POSÚDENIE VPLYVU NA OCHRANU OSOBNÝCH ÚDAJOV
DATA PROTECTION IMPACT ASSESSMENT

Mária Kevická[1]

https://doi.org/10.24040/pros.07.05.2021.ssp.102-117

Abstrakt

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 tým, že sa tieto riziká posúdia a určia sa opatrenia na vysporiadanie sa s nimi. Je to proces budovania a preukazovania zhody.[2]

Kľúčové slová

osobný údaj, osobitná kategória osobných údajov, ochrana osobných údajov, posúdenie vplyvu na ochranu údajov, princíp zodpovednosti, analýza právnych rizík pre práva a slobody fyzických osôb, spracovateľská operácia, automatizované spracúvanie, veľký rozsah osobných údajov, systematické monitorovanie dotknutých osôb, súlad

Abstract

A data protection impact assessment is a process designed to describe the processing, assess its necessity and adequacy, as well as to help manage the risks to the rights and freedoms of individuals arising from the processing of personal data by assessing those risks and identifying measures to deal with them. It is a process of building and demonstrating compliance.

Keywords

personal data, special categories of personal data, personal data protection, data protection impact assessment, principle of responsibility, analysis of legal risks to the rights and freedoms of natural persons, processing operation, automated processing, large amount of personal data, systematic monitoring of data subject, compliance

[1] JUDr. Mária Kevická, PhD., riaditeľka neziskovej organizácie, komunálna právnička, konzultantka v oblasti ochrany osobných údajov

[2] WP 29: Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“. Dostupné na: https://ec.europa.eu/newsroom/article29/items/611236 .

Úvod

Posúdenie vplyvu na ochranu osobných údajov je jednou z povinností, ktoré ukladá Všeobecné nariadenie o ochrane osobných údajov[3] prevádzkovateľom pri spracúvaní osobných údajov. Predstavuje inštitút, ktorý nahrádza notifikačnú povinnosť ustanovenú v Slovenskej republike zákonom č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Posúdenie vplyvu na ochranu údajov je veľmi dôležitý proces, počas ktorého prevádzkovateľ posudzuje riziká pre práva a slobody fyzických osôb, ktoré potenciálne vznikajú pri spracúvaní ich osobných údajov a následne sa snaží s predmetnými rizikami vysporiadať. Vypracovanie posúdenia vplyvu pomáha prevádzkovateľovi preukázať princíp zodpovednosti vo vzťahu k spracúvaniu osobných údajov a súlad s nariadením. Prípadná absencia posúdenia vplyvu môže mať za následok uloženie pokuty zo strany dozorného orgánu vo výške do 10 mi. EUR alebo do 2% celosvetového obratu.

Právo na ochranu osobných údajov

V rámci právnej teórie existujú tri názorové prúdy, ktoré vymedzujú postavenie práva na ochranu osobných údajov v rámci hierarchie ľudských práv. Prvý názorový prúd považuje právo na ochranu osobných údajov za samostatné právo, ktoré chráni viacero objektov vrátane súkromia. Druhý názorový prúd považuje právo na ochranu súkromia za derivát práva na súkromie. Tretí názorový prúd uvádza, že právo na ochranu osobných údajov dopĺňa právo na súkromie. Máme za to, že právo na ochranu osobných údajov je právo samostatné, a to najmä z dôvodu, že porušením práva na ochranu osobných údajov nemusí bezprostredne dôjsť k porušeniu práva na súkromie.

Vymedzenie práva na ochranu osobných údajov nachádzame v nasledovných právnych aktoch: Všeobecná deklarácia ľudských práv (1948), Dohovor o ochrane ľudských práv a základných slobôd (1950), Charta základných práv Európskej únie, Ústava Slovenskej republiky. Špecifická práva úprava práva na ochranu osobných údajov je zmienená v rámci:

[3] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) – ďalej len „Všeobecné nariadenie o ochranu osobných údajov“ alebo „GDPR“ alebo „nariadenie“

(i) medzinárodného práva: v Dohovore Rady Európy č. 108 o ochrane jednotlivcov pri automatizovanom spracúvaní osobných údajov (Modernizovaný dohovor 108),
(ii) práva Európskej únie: v rámci Všeobecného nariadenia o ochrane osobných údajov, v Smernici o súkromí a elektronických komunikáciách (Smernica ePrivacy) a v Smernici o spracúvaní osobných údajov inštitúciami EÚ,
(iii) slovenského právneho poriadku: v zákone č. 18/2018 Z.z. o ochrane osobných údajov a v zákone č. 351/2011 Z.z. o elektronických komunikáciách. [4]

Posúdenie vplyvu – definícia

Posúdenie vplyvu na ochranu osobných údajov je komplex činností, ktoré sú súhrnom právnej analýzy, odôvodnení potreby spracúvania osobných údajov prostredníctvom spracovateľskej operácie vrátane analýzy dopadov na práva a slobody fyzických osôb založenej na rizikách a aplikácii bezpečnostných opatrení, ktoré môžu prispieť k zmierneniu rizika. [5]

Posúdenie vplyvu na ochranu osobných údajov, tiež známe ako *„Data protection impact assessment“* (skratka *„DPIA“*) predstavuje nový právny inštitút, ktorý nahrádza notifikačnú povinnosť (viď Recitál 89 Všeobecného nariadenia o ochrane osobných údajov[6]). Na území Slovenskej republiky sa však nejedná o úplnú novinku, v súlade s predchádzajúcou právnou úpravou bolo posúdenie vplyvu realizované Úradom na ochranu osobných údajov pri

[4] MESARČÍK, M.: Ochrana osobných údajov. 1. vydanie. Bratislava: C. H. Beck, s. r. o.,2020, str. 9 – str. 12
[5] VALENTOVÁ, T. – BIRNSTEIN, M. – GOLAIS, J.: GDPR / Všeobecné nariadenie o ochrane osobných údajov. Zákon o ochrane osobných údajov. Praktický komentár. 1. vydanie. Bratislava: Wolters Kluwer SR s. r. o., 2018. 224 s. ISBN 978-80-8168-852-2
[6] Recitál 89 Všeobecného nariadenia o ochrane osobných údajov: *„V smernici 95/46/ES bola stanovená všeobecná povinnosť oznamovať spracúvanie osobných údajov dozorným orgánom. Uvedená povinnosť spôsobuje administratívnu a finančnú záťaž, a pritom neprispela vždy k zlepšeniu ochrany osobných údajov. Takéto nerozlišujúce všeobecné oznamovacie povinnosti by sa preto mali zrušiť a mali by sa nahradiť efektívnymi postupmi a mechanizmami zameranými namiesto toho na tie typy spracovateľských operácií, ktoré pravdepodobne povedú k vysokému riziku pre práva a slobody fyzických osôb z dôvodu ich povahy, rozsahu, kontextu a účelu. Takýmito typmi spracovateľských operácií môžu byť najmä tie, ktoré používajú nové technológie, alebo tie, ktoré sú nového druhu a v súvislosti s ktorými prevádzkovateľ ešte nevykonal posúdenie vplyvu na ochranu údajov, alebo ak sa stanú nevyhnutnými vzhľadom na čas, ktorý uplynul od prvotného spracúvania.“*

posudzovaní miery nebezpečenstva porušenia práv a slobôd pri osobitnej registrácii v zmysle z. č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. [7]

V zmysle Článku 35 Všeobecného nariadenia o ochrane osobných údajov, ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov. Posúdenie vplyvu môže pokrývať jednu spracovateľskú operáciu alebo skupinu podobných operácií s podobnými rizikami. Text Všeobecného nariadenia o ochrane osobných údajov je abstraktný a obsahuje neurčité právne pojmy, ktoré upresňuje Európsky výbor pre ochranu osobných údajov (v angl. jazyku skratka EDPB). EDPB (nahrádza pracovnú skupinu zriadenú podľa článku 29 smernice 95/46/ES, skratka WP29) je nezávislý orgán EÚ s právnou subjektivitou, ktorý prispieva k zjednoteniu uplatňovania pravidiel ochrany údajov v rámci EÚ, poskytuje všeobecné usmernenia, poradenstvo a podporuje vzájomnú spoluprácu dozorných úradov.

Posúdenie vplyvu na ochranu osobných údajov je proces zahŕňajúci najmä:

(i) systematické analyzovanie, identifikovanie a minimalizovanie možného rizika s ohľadom na práva dotknutých osôb (t.j. vypracovanie analýzy rizík),
(ii) odôvodnenie nevyhnutnosti daného druhu spracúvania osobných údajov s ohľadom na riziká v súvislosti s právami dotknutých osôb,
(iii) prijatie opatrení, záruk a mechanizmov na zmiernenie daného rizika[8].

Posúdenie vplyvu je dôležitá súčasť preukázania súladu v zmysle Všeobecného nariadenia o ochrane osobných údajov. Dôležitosť posúdenia vplyvu je možné odvodiť z Recitálu 84 Všeobecného nariadenia o ochrane osobných údajov.[9] Posúdenie vplyvu tvorí

[7] VALENTOVÁ, T. – BIRNSTEIN, M. – GOLAIS, J.: GDPR / Všeobecné nariadenie o ochrane osobných údajov. Zákon o ochrane osobných údajov. Praktický komentár. 1. vydanie. Bratislava: Wolters Kluwer SR s. r. o., 2018. 224 s. ISBN 978-80-8168-852-2

[8] pozri napr. HUDECOVÁ, I. a kol.: Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. 2. zväzok, 2. aktualizované vydanie. Žilina: EUROKÓDEX, s.r.o., 2020, str. 79

[9] Recitál 84 Všeobecného nariadenia o ochrane osobných údajov: „*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. 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. Ak sa na základe posúdenia vplyvu na ochranu údajov ukáže, že spracovateľské operácie zahŕňajú vysoké riziko, ktoré prevádzkovateľ nemôže zmierniť primeranými opatreniami, pokiaľ ide o najnovšie technológie a náklady na vykonanie opatrení, mala by sa pred spracúvaním uskutočniť konzultácia s dozorným orgánom.*“

základnú súčasť preukazovania súladu s nariadením a preukazuje zavedenie princípu zodpovednosti prevádzkovateľa. Jedná sa o legislatívnu povinnosť pre určité špecifické typy spracúvania osobných údajov, pri ktorých je pravdepodobné, že budú mať za následok vysoké riziko pre práva a slobody jednotlivcov. Nevykonanie posúdenia vplyvu v prípade, že spracúvanie tejto povinnosti podlieha, je sankcionované až do výšky 10 mil. EUR / 2% celosvetového obratu.

Výsledkom posúdenia vplyvu je prijatie primeraných technických a organizačných opatrení na minimalizáciu rizika pre práva dotknutých osôb. Uvedený výstup je v súlade so znením Článku 25 Všeobecného nariadenia o ochrane osobných údajov, na základe ktorého je prevádzkovateľ povinný, v čase určenia prostriedkov spracúvania, aj v čase samotného spracúvania, prijať primerané technické a organizačné opatrenia a začleniť do spracúvania nevyhnutné záruky s cieľom splniť požiadavky nariadenia a chrániť práva dotknutých osôb. Prevádzkovateľ je povinný vykonať primerané technické a organizačné opatrenia, aby zabezpečil, že štandardne sa spracúvajú len osobné údaje, ktoré sú nevyhnutné pre každý konkrétny účel spracúvania s ohľadom na množstvo získaných osobných údajov, rozsah ich spracúvania, dobu ich uchovávania a ich dostupnosť.

Posúdenie vplyvu by malo byť vypracované s ohľadom na existujúce zásady Všeobecného nariadenia na ochranu osobných údajov, t.j. *„privacy by design“* a *„privacy by default“*[10]:

(i) zásada *„privacy by design“* - akékoľvek operácie zahŕňajúce spracúvanie osobných údajov, ktoré prevádzkovateľ podnikne, musia zohľadňovať dodržiavanie podmienok ochrany osobných údajov a súkromia, prevádzkovateľ by mal daný postup dodržiavať okrem iného pri zavádzaní nových interných projektov, nových procesov, pri vývoji produktov, vývoji

[10] Recitál 78 Všeobecného nariadenia o ochrane osobných údajov: „*Ochrana práv a slobôd fyzických osôb pri spracúvaní osobných údajov si vyžaduje, aby sa prijali primerané technické a organizačné opatrenia s cieľom zabezpečiť splnenie požiadaviek tohto nariadenia. Na to, aby mohol prevádzkovateľ preukázať súlad s týmto nariadením, by mal prijať interné pravidlá a prijať opatrenia, ktoré budú predovšetkým spĺňať zásady špecificky navrhnutej ochrany údajov a štandardnej ochrany údajov. Takéto opatrenia by mohli okrem iného pozostávať z minimalizácie spracúvania osobných údajov, čo najskoršej pseudonymizácie osobných údajov, transparentnosti v súvislosti s funkciami a spracúvaním osobných údajov, umožnenia dotknutým osobám monitorovať spracúvanie údajov, umožnenia prevádzkovateľovi vypracovať a zlepšiť bezpečnostné prvky. Pri vypracovaní, navrhovaní, výbere a používaní aplikácií, služieb a produktov, ktoré sú založené na spracúvaní osobných údajov alebo spracúvajú osobné údaje, aby splnili svoju úlohu, by sa výrobcovia týchto produktov, služieb a aplikácií mali vyzvať, aby pri vypracovaní a navrhovaní takýchto produktov, služieb a aplikácií zohľadnili právo na ochranu údajov, pričom náležite zohľadnia najnovšie poznatky, aby sa zabezpečilo, že prevádzkovatelia a sprostredkovatelia môžu plniť svoje povinnosti týkajúce sa ochrany údajov. Zásady špecificky navrhnutej ochrany údajov a štandardnej ochrany údajov by sa mali zohľadniť aj v súvislosti s verejným obstarávaním.*“

softvéru, vývoji IT systémov a pod.), ochrana súkromia má byť súčasťou systémov a operácií počas celého životného cyklu systému alebo procesu,
(ii) zásada *„privacy by default*“ - systémy by mali obsahovať najprísnejšie nastavenia ochrany osobných údajov bez manuálneho zadávania koncovým používateľom, osobné údaje poskytnuté používateľom s cieľom umožniť optimálne použitie produktu by sa mali uchovávať iba po dobu nevyhnutnú na poskytnutie produktu alebo služby, nemalo by dôjsť k spracovaniu viac informácií, ako je potrebné na poskytnutie služby.

Posúdenie vplyvu napomáha skorému identifikovaniu problémov a ich možnej náprave, a tak dochádza nielen k ochrane osobných údajov fyzických osôb, ale aj k ochrane podnikania. V neposlednom rade je potrebné poukázať na skutočnosť, že posúdenie vplyvu nie je jednorazová záležitosť, ale živý proces, ktorý pomáha priebežne spravovať a kontrolovať riziká spracovania a zavedené opatrenia.

Riziko – definícia

Riziko je scenár, ktorý opisuje udalosť a možné následky udalosti odhadovane v kategóriách závažnosť a pravdepodobnosť.[11] V zmysle Všeobecného nariadenia o ochrane osobných údajov je vykonanie posúdenia vplyvu podmienené pravdepodobnou existenciou vysokého rizika pre práva a slobody fyzických osôb. Definícia rizika, resp. vysokého rizika pre práva a slobody fyzických osôb, je nejednoznačná. Všeobecného nariadenia o ochrane osobných údajov chápe pojem „riziko“ ako funkciu určitej pravdepodobnosti a závažnosti rizika pre práva a slobody fyzických osôb ovplyvnená najmä povahou, rozsahom, kontextom a účelmi spracúvania[12]. V zmysle Recitálu 75[13] Všeobecného nariadenia o ochrane osobných

[11] viac: HUDECOVÁ, I. a kol.: Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. Veľký komentár. Bratislava: EUROKÓDEX, s.r.o., 2018, str. 341
[12] Recitál 76 Všeobecného nariadenia o ochrane osobných údajov: „*Pravdepodobnosť a závažnosť rizika pre práva a slobody dotknutých osôb by sa mala stanoviť v závislosti od povahy, rozsahu, kontextu a účelov spracúvania. Riziko by sa malo posudzovať na základe objektívneho posúdenia, ktorým sa určí, či spracovateľské operácie obsahujú riziko alebo vysoké riziko.*“
[13] Recitál 75 Všeobecného nariadenie o ochrane osobných údajov: *„Riziko pre práva a slobody fyzických osôb s rôznym stupňom pravdepodobnosti a závažnosti môžu vyplývať zo spracúvania osobných údajov, ktoré by mohlo viesť k ujme na zdraví, majetkovej alebo nemajetkovej ujme, a to najmä ak spracúvanie môže viesť k diskriminácii, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena, strate dôvernosti osobných údajov chránených profesijným tajomstvom, neoprávnenej reverznej pseudonymizácii alebo akémukoľvek inému závažnému hospodárskemu alebo sociálnemu znevýhodneniu; ak by dotknuté osoby mohli*

údajov riziko pre práva a slobody fyzických osôb s rôznym stupňom pravdepodobnosti a závažnosti môže vyplývať zo spracúvania osobných údajov, ktoré by mohlo viesť k potenciálnej škode (k ujme na zdraví, majetkovej alebo nemajetkovej ujme).

Vysoké riziko na práva a slobody fyzických osôb môže byť prítomné najmä ak spracovanie môže viesť k: diskriminácii, krádeži identity alebo podvodu, finančnej strate, poškodeniu dobrého mena, negatívnemu vplyvu na spoločnosť, strate dôvernosti osobných údajov chránených profesijným tajomstvom, neoprávnenej reverznej pseudonymizácii, akejkoľvek inej významnej hospodárskej alebo sociálnej nevýhode (znevýhodneniu).

Spracovateľské operácie vedúce k vysokému riziku[14]

Článok 35 ods. 1 Všeobecného nariadenia o ochrane osobných údajov možno považovať za tzv. Všeobecnú klauzulu[15], podľa ktorej využitie nových technológií s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb.

Príklad: Nová aplikácia zameraná na poskytovanie rád v oblasti životného štýlu, ktorá pomocou náramku sleduje výkony a životné funkcie používateľa, jeho polohu a pod. Následne údaje vyhodnocuje a dáva užívateľovi odporúčania.

Článok 35 ods. 3 Všeobecného nariadenia o ochrane osobných údajov definuje špecifické podmienky spracúvania podliehajúce posúdeniu vplyvu[16] ako:

a) systematické a rozsiahle[17] hodnotenie osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania a z ktorého

---

byť pozbavené svojich práv a slobôd alebo im bolo bránené v kontrole nad svojimi osobnými údajmi; 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; 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; ak sa spracúvajú osobné údaje zraniteľných fyzických osôb, najmä detí; alebo ak spracúvanie zahŕňa veľké množstvo osobných údajov a má dôsledky na veľký počet dotknutých osôb."

[14] VALENTOVÁ, T.: GDPR / Všeobecné nariadenie o ochrane osobných údajov. Zákon o ochrane osobných údajov. Praktický komentár. Bratislava: Wolters Kluwer, s. r. o., 2018, str. 224

[15] MESARČÍK, M.: Ochrana osobných údajov. 1. vydanie. Bratislava: C. H. Beck, s. r. o.,2020, str. 126

[16] NULÍČEK, M. a kol.: GDPR / Obecné nařízení o ochraně osobních údajů. Praktický komentář. 1. vydanie. Praha: Wolters Kluwer SR s. r. o., 2017, str. 316

[17] tamtiež, str. 317

vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu,

Príklad: Fyzická osoba požiada o úver, systém banky preskúma žiadateľa a rozhodne o neposkytnutí úver, bez ďalšieho overenia výsledku zamestnancom banky.

b) spracúvanie vo veľkom rozsahu osobitných kategórií údajov alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky,

Príklad: Centrum probácie a mediácie, ktoré spracúva osobné údaje svojich klientov, ktorý boli odsúdení, resp. voči nim prebieha trestné konanie.

c) systematické monitorovanie verejne prístupných miest vo veľkom rozsahu.

Príklad: Monitorovanie parkoviska námestia pred nákupnym centrom.

Negatívne vymedzenie spracovateľských operácií vedúcich k vysokému riziku je uvedené v Recitáli 91 Všeobecného nariadenia o ochrane osobných údajov, podľa ktorého spracúvanie osobných údajov by sa nemalo považovať za spracúvanie veľkého rozsahu, ak sa týka osobných údajov pacientov alebo klientov jednotlivým lekárom, iným zdravotníckym pracovníkom alebo právnikom. V takýchto prípadoch by posúdenie vplyvu na ochranu údajov nemalo byť povinné

Pracovná skupina pre ochranu údajov zriadená podľa článku 29 (WP 29, v súčasnosti nahradená EDPB) zverejnila usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia spracúvanie „pravdepodobne povedie k vysokému riziku“. Stanovisko EDPB (resp. pracovnej skupiny WP 29)[18] zadefinovalo kritériá, ktoré je potrebné vziať do úvahy pre posúdenie spracovateľských operácií a vznik povinnosti vypracovať posúdenie vplyvu:

a) hodnotenie alebo prideľovanie bodov vrátane profilovania a predpovedania *(napr. majetkových pomerov, správania, konania, hodnotenie zvykov, preferencií, záujmov)*,
b) automatizované rozhodovanie s právnym alebo podobne záväzným účinkom *(napr. systémy v bánk, úverových a lízingových spoločností)*,
c) systematické monitorovanie, vrátane monitorovania verejne prístupných priestorov *(napr. monitorovanie kamerou detský ihrísk, námestí, termo-kamera v nákupných centrách, nemocniciach)* ,

[18] viac na: https://dataprotection.gov.sk/uoou/sites/default/files/usmernenia_tykajuce_sa_posudenia_vplyvu_na_ochranu_udajov_a_stanovenie_toho_ci_spracuvanie_pravdepodobne_povedie_k_vysokemu_riziku.pdf .

d) spracovanie citlivých údaje alebo údajov veľmi osobnej povahy *(napr. rôzne aplikácie týkajúce sa zdravia, zápiskov osobnej povahy)*,
e) údaje spracúvané vo veľkom rozsahu *(vzhľadom na okolnosti, región, počet dotknutých osôb a pod.)*,
f) spájanie alebo kombinovanie súborov údajov – priraďovanie alebo zlučovanie dátových súborov *(napr. získavanie údajov z registrácie a ich spojenie s údajmi, ktoré získala stránka o používateľovi pri prezeraní, resp. spojenie s údajmi, ktoré získala stránka z predchádzajúceho prehliadania – jedná sa zároveň aj o profilovanie používateľa web stránky)*,
g) údaje týkajúce sa zraniteľných dotknutých osôb *(napr. údaje týkajúce sa zamestnancov, starších osôb, detí, postihnutých osôb, týraných žien)*,
h) inovačné využitie alebo uplatňovanie nových technologických alebo organizačných riešení *(napr. vývoj nových aplikácií, zariadení, zdokonaľovanie existujúcich zariadení - mobilných telefónov, hodiniek, go pro)*,
i) samotné spracúvanie bráni dotknutým osobám uplatniť svoje právo alebo využiť službu alebo zmluvu *(napr. odmietnutie reklamných cookies má za následok nesprístupnenie web stránky a jej obsahu)*.

Splnenie aspoň 2 kritérií má za následok aktiváciu všeobecnej klauzuly posúdenia vplyvu, t.j. vyvodzuje nevyhnutnosť vypracovať posúdenie vplyvu na ochranu osobných údajov pre dané spracovateľské operácie.

Recitál 91 Všeobecného nariadenia o ochrane osobných údajov pozitívne vymedzuje povinnosť posúdenia vplyvu na ochranu osobných údajov pri nasledujúcich spracovateľských operáciách:

a) spracovateľské operácie veľkého rozsahu, ktorých cieľom je spracúvať značný objem osobných údajov na regionálnej, vnútroštátnej alebo nadnárodnej úrovni, ktoré by mohli ovplyvniť veľký počet dotknutých osôb a ktoré pravdepodobne povedú k vysokému riziku, napríklad z hľadiska ich citlivosti, ak sa v súlade s dosiahnutým stavom technologických znalostí vo veľkom rozsahu využíva nová technológia,
b) spracovateľské operácie predstavujúce vysoké riziko pre práva a slobody dotknutých osôb, najmä ak je pre dotknuté osoby náročnejšie uplatniť svoje vlastné práva,

c) spracovateľské operácie realizované s cieľom prijať rozhodnutie, ktoré sa týka konkrétnych fyzických osôb a ktoré sa prijíma po akomkoľvek systematickom a rozsiahlom zhodnotení osobných aspektov súvisiacich s fyzickými osobami na základe profilovania týchto údajov alebo v nadväznosti na spracúvanie osobitných kategórií osobných údajov, biometrických údajov alebo údajov o uznaní viny za trestné činy a priestupky či súvisiacich bezpečnostných opatreniach,
d) keď prebieha monitorovanie verejne prístupných miest vo veľkom rozsahu, najmä ak sa používajú optické elektronické zariadenia,
e) kedy spracúvanie pravdepodobne povedie k vysokému riziku pre práva a slobody dotknutých osôb, najmä preto, lebo tieto operácie bránia dotknutým osobám uplatniť svoje právo alebo využiť službu alebo zmluvu, alebo preto, že sa systematicky vykonávajú vo veľkom rozsahu.

Zoznam spracovateľských operácií vo vybraných krajinách

Dozorný orgán štátu má povinnosť vypracovať zoznam spracovateľských operácií, ktoré budú podliehať povinnosti vypracovania posúdenia vplyvu. Následne bude tento zoznam predložený zo strany dozorného orgánu príslušného štátu na schválenie EDPB. V európskych krajinách nachádzame kvalitatívne a kvantitatívne rozdiely v zoznamoch spracovateľských operácií, ktoré podliehajú požiadavke vypracovania vplyvu. Väčšina dozorných orgánov členských štátov EÚ vydala tzv. *Blacklist* – zoznam spracovateľských operácií, ktoré vždy podliehajú posúdeniu vplyvu na ochranu osobných údajov. Tzv. *Whitelist* – zoznam spracovateľských operácií, ktoré nepodliehajú posúdeniu vplyvu na ochranu osobných údajov, zverejnil dozorný orgán Rakúska. Kombináciu *Blacklist-u* a *Whitelist-u*, za účelom zníženia administratívnej záťaže, zverejnili dozorné orgány Belgicka, Českej republiky.

Slovenská republika, resp. dozorný orgán - Úrad na ochranu osobných údajov Slovenskej republiky, vydal zoznam spracovateľských operácií, ktoré vždy podliehajú

posúdeniu vplyvu, tzv. *Blacklist*[19]. Posúdenie vplyvu je nevyhnutné vypracovať, ak sa jedná o:

a) spracúvanie biometrických údajov fyzických osôb na účely individuálnej identifikácie fyzickej osoby v spojení aspoň s jedným kritériom uvedeným v usmerneniach WP 248,
b) spracúvanie genetických údajov fyzických osôb v spojení aspoň s jedným kritériom uvedeným v usmerneniach WP 248,
c) spracúvanie lokalizačných údajov v spojení aspoň s jedným kritériom uvedeným v usmerneniach WP 248,
d) spracovateľské operácie vykonávané podľa čl. 14 Všeobecného nariadenia o ochrane údajov. Ak informácie, ktoré by mali byť poskytnuté dotknutej osobe sú predmetom výnimky podľa čl. 14 ods. 5 písm. b), c) a d) Všeobecného nariadenia o ochrane údajov, posúdenie vplyvu je vyžadované iba v spojení aspoň s jedným kritériom uvedeným v usmerneniach WP 248,
e) hodnotenie alebo prideľovanie bodov, ak účelom spracovateľskej operácie je posúdenie určitých charakteristík dotknutej osoby, pričom jeho výsledok má vplyv na kvalitu služby alebo možnosť jej poskytnutia dotknutej osobe,
f) posúdenie dôveryhodnosti, pričom účelom spracovateľskej operácie je posúdenie dôveryhodnosti dotknutej osoby prostredníctvom systematického hodnotenia osobných údajov alebo hodnotenia osobných údajov vo veľkom rozsahu,
g) posúdenie platobnej schopnosti, pričom účelom spracovateľskej operácie je posúdenie platobnej schopnosti dotknutej osoby prostredníctvom systematického hodnotenia osobných údajov alebo hodnotenia osobných údajov vo veľkom rozsahu,
h) profilovanie, pričom účelom spracovateľskej operácie je profilovanie prostredníctvom systematického hodnotenia osobných údajov, obzvlášť keď je založené na hodnotení charakteristík pracovnej výkonnosti, finančného stavu, zdravotného stavu, osobných preferencií alebo záujmov, spoľahlivosti alebo správania sa, pobytu alebo pohybu dotknutej osoby,
i) monitoring práce zamestnanca na základe vážnych dôvodov vyplývajúcich z osobitnej povahy činnosti zamestnávateľa (ďalej len „spracúvanie osobných údajov zamestnancov monitorovaním“). Vzhľadom na osobitnú povahu spracúvanie osobných údajov zamestnancov monitorovaním, ktoré spĺňa kritérium spracúvania údajov o zraniteľných

[19] viac na: https://iapp.org/resources/article/eu-member-state-dpia-whitelists-and-blacklists/

dotknutých osobách a kritérium systematického monitorovania, ako dvoch kritérií uvedených v usmernení WP 248, si vyžaduje vykonanie posúdenia vplyvu na ochranu osobných údajov,

j) spracúvanie osobných údajov na účely vedeckého alebo historického výskumu bez súhlasu dotknutej osoby v spojení aspoň s jedným kritériom uvedeným v usmerneniach WP 248,
k) spracovateľské operácie využívajúce nové alebo inovatívne technológie v spojení aspoň s jedným kritériom uvedeným v usmerneniach WP 248,
l) systematické kamerové monitorovanie verejných priestorov (v jednotlivých mestách, obciach a dopravcami mestskej a prímestskej verejnej dopravy),
m) sledovanie osôb súkromnými detektívnymi, resp. bezpečnostnými službami.

Poľská republika vydala (tak ako Slovenská republika) zoznam spracovateľských operácií, ktoré vždy podliehajú posúdeniu vplyvu a sú postavené na kritériách WP29[20]. Na rozdiel od Slovenskej republiky, ale pridala k vymedzeniu zoznamu spracovateľských operácií aj konkrétne príklady, ktorých sa vypracovanie posúdenia vplyvu týka. Posúdenie vplyvu je nevyhnutné vypracovať v nasledovných prípadoch, o.i.:

a) profilovanie sociálnej siete, spam – sociálne médiá, marketing, *headhunting*,
b) profilovanie nezamestnaných z hľadisku prístup k rôznym formám pomoci bez súhlasu – úrad práce,
c) hodnotenie bonity fyzických osôb pomocou algoritmov a umelej inteligencie,
d) posúdenie životného štýlu – ponuka zliav a akcií,
e) monitorovanie premávky – správanie na cestách a identifikácia vozidiel – cestné úseky s výberom mýta,
f) monitorovanie pracovného času a používaných nástrojov (e-mail, internet) – spoločnosti a ich pracoviská,
g) zber dát aplikáciami, ktoré môžu byť aj integrované do oblečenia a príslušenstva – inteligentné hodinky, prilba s *GoPro*, mobily a pod.,
h) mobilný monitorovací systém zriadený z dôvodu verejného záujmu – polícia, hasiči, mestská polícia, pohraničná stráž a pod.,

[20] viac na: https://iapp.org/resources/article/eu-member-state-dpia-whitelists-and-blacklists/

i) IT systém ponúkajúci fyzickým osobám spracovanie informácií na osobné účely – *cloud*, e-mail, kalendár, čítačky kníh – spoločnosti ponúkajúce dané služby,
j) centrálna správa osobných údajov - centrálny vzdelávací informačný systém, vysokoškolský systém, systém poistenia motorových vozidiel, systémy rôznych odborných kvalifikácií.

Maďarsko, resp. maďarský úrad na ochranu osobných údajov, vydal taktiež *Blacklist*, ktorý je hybridom slovenského a poľského prístupu[21]. Posúdenie vplyvu je v zmysle maďarského *Blacklistu* nutné vypracovať, ak sa jedná napr. o: spracovanie biometrických údajov, genetických údajov; bodovanie, rating, hodnotenie solventnosti; ďalšie použitie údajov zhromaždených od tretích osôb; používanie osobných údajov žiakov a študentov na hodnotenie; profilovanie; činnosť zameraná proti podvodom; inteligentné merače; automatizované rozhodovanie, ktoré má právne účinky alebo podobne významné účinky; systematické monitorovanie, údaje o polohe, monitorovanie práce zamestnancov.

Česká republika na rozdiel od ostatných krajín V4, zaujala odlišný prístup. Vydala nielen *Blacklist* ale aj *Whitelist*[22]. V zmysle *Whitelistu* zverejnila zoznam spracovateľských operácií, ktoré nepodliehajú vypracovaniu posúdenia vplyvu. Posúdenie vplyvu nie je nevyhnutné vypracovať, ak sa jedná o:

a) spracovávanie osobných údajov českých zamestnancov v Českej republike za účelom plnenia zákonných povinností (účtovníctvo, mzdy a personalistika),
b) spracovávanie osobných údajov českých zamestnancov v Českej republike, ak neobsahuje biometrické údaje, hodnotenie zamestnancov a ich systematické monitorovanie okrem systému *whistleblowingu*,
c) spracovávanie osobných údajov zákazníkov v Českej republike v rámci obchodnej činnosti (vrátane posielania *newslettra* a organizovania súťaží), vykonávaných v českom jazyku, neobsahujúce osobitnú kategóriu osobných údajov, hodnotenie, bodovanie alebo systematické monitorovanie,
d) spracovanie osobných údajov návštevníka webu založené na jeho výbere z ponuky výrobkov a služieb na danom webe, ak sa nespracováva osobitná kategória osobných údajov a údaje vysoko osobnej povahy a nedochádza k zameraniu na ohrozené skupiny,

[21] viac na: https://iapp.org/resources/article/eu-member-state-dpia-whitelists-and-blacklists/
[22] viac na: https://iapp.org/resources/article/eu-member-state-dpia-whitelists-and-blacklists/

e) spracovanie osobných údajov je zabezpečované osobou oprávnenou na poskytovanie zdravotných služieb, ktorá nie je v zamestnaneckom pomere; advokátmi a notármi; osobami poskytujúcimi sociálne služby; v daných prípadoch sa jedná len o spracovanie nevyhnutných údajov a zároveň nemôže ísť o prenos osobných údajov do 3. krajiny a nejedná sa o prepojenie dvoch a viacerých subjektov,
f) ak spracovanie osobných údajov stanovuje zákon.

Blacklist vydaný českým úradom na ochranu osobných údajov obsahuje zoznam, ktorý určuje kritériá (charakteristiky) spracovania osobných údajov, pomocou ktorých by mal prevádzkovať popísať operácie spracúvania osobných údajov a následne s ich pomocou stanoviť, či sa jedná o spracovanie osobných údajov s vysokou mierou rizika pre práva a slobody fyzických osôb. Posudzované kritériá sú nasledovné: spracovanie v oblasti monitorovania dotknutých osôb; spracovanie kritických údajov, údajov umožňujúcich priamu identifikáciu a/alebo údajov vysoko osobnej povahy dotknutých osôb; spracovanie osobných údajov, ktoré môžu vystaviť dotknuté osoby ohrozeniu z okolitého prostredia; spracovanie osobných údajov veľkého rozsahu; spracovanie zahŕňajúce snímanie verejne prístupných priestorov; spracovanie osobných údajov s obmedzeným ovplyvnením dotknutých osôb; spracovanie osobných údajov verejne prístupných; spracovanie osobných údajov v technologicky zložitých alebo pokročilých infraštruktúrach alebo platformách; spracovanie osobných údajov s väzbou na iného prevádzkovateľa alebo sprostredkovateľa; spracovanie osobných údajov s využitím nových technologických alebo organizačných riešení.

Ku každému kritériu (charakteristike) sú priradené kritické, významné alebo nízke hodnoty. Prevádzkovateľ je povinný vykonať posúdenie vplyvu na ochranu osobných údajov, ak spracovanie dosiahne aspoň dvakrát kritické hodnoty alebo ak dosiahne raz kritické hodnoty a zároveň najmenej päťkrát významné hodnoty.

Záver

Posúdenie vplyvu na ochranu údajov je komplexný inštitút neoddeliteľne spätý s ochranou osobných údajov, ktorá predstavuje súčasť jedného zo základných ľudských práv. Inštitútu posúdenia vplyvu je nevyhnutné venovať zvýšenú pozornosť. Najdôležitejšou

súčasťou posúdenia vplyvu sú konkrétne technické a organizačné opatrenia, ktoré sú prijaté za účelom zníženia rizika pre práva a slobody dotknutých osôb. Po prijatí technických a organizačných je nevyhnutné vykonávať aj následnú kontrolnú činnosť. Posúdenie vplyvu nie je jednorazová činnosť, je to kontinuálna činnosť.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

Monografie a učebnice:

HUDECOVÁ, I. a kol.: Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. Veľký komentár. Bratislava: EUROKÓDEX, s.r.o., 2018. 676 s. ISBN 978-80-8155-077-5.

HUDECOVÁ, I. a kol.: Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. 1. zväzok, 2. aktualizované vydanie. Žilina: EUROKÓDEX, s.r.o., 2020. 592 s. ISBN 978-80-8155-094-2.

HUDECOVÁ, I. a kol.: Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. 2. zväzok, 2. aktualizované vydanie. Žilina: EUROKÓDEX, s.r.o., 2020. 681 s. ISBN 978-80-8155-095-9.

MESARČÍK, M.: Ochrana osobných údajov. 1. vydanie. Bratislava: C. H. Beck, s. r. o., 2020. 320 s. ISBN 978-80-89603-92-3.

NULÍČEK, M. a kol.: GDPR / Obecné nařízení o ochraně osobních údajů. Praktický komentář. 1. vydanie. Praha: Wolters Kluwer SR s. r. o., 2017. 544 s. ISBN 978-80-7552-765-3.

ŠVEC, M. – VALENTOVÁ, T. – HORECKÝ, J.: GDPR v pracovnoprávnej praxi. Ako byť v súlade s nariadením o ochrane osobných údajov. 1. vydanie. Bratislava: Wolters Kluwer SR s. r. o., 2020. 264 s. ISBN 978-80-571-0237-3.

VALENTOVÁ, T. – BIRNSTEIN, M. – GOLAIS, J.: GDPR / Všeobecné nariadenie o ochrane osobných údajov. Zákon o ochrane osobných údajov. Praktický komentár. 1. vydanie. Bratislava: Wolters Kluwer SR s. r. o., 2018. 568 s. ISBN 978-80-8168-852-2.

Internetové zdroje:

Pracovná skupina pre ochranu údajov zriadená podľa článku 29: Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“. Dostupné na internete: https://dataprotection.gov.sk/uoou/sites/default/files/usmernenia_tykajuce_sa_posudenia_vplyvu_na_ochranu_udajov_a_stanovenie_toho_ci_spracuvanie_pravdepodobne_povedie_k_vysokemu_riziku.pdf .

IAPP: EU Member State DPIA Whitelists, Blacklists and Guidance. Dostupné na internete: https://iapp.org/resources/article/eu-member-state-dpia-whitelists-and-blacklists/ .

Grafická schéma procesu DPIA dostupná na: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/