoja môže byť tiež potrebné zopakovať jednotlivé kroky posúdenia, keďže výber určitých technických alebo organizačných opatrení môže mať vplyv na závažnosť alebo pravdepodobnosť rizík, ktoré predstavuje spracúvanie.

To, že posúdenie vplyvu na ochranu údajov možno bude potrebné po reálnom začatí spracúvania aktualizovať, nie je platným dôvodom na to, aby sa takéto posúdenie odložilo alebo nevykonalo. Posúdenie vplyvu na ochranu údajov je prebiehajúci proces, najmä v prípadoch, keď je spracovateľská operácia dynamická a podlieha neustálej zmene. **Vykonávanie posúdenia vplyvu na ochranu údajov je neustály proces, a nie jednorázová záležitosť**.

b) Kto je povinný vykonať posúdenie vplyvu na ochranu údajov? Prevádzkovateľ so zodpovednou osobou a spracovateľmi.

**Zodpovednosťou prevádzkovateľa je zabezpečiť vykonanie posúdenia vplyvu na ochranu údajov (článok 35 ods. 2)**. Posúdenie vplyvu na ochranu údajov môže vykonať niekto iný, či už z organizácie alebo mimo nej, ale v konečnom dôsledku je za túto úlohu zodpovedný prevádzkovateľ.

**Prevádzkovateľ sa musí tiež poradiť so zodpovednou osobou**, ak je určená (článok 35 ods. 2), a táto rada a rozhodnutia prijaté prevádzkovateľom by sa mali zdokumentovať v posúdení vplyvu na ochranu údajov. Zodpovedná osoba by mala tiež monitorovať vykonávanie posúdenia vplyvu na ochranu údajov [článok 39 ods. 1 písm. c)]. Ďalšie usmernenie sa uvádza v usmerneniach WP29 týkajúcich sa zodpovednej osoby 16/EN WP 243.

Ak spracúvanie úplne alebo čiastočne vykonáva sprostredkovateľ údajov, mal by prevádzkovateľovi pomáhať pri výkone posúdenia vplyvu na ochranu údajov a poskytnúť všetky potrebné informácie [v súlade s článkom 28 ods. 3 písm. f)].

**Prevádzkovateľ sa musí podľa potreby usilovať *získať názory dotknutých osôb alebo ich zástupcov* (článok 35 ods. 9)**. WP29 sa domnieva, že:

- o získanie týchto názorov by sa malo v závislosti od kontextu usilovať rôznymi spôsobmi (napr. všeobecnou štúdiou týkajúcou sa účelu a prostriedkov spracovateľskej operácie, otázkou pre zástupcov zamestnancov alebo obvyklými prieskumami zasielanými budúcim zákazníkom prevádzkovateľa), pričom je potrebné zabezpečiť, aby prevádzkovateľ mal právny základ pre spracúvanie akýchkoľvek osobných údajov, ktoré súvisia s úsilím o získanie uvedených názorov. Hoci je potrebné poznamenať, že súhlas so spracúvaním samozrejme nie je spôsob ako získať názory dotknutých osôb;
- ak sa konečné rozhodnutie prevádzkovateľa líši od názorov dotknutých osôb, mali by sa zdokumentovať jeho dôvody na to, či sa bude v spracúvaní pokračovať alebo nie;
- prevádzkovateľ by mal zdokumentovať aj svoje odôvodnenie, prečo sa neusiloval získať názory dotknutých osôb, ak sa rozhodol, že to nie je vhodné, napríklad ak by to viedlo k narušeniu dôvernosti podnikateľských plánov spoločností alebo by bolo neprimerané alebo nepraktické.

Nakoniec, je dobrou praxou, aby sa v závislosti od vnútornej politiky vymedzili a zdokumentovali iné špecifické úlohy a zodpovednosti, procesy a pravidlá, napr.:

- ak konkrétne podnikateľské jednotky môžu navrhnúť vykonanie posúdenia vplyvu na ochranu údajov, mali k tomuto posúdeniu prispieť a mali by byť zapojené do procesu jeho validácie;
- ak je to vhodné, odporúča sa zabezpečiť poradenstvo od nezávislých expertov z rôznych profesií[24] (právnikov, IT expertov, bezpečnostných expertov, sociológov, expertov v oblasti etiky atď.)
- úlohy a zodpovednosti sprostredkovateľov musia byť zmluvne vymedzené; a posúdenie vplyvu na ochranu údajov sa musí vykonať s pomocou sprostredkovateľa s prihliadnutím na povahu spracúvania a informácie dostupné sprostredkovateľovi [článok 28 ods. 3 písm. f)];
- hlavný úradník pre informačnú bezpečnosť, ak sa vymenuje, ako aj zodpovedná osoba by mohli navrhnúť, aby prevádzkovateľ vykonal posúdenie vplyvu na ochranu údajov v súvislosti s konkrétnou spracovateľskou operáciou, a mal by pomôcť zainteresovaným stranám s metodikou, s hodnotením kvality posúdenia rizík a s tým, či je zvyškové riziko prijateľné, ako aj s rozvojom poznatkov, ktoré sú špecifické pre kontext daného prevádzkovateľa;
- hlavný úradník pre informačnú bezpečnosť, ak sa vymenuje, a/alebo IT oddelenie, by mali prevádzkovateľovi poskytnúť pomoc a v závislosti od bezpečnostných a prevádzkových potrieb by mohli navrhnúť vykonanie posúdenia vplyvu na ochranu údajov v súvislosti s konkrétnou spracovateľskou operáciou.

c) Aká metodika sa má použiť na vykonanie posúdenia vplyvu na ochranu údajov? Rôzne metodiky alebo spoločné kritériá.

[24] *Odporúčania pre Európsku úniu týkajúce sa rámca na posúdenie vplyvu na ochranu údajov, cieľ D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

Vo všeobecnom nariadení o ochrane údajov sa stanovujú minimálne prvky posúdenia vplyvu na ochranu údajov (článok 35 ods. 7 a odôvodnenia 84 a 90):

- „ *opis plánovaných spracovateľských operácií a účely spracúvania*“;
- „*posúdenie nutnosti a primeranosti spracúvania*“;
- „*posúdenie rizík pre práva a slobody dotknutých osôb*“;
- „*opatrenia na*:
  - *„riešenie rizík*“;
  - *„preukázanie súladu s týmto nariadením*“.

Nasledujúci obrázok ilustruje všeobecný iteratívny proces vykonávania posúdenia vplyvu na ochranu údajov[25]:


Pri posudzovaní vplyvu určitej spracovateľskej operácie je potrebné zohľadniť (článok 35 ods. 8) dodržiavanie kódexu správania (článok 40). Môže to byť užitočné na preukázanie toho, že sa vybrali alebo zaviedli primerané opatrenia, a to za predpokladu, že kódex správania je pre spracovateľskú operáciu primeraný. Na účely toho, aby prevádzkovatelia a spracovatelia preukázali, že sa pri spracovateľských operáciách dodržiava všeobecné nariadenie o ochrane údajov (článok 42), ako aj záväzné vnútropodnikové pravidlá, by sa mala zohľadniť aj certifikácia, pečate a značky.

Vo všetkých relevantných požiadavkách uvedených vo všeobecnom nariadení o ochrane údajov sa stanovuje široký všeobecný rámec na navrhnutie a vykonanie posúdenia vplyvu na ochranu údajov.

[25] Je potrebné zdôrazniť, že proces, ktorý sa tu uvádza, je iteratívny: v praxi je pravdepodobné, že pred tým, ako posúdenie vplyvu na ochranu údajov ukončí, sa každá z etáp niekoľko krát zopakuje.

Praktické vykonávanie posúdenia vplyvu na ochranu údajov bude závisieť od požiadaviek stanovených vo všeobecnom nariadení o ochrane údajov, ktoré možno doplniť podrobnejšími praktickými usmerneniami. Vykonávanie posúdenia vplyvu na ochranu údajov je preto odstupňovateľné. Znamená to, že aj malý prevádzkovateľ môže navrhnúť a vykonať posúdenie vplyvu na ochranu údajov, ktoré je vhodné pre ich spracovateľské operácie.

V odôvodnení 90 všeobecného nariadenia o ochrane údajov sa uvádza viacero prvkov posúdenia vplyvu na ochranu údajov, ktoré sa prekrývajú s dobre vymedzenými prvkami riadenia rizika (napr. ISO 31000[26]). V terminológii riadenia rizík je cieľom posúdenia vplyvu na ochranu údajov „riadenie rizík" pre práva a slobody fyzických osôb, pričom sa využívajú tieto procesy:

- stanovenie kontextu: „*zohľadnenie povahy, rozsahu, kontextu a účelu spracúvania a zdrojov*";
- posúdenie rizík: „*posúdenie osobitnej pravdepodobnosti a závažnosti vysokého rizika*";
- riešenie rizík: „*zmiernenie daného rizika*" a „*zabezpečenie ochrany osobných údajov*" a „*preukázanie súladu s týmto nariadením*".

Poznámka: posúdenie vplyvu na ochranu údajov vykonávané v rámci všeobecného nariadenia o ochrane údajov je nástrojom riadenia rizík pre práva dotknutých osôb, a tým zohľadňuje ich pohľad, ako je to v prípade niektorých oblastí (napr. bezpečnosť spoločnosti). Naopak, riadenie rizík v iných oblastiach (napr. informačná bezpečnosť) je zamerané na konkrétnu organizáciu.

Vo všeobecnom nariadení o ochrane údajov sa prevádzkovateľom umožňuje, aby stanovili presnú štruktúru a podobu posúdenia vplyvu na ochranu údajov, aby tak toto posúdenie bolo v súlade s existujúcimi pracovnými postupmi. V EÚ a na celom svete je viacero rozdielnych etablovaných postupov, v ktorých sa zohľadňujú prvky opísané v odôvodnení 90. Bez ohľadu na formu posúdenia vplyvu na ochranu údajov však musí ísť o skutočné posúdenie rizík, ktoré prevádzkovateľom umožní prijať opatrenia na ich vyriešenie.

S cieľom pomôcť pri vykonávaní základných požiadaviek stanovených vo všeobecnom nariadení o ochrane údajov sa môžu použiť rôzne metodiky (príklady metodiky na ochranu údajov a metodiky na posúdenie vplyvu na ochranu údajov sa uvádzajú v prílohe 1). Aby mohli tieto rozdielne prístupy existovať a prevádzkovateľom sa zároveň umožnilo dodržiavať ustanovenia všeobecného nariadenia o ochrane údajov, identifikovali sa spoločné kritériá (pozri prílohu 2). Objasňujú sa v nich základné požiadavky nariadenia, ale poskytujú dostatočný priestor pre rôzne formy vykonávania. Tieto kritéria sa môžu použiť na preukázanie toho, že konkrétna metodika posúdenia vplyvu na ochranu údajov spĺňa normy požadované vo všeobecnom nariadení o ochrane údajov. **Výber metodiky zostáva na prevádzkovateľovi, ale táto metodika by mala byť v súlade s kritériami uvedenými v prílohe 2.**

WP29 nabáda na to, aby sa pre každý sektor vypracovali samostatné rámce na posúdenie vplyvu na ochranu údajov. Je to z toho dôvodu, že takéto rámce môžu vychádzať zo znalostí špecifických pre daný sektor, t. z., že v posúdení vplyvu na ochranu údajov sa môžu riešiť špecifické aspekty konkrétneho druhu spracovateľskej operácie (napr. konkrétne typy údajov, podnikové aktíva, potenciálne dôsledky, hrozby, opatrenia). Znamená to, že v posúdení vplyvu na ochranu údajov sa môžu riešiť problémy, ktoré vznikajú v konkrétnom hospodárskom sektore alebo pri použití konkrétnych technológií alebo pri vykonávaní konkrétnych typov spracovateľskej operácie.

[26] Procesy riadenia rizík: komunikácia a konzultácia, stanovenie kontextu, posúdenie rizík, riešenie rizík, monitorovanie a preskúmanie (pozri termíny a vymedzenia pojmov a obsah v náhľade ISO 31000: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

Nakoniec, v prípade potreby „*prevádzkovateľ vykoná prehodnotenie s cieľom posúdiť, či sa spracúvanie uskutočňuje v súlade s posúdením vplyvu na ochranu údajov, a to aspoň vtedy, keď došlo k zmene rizika, ktoré predstavujú spracovateľské operácie*“ (článok 35 ods. 11[27]).

d) Existuje povinnosť zverejniť posúdenie vplyvu na ochranu údajov? Nie, ale zverejnenie súhrnu by mohlo podporiť dôveru a v prípade predchádzajúcej konzultácie alebo, ak o to požiadala zodpovedná osoba, sa dozornému orgánu musí zaslať úplné posúdenie vplyvu na ochranu údajov.

**Zverejnenie posúdenia vplyvu na ochranu údajov nie je právnou požiadavkou uvedenou vo všeobecnom nariadení o ochrane údajov, závisí od rozhodnutia prevádzkovateľa. Prevádzkovatelia by však mali zvážiť zverejnenie aspoň niektorých častí, ako je napríklad súhrn alebo záver ich posúdenia vplyvu na ochranu údajov.**

Účelom takéhoto postupu by bolo pomôcť posilniť dôveru v spracovateľské operácie prevádzkovateľa a preukázať zodpovednosť a transparentnosť. Osobitne dobrou praxou je zverejniť posúdenie vplyvu na ochranu údajov, ak je touto spracovateľskou operáciou dotknutá časť verejnosti. Mohlo by ísť najmä o prípad, ak posúdenie vplyvu na ochranu údajov vykonáva orgán verejnej moci.

Zverejnené posúdenie vplyvu na ochranu údajov nemusí obsahovať celé posúdenie, najmä v prípadoch, ak by sa v ňom mohli uvádzať konkrétne informácie o bezpečnostných rizikách pre prevádzkovateľa alebo by sa mohli prezradiť obchodné tajomstvá alebo citlivé obchodné informácie. Za takýchto okolností by zverejnená verzia mohla pozostávať len zo súhrnu hlavných zistení posúdenia vplyvu na ochranu údajov alebo dokonca len z vyhlásenia, že sa takéto posúdenie vykonalo.

Okrem toho, ak sa na základe posúdenia vplyvu na ochranu údajov odhalia vysoké zvyškové riziká, od prevádzkovateľa sa bude vyžadovať, aby pred spracúvaním konzultoval s dozorným orgánom (článok 36 ods. 1). Súčasťou toho je, že posúdenie vplyvu na ochranu údajov sa musí poskytnúť v plnej miere [článok 36 ods. 3 písm. e)]. Dozorný orgán môže poskytnúť poradenstvo[28] a nenaruší obchodné tajomstvá ani neprezradí zraniteľné miesta v oblasti bezpečnosti, a to s výhradou zásad uplatniteľných v každom členskom štáte, ktoré sa týkajú prístupu verejnosti k úradným dokumentom.

E. Kedy sa musí konzultovať dozorný orgán? Keď sú zvyškové riziká vysoké.

Ako sa vysvetľuje vyššie:

- posúdenie vplyvu na ochranu údajov sa vyžaduje len vtedy, keď spracovateľská operácia „*pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb*“ (článok 35 ods. 1, pozri časť III.B.a). Napr., spracúvanie údajov o zdravotnom stave vo veľkom rozsahu sa považuje za také spracúvanie, ktoré pravdepodobne povedie k vysokému riziku a vyžaduje si posúdenie vplyvu na ochranu údajov;
- potom je zodpovednosťou prevádzkovateľa, aby posúdil riziká pre práva a slobody dotknutých osôb a identifikoval opatrenia[29] plánované na zníženie uvedených rizík na akceptovateľnú úroveň a preukázal súlad so všeobecným nariadením o ochrane údajov (článok 35 ods. 7, pozri

[27] V článku 35 ods. 10 sa vyslovene vylučuje len uplatňovanie článku 35 ods. 1 až 7.

[28] Písomná odpoveď prevádzkovateľovi je potrebná len v tom prípade, keď sa dozorný orgán domnieva, že plánované spracúvanie nie je v súlade s týmto nariadením podľa článku 36 ods. 2.

[29] Vrátane zohľadnenia existujúcich usmernení od Európskeho výboru pre ochranu údajov a dozorných orgánov a so zreteľom na technologickú úroveň a náklady na vykonávanie, ako sa uvádza v článku 35 ods. 1.

časť III.C.c). Príkladom pre uchovávanie osobných údajov na prenosných počítačoch by popri existujúcich postupoch (oznam, súhlas, právo na prístup, právo namietať atď.) mohlo byť používanie primeraných technických a organizačných bezpečnostných opatrení (účinné úplné šifrovanie pevného disku, rozsiahla správa kľúčov, primeraná kontrola prístupu, zabezpečené zálohovania atď.)

Pokiaľ ide o prípad s prenosným počítačom uvedený vyššie, ak sa prevádzkovateľ domnieva, že riziká sa dostatočne znížili, a v zmysle článku 36 ods. 1 a odôvodnení 84 a 94 môže spracúvanie pokračovať bez konzultácie s dozorným orgánom. V prípadoch, keď prevádzkovateľ nemôže dostatočne znížiť identifikované riziká (t. j. zvyškové riziká zostávajú vysoké), musí konzultovať s dozorným orgánom.

K príkladom neakceptovateľného vysokého zvyškového rizika patria prípady, keď dotknuté osoby môžu byť vystavené závažným alebo dokonca nezvratným dôsledkom, ktoré nemusia dokázať prekonať (napr. neoprávnený prístup k údajom, ktorý vedie k ohrozeniu života dotknutých osôb, prepusteniu, ohrozeniu finančnej situácie), a/alebo, keď sa ukazuje ako zrejmé, že k riziku dôjde (napr. nie je možné znížiť počet osôb s prístupom k údajom z dôvodu toho, ako sa údaje vymieňajú, používajú alebo rozširujú alebo, ak sa známe zraniteľné miesto z bezpečnostného hľadiska neopraví).

**Keď prevádzkovateľ nedokáže nájsť dostatočné opatrenia na zníženie rizík na akceptovateľnú úroveň (t.j. zvyškové riziká sú naďalej vysoké), vyžaduje sa konzultácia s dozorným orgánom[30].**

Okrem toho, prevádzkovateľ bude musieť uskutočniť konzultácie s dozorným orgánom vždy, keď sa v práve členského štátu vyžaduje, aby prevádzkovatelia uskutočnili konzultácie s dozorným orgánom a/alebo od neho získali predchádzajúce povolenie v súvislosti so spracúvaním vykonávaným prevádzkovateľom na plnenie úlohy prevádzkovateľa vo verejnom záujme vrátane spracúvania v súvislosti so sociálnym zabezpečením a verejným zdravím (článok 36 ods. 5).

Je však potrebné poznamenať, že bez ohľadu na to, či sa podľa úrovne zvyškového rizika vyžaduje konzultácia s dozorným orgánom, povinnosť uchovávať záznam o posúdení vplyvu na ochranu údajov a aktualizovať posúdenie vplyvu na ochranu údajov v náležitom čase zostáva zachovaná.

## IV. Závery a odporúčania

Posúdenia vplyvu na ochranu údajov sú pre prevádzkovateľov užitočným spôsobom, ako zaviesť systémy na spracúvanie údajov, ktoré spĺňajú všeobecné nariadenie o ochrane údajov, a v prípade niektorých druhov spracovateľských operácií môžu byť povinné. Sú odstupňovateľné a môžu mať rôznu podobu, ale vo všeobecnom nariadení o ochrane údajov sa stanovujú základné požiadavky účinného posúdenia vplyvu na ochranu údajov. Prevádzkovatelia by mali vnímať vykonanie posúdenia vplyvu na ochranu údajov ako užitočnú a pozitívnu činnosť, ktorá pomáha pri dodržiavaní právnych predpisov.

V článku 24 ods. 1 sa stanovuje základná zodpovednosť prevádzkovateľa, pokiaľ ide o dodržiavanie všeobecného nariadenia o ochrane údajov: „*S ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody*

[30] Poznámka: „*pseudonymizácia a šifrovanie osobných údajov*“ (ako aj minimalizácia údajov, mechanizmy dohľadu atď.) nie sú nevyhnutne primerané opatrenia. Sú len príkladmi. Primerané opatrenia závisia od kontextu a rizík, ktoré sú špecifické pre príslušné spracovateľské operácie.

*fyzických osôb prevádzkovateľ prijme vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie sa vykonáva v súlade s týmto nariadením. Uvedené opatrenia sa podľa potreby preskúmajú a aktualizujú*“.

Posúdenie vplyvu na ochranu údajov je kľúčovou časťou zabezpečenia súladu s nariadením v prípadoch, keď sa plánuje alebo vykonáva spracúvanie údajov, pri ktorom dochádza k vysokému riziku. Znamená to, že prevádzkovatelia by mali použiť kritériá uvedené v tomto dokumente s cieľom určiť, či sa má vykonať posúdenie vplyvu na ochranu údajov. Na základe internej politiky prevádzkovateľa by tento zoznam mohol ísť nad rámec zákonných požiadaviek uvedených vo všeobecnom nariadení o ochrane údajov. Malo by to viesť k väčšej dôvere dotknutých osôb a iných prevádzkovateľov.

Ak sa plánuje spracúvanie s pravdepodobne vysokým rizikom, prevádzkovateľ musí:

- vybrať metodiku posúdenia vplyvu na ochranu údajov (príklady sa uvádzajú v prílohe 1), ktorá spĺňa kritéria uvedené v prílohe 2, alebo stanoviť a vykonať systematický proces posúdenia vplyvu na ochranu údajov, ktorý:
  - spĺňa kritériá uvedené v prílohe 2,
  - je integrovaný do existujúcich procesov týkajúcich sa návrhu, vývoja, zmeny, rizika a do operačných postupov v oblasti preskúmania, a to v súlade s vnútornými procesmi, kontextom a kultúrou,
  - zahŕňa primerané zainteresované strany a jasne vymedzuje ich zodpovednosť (prevádzkovateľ, zodpovedná osoba, dotknuté osoby alebo ich zástupcovia, podniky, technické služby, sprostredkovatelia, úradník pre informačnú bezpečnosť atď.),
- v prípade požiadania poskytnúť príslušnému dozornému orgánu správu o posúdení vplyvu na ochranu údajov,
- konzultovať s dozorným orgánom, keď nedokáže určiť dostatočné opatrenia na zmiernenie vysokých rizík,
- pravidelne prehodnocovať posúdenie vplyvu na ochranu údajov a spracúvanie, ktoré sa ním posudzuje, a to aspoň vtedy, keď došlo k zmene rizika, ktoré predstavujú spracovateľské operácie,
- dokumentovať prijaté rozhodnutia.

## Príloha 1 – príklady existujúcich rámcov EÚ na posúdenie vplyvu na ochranu údajov

Vo všeobecnom nariadení o ochrane údajov sa neupresňuje, ktoré procesy posúdenia vplyvu na ochranu údajov sa majú používať, ale namiesto toho sa prevádzkovateľom umožňuje, aby zaviedli rámec dopĺňajúci ich existujúce pracovné postupy za predpokladu, že sa pri tom zohľadňujú prvky opísané v článku 35 ods. 7. Takýto rámec môže byť prispôsobený konkrétnemu prevádzkovateľovi alebo spoločný pre určitý sektor. Predtým zverejnené rámce, ktoré vypracovali orgány pre ochranu osobných údajov, a sektorovo špecifické rámce EÚ zahŕňajú (nielen):

príklady všeobecných rámcov EÚ:

- Nemecko: štandardný vzor na ochranu údajov, V.1.0 – skúšobná verzia, 2016[31]. https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- Španielsko: *Príručka pre posúdenie vplyvu na ochranu údajov* (*Guía para una Evaluación de Impacto en la Protección de Datos Personales – EIPD)*, Španielska agentúra pre ochranu údajov (Agencia española de protección de datos – AGPD), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- Francúzsko: *Posúdenie vplyvu na súkromie* (*Privacy Impact Assessment – PIA)*, Národná komisia pre informatiku a slobody (Commission nationale de l'informatique et des libertés – CNIL), 2015. https://www.cnil.fr/fr/node/15798
- Spojené kráľovstvo: *Kódex postupov pre vykonávanie posúdení vplyvu na súkromie* (*Conducting privacy impact assessments code of practice*), Úrad komisára pre informácie (Information Commissioner's Office – ICO), 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Príklady sektorovo špecifických rámcov EÚ:

- Rámec posudzovania vplyvu na súkromie a ochranu údajov, pokiaľ ide o aplikácie využívajúce rádiofrekvenčnú identifikáciu[32]. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Vzor na posúdenie vplyvu inteligentných sietí a inteligentných meracích systémov na ochranu údajov[33]

---

[31] Jednomyseľne schválený a potvrdený (Bavorsko sa zdržalo) na 92. konferencii nezávislých orgánov pre ochranu osobných údajov spolku a spolkových krajín v Kühlungsborne 9. – 10. novembra 2016.

[32] Pozri aj:

- Odporúčanie Komisie z 12. mája 2009 o vykonávaní zásad ochrany súkromia a údajov v aplikáciách, ktoré podporujú rádiofrekvenčnú identifikáciu. https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Stanovisko 9/2011 k revidovanému sektorovému návrhu na rámec posudzovania vplyvu na súkromie a ochranu údajov, pokiaľ ide o aplikácie využívajúce rádiofrekvenčnú identifikáciu. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf

[33] Pozri aj stanovisko 07/2013 k vzoru na posúdenie vplyvu inteligentných sietí a inteligentných meracích systémov na ochranu údajov (vzor DPIA), ktorý vypracovala expertná skupina 2 v rámci osobitnej skupiny Komisie pre inteligentné siete. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

V medzinárodnom štandarde sa poskytnú aj usmernenia pre metodiku, ktorá sa má používať na vykonanie posúdenia vplyvu na ochranu údajov (ISO/IEC 29134[34]).

[34] ISO/IEC 29134 (projekt), *Informačné technológie – Bezpečnostné techniky – Posúdenie vplyvu na súkromie – Usmernenia*, Medzinárodná organizácia pre normalizáciu (ISO).

## Príloha 2 – kritéria prijateľného posúdenia vplyvu na ochranu údajov

WP29 navrhuje nasledujúce kritériá, ktoré môžu prevádzkovatelia použiť na posúdenie toho, či je posúdenie vplyvu na ochranu údajov alebo metodika na jeho vykonanie dostatočne komplexná na splnenie všeobecného nariadenia o ochrane údajov:

- ☐ je k dispozícii systematický opis spracúvania [článok 35 ods. 7 písm. a)]:
  - ☐ zohľadnila sa povaha, rozsah, kontext a účely spracúvania (odôvodnenie 90),
  - ☐ sú zaznamenané osobné údaje, príjemcovia a obdobie, na ktoré sa budú osobné údaje uchovávať,
  - ☐ je k dispozícii funkčný opis spracovateľskej operácie,
  - ☐ identifikovali sa aktíva, ktoré vplývajú na spracovanie osobných údajov (hardvér, softvér, siete, ľudia, papier alebo kanály na prenos papiera),
  - ☐ zohľadnilo sa dodržiavanie schválených kódexov správania (článok 35 ods. 8),
- ☐ posúdila sa nutnosť a primeranosť [článok 35 ods. 7 písm. b)]:
  - ☐ stanovili sa opatrenia na dosiahnutie súladu s nariadením [článok 35 ods. 7 písm. d) a odôvodnenie 90], pričom sa zohľadnili:
    - ☐ opatrenia prispievajúce k primeranosti a nutnosti spracúvania na základe:
      - ☐ konkrétne určeného, výslovne uvedeného a legitímneho účelu (-ov) [článok 5 ods. 1 písm. b)],
      - ☐ zákonnosti spracúvania (článok 6),
      - ☐ primeranosti, relevantnosti a obmedzenia na to, ktoré údaje sú potrebné [článok 5 ods. 1 písm. c)],
      - ☐ obmedzenej doby uchovávania [článok 5 ods. 1 písm. e)],
    - ☐ opatrenia prispievajúce k právam dotknutých osôb:
      - ☐ informácie poskytnuté dotknutej osobe (články 12, 13 a 14),
      - ☐ právo na prístup k údajom a právo na prenosnosť údajov (články 15 a 20),
      - ☐ právo na opravu a právo na vymazanie (články 16, 17 a 19),
      - ☐ právo namietať a právo na obmedzenie spracúvania (články 18, 19 a 21),
      - ☐ vzťah so sprostredkovateľom (článok 28),
      - ☐ záruky v súvislosti s medzinárodným prenosom (-mi) (kapitola V),
      - ☐ predchádzajúca konzultácia (článok 36).
- ☐ riadia sa riziká pre práva a slobody dotknutých osôb [článok 35 ods. 7 písm. c)]:
  - ☐ zhodnotil sa pôvod, povaha, osobitosť a závažnosť rizík (pozri odôvodnenie 84) alebo, konkrétnejšie, každé riziko (neoprávnený prístup, neželané úpravy a strata údajov) sa posúdilo z pohľadu dotknutých osôb:
    - ☐ zohľadnili sa zdroje rizík (odôvodnenie 90),
    - ☐ identifikovali sa prípadné dôsledky na práva a slobody dotknutých osôb v súvislosti s určitými prípadmi vrátane neoprávneného prístupu, neželaných úprav a straty údajov,
    - ☐ identifikovali sa hrozby, ktoré by mohli viesť k neoprávnenému prístupu, neželaným úpravám a strate údajov,
    - ☐ odhadla sa pravdepodobnosť a závažnosť (odôvodnenie 90),
  - ☐ stanovili sa opatrenia na riešenie uvedených rizík [článok 35 ods. 7 písm. d) a odôvodnenie 90],
- ☐ zapojili sa zainteresované strany:
  - ☐ zodpovedná osoba poskytla poradenstvo (článok 35 ods. 2),

podľa potreby sa vynaloží úsilie na získanie názorov dotknutých osôb alebo ich zástupcov (článok 35 ods. 9).