

GDPR: Kedy ste povinní vypracovať DPIA – Posúdenie vplyvu na ochranu osobných údajov?

GDPR so sebou prináša viacero nových práv dotknutých osôb a postupov prevádzkovateľov viažucich sa k procesu spracúvania. Prostredníctvom nich musia preukázať administratívno-právnu dokumentáciu, ktorá slúži ako písomný právny základ pre „nakladanie“ s osobnými údajmi v rámci daného subjektu, ktorý ich spracúva. Základným dokumentom každého subjektu spracúvajúceho osobné údaje je Dátový plán, ktorý „mapuje“ jednotlivé dáta spracúvané vašou organizáciou, vrátane vymedzenia prostriedkov a účelov spracúvania, informačných systémov a následného „toku“ údajov voči sprostredkovateľom (napr. cloudové datacentrá) alebo voči tretím osobám. Doterajšia dokumentácia ochrany osobných údajov označovaná ako „Bezpečnostný projekt“ sa s účinnosťou od 25. 5. 2018 ruší.

Ochrana osobných údajov sa v poslednom čase stala jednou z horúcich tém v oblasti biznisu. Náš trh ovplyvnila hneď z dvoch biznisových hľadísk. Nielenže priniesla väčší rozvoj tzv. compliance služieb¹, ale aj zasiahla svojich adresátov v podobe subjektov spracúvajúcich osobné údaje. Pojem subjekt používame práve preto, lebo GDPR² regulácia nezasiahne len samotných podnikateľov, ale aj verejnoprávne subjekty, akými sú úrady, ministerstvá, príspevkové a rozpočtové organizácie štátu, obecné či mestské úrady a množstvo iných subjektov štátnej správy a samosprávy. Práve verejnoprávne subjekty sú tie, ktoré budú reguláciou GDPR zasiahnuté najviac, pretože spracúvajú najväčšie množstvá osobných údajov, rôznymi prostriedkami a na rôzne účely. Súkromnoprávne subjekty na tom však nebudú o nič lepšie.

„Identifikovateľnosť“ ako pojmový základ osobných údajov

Pri úvahe nad podstatou osobných údajov a polemike o potrebnosti ich zvýšenej ochrany je potrebné si uvedomiť, že osobné údaje nemajú len charakter „údaja v pravom slova zmysle“ v podobe jednoznačných identifikátorov uvedených napríklad na občianskom preukaze, ale ide aj o druhý rozmer osobných údajov, o ktorom sa najmä na Slovensku a v Česku hovorí oveľa menej. Druhým rozmerom slova „osobný údaj“ je to, čomu sa hovorí „identifikovateľnosť“³danej (dotknutej) osoby. Zjednodušene povedané, ide najmä o tie údaje, ktoré sú charakteristické pre konkrétnu osobu a ktoré navonok najmä voči laickému podnikateľovi nemusia pôsobiť ako identifikátor konkrétnej osoby, avšak z povahy týchto údajov a informácie, ktorú nesú, je možné danú osobu „vyňať“ z anonymity celého radu iných osôb, a tak ju následne jednoznačne identifikovať. V tomto prípade sa skloňuje aj slovo „privacy“, a teda ochrana súkromia danej osoby. Hovoríme teda o údajoch, ktoré nemusia jednoznačne „pomenovávať“ konkrétnu osobu menom, priezviskom, bydliskom a pod., ale v prípade týchto údajov postačuje hoci aj to, že môžu byť priradené konkrétnej osobe, a tak ju následne charakterizovať, prípadne profilovať. V prípade údajov viažucich sa k identifikovateľnosti hovoríme v podstate o vstupe do osobnostnej a súkromnej sféry danej osoby. Táto skutočnosť tak prispieva k zvýšenému významu samotnej ochrany osobných údajov a lepšiemu pochopeniu regulácie, ktorá je podnikateľmi často označovaná ako nadmerná a nezmyselná administratívna záťaž.

K vymedzeniu toho, aké dáta by mali požívať ochranu osobných údajov, je potrebné pristupovať veľmi opatrne a súčasne s odbornou precíznosťou (bližšie sa tejto téme venujeme v článku GDPR: Rozmer osobných údajov, o ktorom ste nevedeli). Na jednej strane podstatou compliance služieb musí nevyhnutne byť nastavenie vnútorných procesov u daného subjektu tak, aby vyhovovali požiadavkám regulácie a Úradu na ochranu osobných údajov. Súčasne však compliance služby nesmú neprimerane zasiahnuť do obchodných modelov daných podnikateľov a sťažovať im tak svoju vlastnú podnikateľskú činnosť (bližšie sa tejto téme venujeme v článku GDPR: Ako vyriešiť reguláciu vo vašej firme alebo úrade).

Tento krátky úvod do problematiky osobných údajov a ich vymedzenia nás dostáva k novým compliance povinnostiam pre povinné subjekty. GDPR so sebou prináša viacero nových práv dotknutých osôb a postupov prevádzkovateľov viažucich sa k procesu spracúvania, prostredníctvom ktorých musia preukázať, že ich spracúvanie je v súlade s právnymi predpismi, a to počas celého priebehu tejto činnosti, ako aj preukázanie administratívno-právnej dokumentácie, ktorá slúži ako písomný právny základ pre „nakladanie“ s osobnými údajmi v rámci daného subjektu, ktorý ich spracúva. Základným dokumentom každého subjektu spracúvajúceho osobné údaje je Dátový plán, ktorý „mapuje“ jednotlivé dáta spracúvané vašou organizáciou, vrátane vymedzenia prostriedkov a účelov spracúvania, informačných systémov a následného „toku“ údajov voči sprostredkovateľom (napr. cloudové datacentrá) alebo voči tretím osobám. Doterajšia dokumentácia ochrany osobných údajov označovaná ako „Bezpečnostný projekt“ sa s účinnosťou od 25. 5. 2018 ruší. Nebude teda postačovať pre naplnenie compliance požiadaviek stanovených reguláciou GDPR a našim novým [zákonom na ochranu osobných údajov](#), ktorý bude len špecifikovať niektoré otvorené ustanovenia inak unifikovanej celoeurópskej regulácie GDPR (ďalšie informácie o potrebnej dokumentácii vo vašej organizácii sa dočítate v pripravovanom článku GDPR: Aké dokumenty potrebujete?).

Tento článok je však venovaný špeciálnej dokumentácii označovanej ako DPIA, ktorá v našom právnom prostredí zažije svoju premiéru práve so vstupom GDPR do svojej účinnosti. Vysvetlíme teda, čím je táto dokumentácia špecifická a koho sa jej obligatórne vypracovanie týka.

Označenie DPIA pochádza z anglického výrazu „Data Protection Impact Assessment“⁴ V našom jazyku bolo zvolené označenie „Posúdenie vplyvu na ochranu osobných údajov“. Inak povedané, ide o dokument a s ním súvisiaci proces vyhodnocovania rizík spojených s osobitným spôsobom spracúvania osobných údajov. Vypracovanie DPIA stanovuje nariadenie GDPR vo svojom článku 35, kde súčasne demonštratívne definuje okolnosti, za ktorých je subjekt nevyhnutne povinný vypracovať DPIA. V záujme jasnejšieho vymedzenia toho, kedy budete povinní vypracovať DPIA, pristúpime k štruktúrovaniu článku 35 ods. 1 a jeho jednotlivých hypotéz (predpokladov), ktoré sú základom pre posúdenie toho, či sme alebo nie sme povinní vypracovať DPIA.

Základné hypotézy (predpoklady) sú preto tieto:

1. ide o prevádzkovateľa osobných údajov,

2. ide o osobitný typ spracúvania osobných údajov (napríklad nové technológie),
3. súčasne je potrebné hodnotiť povahu, rozsah, kontext a účely spracúvania,
4. pravdepodobnosť vysokého rizika pre práva a slobody fyzických osôb, ktoré môže vyplývať z horeuvedeného spracúvania.

Súčasne tzv. dispozíciou (následkom) právnej normy uvedenej v čl. 35 ods. 1 GDPR je nielen to, že vypracovanie DPIA je povinné, ale aj to, že je potrebné ho vykonať ešte pred samotným spracúvaním osobných údajov.

Prejdime teda k jednotlivým bodom:

a) Prevádzkovateľ5:

Povinnosť vypracovať DPIA má výhradne prevádzkovateľ, zjednodušene povedané, ten subjekt, ktorý inicioval spracúvanie osobných údajov na zabezpečenie svojich úloh, kompetencií, plnenie zmlúv alebo biznis modelu založeného napríklad na Big Data, štatistikách, profilovaní osôb a pod. Samotného sprostredkovateľa (napr. cloudové datacentrum, obchodné zastúpenie a pod.) sa vypracovanie DPIA bezprostredne netýka. Avšak GDPR v čl. 28 ods. 3 písm. f) ustanovuje povinnosť sprostredkovateľa „pomáhať prevádzkovateľovi“ pri plnení jeho povinností podľa čl. 32 až 36, t. j. pri plnení povinností vyplývajúcich najmä z bezpečnosti osobných údajov a vypracovania DPIA. Keďže sprostredkovateľ spracúva osobné údaje v mene prevádzkovateľa (delegovaný princíp), je prirodzene povinný zúčastňovať sa na plnení povinností prevádzkovateľa. Samozrejme, každý prevádzkovateľ by mal v prvom rade riešiť dodržiavanie právnych regulácií prostredníctvom zmluvnej úpravy a garancií daných sprostredkovateľom.

b) Osobitný typ spracúvania:

Nariadenie GDPR v súvislosti s DPIA uvádza len veľmi náhodne, že ide najmä o typy spracovateľských operácií, ktoré súvisia s novými technológiami. Konkrétne tento pojem je natoľko neurčitý, že bude otázkou aplikačnej praxe a tzv. best practices ustálených spôsobov, ako sa obsah tohto pojmu plnohodnotne rozvinie. Avšak pripomíname, že GDPR používa slovo „najmä“, a teda len demonštratívne naznačuje, že primárna pozornosť pri vypracovaní DPIA by mala byť sústredená na nové technológie. Recitál Nariadenia GDPR bod 89 hovorí, že: „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 nevykonával posúdenie vplyvu na ochranu údajov, alebo ak sa stanú nevyhnutnými vzhľadom na čas, ktorý uplynul od prvotného spracúvania.“ Výklad a posúdenie tohto ustanovenia v praxi vždy vyžaduje individuálny prístup a skúmanie všetkých atribútov spracúvania osobných údajov u konkrétného prevádzkovateľa, preto je ťažké paušalizovať výklad tohto ustanovenia, avšak všeobecne môžeme konštatovať, že ide o nové spracovateľské technológie, ktorých dosah na ochranu osobných údajov, súkromie a osobnostnú sféru jednotlivca nevieme plnohodnotne definovať. Inak povedané, používanie týchto technológií a s tým súvisiace riziká pre dotknuté osoby sa nemusia obmedzovať výhradne na spracovanie osobných údajov, na ktoré technológie reálne využívate, ale aj na reziduálne a neočakávané riziká, ktoré sa skrývajú v pozadí vášho pôvodného zámeru. Práve preto je potrebné hodnotiť nielen napríklad samotné spracúvanie,

kategórie osobných údajov, rozsah spracúvania, ale aj typ spracúvania. V záujme lepšej predstavy o tom, čo sa môže rozumieť spracovateľskou operáciou, uvádzame tieto príklady:

1) Vyhodnocovanie a scoring:

Tieto operácie zahŕňajú aj profilovanie a predikcie. V praxi je to najmä vyhodnocovanie osôb na hodnotenie plnenia pracovných úloh, ekonomickej a finančnej situácie, zdravia, osobných preferencií a záujmov, spoľahlivosti a správania alebo lokalizácie a pohybu.

2) Prostriedky automatizovaného rozhodovania:

Ide o rozhodovanie s možným právnym alebo iným podobne podstatným účinkom vo vzťahu k danej osobe. Tu je ale potrebné posudzovať aj mieru zásahu do osobnej sféry danej osoby. Pri menšej a pomerne nepodstatnej miere nevzniká ani riziko voči právam dotknutej osoby.

3) Systematické monitorovanie:

Je potrebné upozorniť, že slovom monitorovanie sa nechápe len vykonávanie kamerových záznamov, ale označuje sa ním spracovateľská operácia ako taká. Ide teda najmä o získavanie, kontrolu a vyhodnocovanie dát alebo dát extrahovaných z audiovizuálnych záznamov⁶.

4) Porovnávanie a kombinovanie datasetov:

Datasetom by sme zjednodušene mohli nazvať konkrétnu zložku databázy, ktorá obsahuje údaje, resp. informácie získané na základe konkrétneho účelu spracúvania (napríklad na účel uzavretia a plnenia zmluvy). Porovnávaním a kombinovaním jednotlivých údajov z viacerých datasetov je možné následne vytvoriť nové informácie, resp. dáta o dotknutej osobe, ktoré môžu mať povahu deduktívnych informácií. Ide o mozaikový prístup spájania jednotlivých zdanlivo nesúvisiacich alebo „sterilných“ osobných údajov, ktoré tak vytvoria komplexný obraz sledovaný prevádzkovateľom.

Samozrejme, existuje aj množstvo iných spracovateľských operácií a uvedený rozpis slúži ako ilustračná pomôcka.

c) Ďalším atribútom, ktorý je potrebné skúmať pri vypracúvaní DPIA, je povaha, rozsah, kontext a účely spracúvania osobných údajov.

Inak povedané, ide o štruktúrovanie spôsobu spracúvania osobných údajov a proporcionálne sledovanie jednotlivých jeho ukazovateľov. Uvedené ukazovatele sú však aj tzv. právne neurčitými pojmami, ktoré nie sú presne definované v GDPR alebo súvisiacich predpisoch. Musíme teda pristúpiť k individuálnemu výkladu týchto pojmov. Povahou by sme mohli v zásade nazvať aj spôsob spracúvania osobných údajov, ku ktorým tak patria aj prostriedky spracúvania. Rozsahom sa rozumie objem dát, a teda množstvo dotknutých osôb, ktoré sú objektom spracúvania. Ani tento pojem nie je však jednoznačne definovaný, čo spôsobuje, že sa povinný subjekt dostáva do stavu právnej neistoty. Určitú indíciu k definovaniu pojmu „rozsah spracúvania“ však ponúka recitál Nariadenia GDPR v bode 91. Skutočnosť, či ide o veľký rozsah spracúvania osobných údajov, by mala závisieť od:

- množstva dotknutých osôb a ich pomeru k relevantnej časti populácie,

- objemu údajov alebo rozsahu (rôznorodosti) ich jednotlivých typov,
- dĺžky trvania spracovávaní údajov a jednotlivých spracovateľských operácií,
- územného rozsahu spracovateľských operácií.

Ako je možné vidieť, rozsahom spracúvania sa nerozumie len množstvo a objem osobných údajov, ale aj časové a územné faktory.

Pokiaľ ide o prihliadanie na kontext spracúvania osobných údajov, tu musíme takisto dedukovať význam a obsah tohto pojmu. V zásade však môžeme konštatovať, že kontextom sa rozumie najmä vykonávanie spracovateľských operácií rovnakou alebo podobnou technológiou, vo vzťahu k rovnakému typu údajov a na rovnaké účely. Pôjde tak napríklad o použitie monitorovania v prípade jedného prevádzkovateľa osobných údajov (napr.: Železničná spoločnosť) vo všetkých jeho jednotlivých objektoch (vlakoch). V tomto prípade nebude potrebné osobitné DPIA pre každý jeden objekt, ale postačí univerzálne DPIA.⁷ Na uvedenom príklade je možné demonštrovať výklad pojmu „kontext“. Tento pojem tak môžeme voľne definovať ako: „potrebu prihliadať na spoločné alebo súvisiace znaky spracovateľských operácií vystupujúcich ako jednotný celok“. Je teda potrebné hodnotiť jednotlivé spoločné znaky spracovateľských operácií, ale vždy vo vzájomných spojeniach, v akých majú byť v praxi použité v podobe jednotného systému spracúvania osobných údajov.

Posledným atribútom je pojem účel spracovania osobných údajov, ktorý ako jediný z uvedených je definovaný v čl. 6 GDPR (spracúvanie na základe súhlasu, plnenia zmluvy, zákonnej povinnosti, životne dôležitého záujmu dotknutej osoby, vo verejnom záujme a na účely oprávnených záujmov prevádzkovateľa).

Pre posúdenie toho, či ste povinní vypracovať DPIA, teda primárne slúži horeuvedený celok hypotéz, ktoré musíte pri dopracovaní sa k uvedenej otázke zodpovedať. Ako je možné vidieť, ide o pomerne komplikovaný a relatívne nejasný proces, ktorý vyžaduje prísne expertný prístup a kvalifikované osoby, ktoré by mali otázku o potrebe vypracovania DPIA spoľahlivo zodpovedať.

Ak si teda prejdeme celým uvedeným procesom hodnotenia spracovateľských operácií a ich dosahu na dotknuté osoby, dostaneme sa k odpovedi na otázku, či danými spracovateľskými operáciami dochádza k tzv. vysokému riziku pre práva a slobody fyzických osôb.

d) Vysoké riziko:

Pojem vysoké riziko je možné odvodiť od povahy spracovateľských operácií. Samotné riziko by mohlo byť definované ako ohrozenie práv a slobôd fyzickej osoby najmä vo vzťahu k osobnostnej, súkromnej, ekonomickej a spoločenskej sfére danej osoby. Inak povedané, ide o prípad, kedy by únik alebo zneužitie osobných údajov mohol významne zasiahnuť život danej osoby alebo jej uplatnenie v spoločnosti. Istým objasnením toho, o aké konkrétne prípady v praxi ide, je práve ustanovenie čl. 35 ods. 3 GDPR, ktoré demonštratívny (príkladný) spôsobom uvádza najmä prípady:

1) systematického a rozsiahleho hodnotenia osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania a z ktorého vychádzajú

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

2) spracúvania vo veľkom rozsahu osobitných kategórií (biometrické, zdravotné údaje a pod.) údajov alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky, alebo

3) systematického monitorovania verejne prístupných miest vo veľkom rozsahu.

Tieto prípady súčasne predstavujú okolnosti, kedy je vypracovanie dokumentácie DPIA obligatórne. Samozrejme, ani tieto prípady nie sú obmedzené, lebo GDPR ustanovuje povinnosť dozorného orgánu vypracovať zoznam ďalších spracovateľských operácií, pre ktoré bude DPIA povinné. Inak povedané, potreba vypracovať DPIA má z hľadiska povinností kladených na prevádzkovateľa osobných údajov dva rozmery. Prvým je vyhodnocovanie toho, či je DPIA vôbec potrebné a druhým je jednoznačné konštatovanie o potrebe DPIA v prípadoch výslovne stanovených právnymi predpismi. Od povahy spracovateľských operácií tak bude závisieť to, či bude prevádzkovateľ povinný podstúpiť ich vyhodnocovanie z hľadiska možných rizík pre fyzické osoby alebo sa tomuto procesu vyhne, lebo na základe povahy jednotlivých operácií presne zapadne do jedného z príkladov, kedy je vypracovanie DPIA výslovne obligatórne. Dokument DPIA a s ním súvisiace hodnotenie rizík však nepredstavuje len pre niektorých prevádzkovateľov „povinnú jazdu“ na ceste k legálnemu spracúvaniu osobných údajov, ale je aj prostriedkom istej prestíže a jasného deklarovania dôveryhodnosti daného prevádzkovateľa v podobe tzv. demonstrating compliance. Dôsledné vypracovanie DPIA vám ako podnikateľovi spolupracujúcemu s inými obchodnými partnermi môže prispieť k zvýšeniu obchodného potenciálu a hodnoty vašej firmy.

Uvedené podmienky sú základnými orientačnými bodmi pri úvahe nad tým, či ste povinní vypracovať DPIA alebo nie. V každom prípade akékoľvek pochybnosti alebo neistoty nesmú byť z vašej strany podceňované. Ak by totiž Úrad na ochranu osobných údajov vyhodnotil, že DPIA ste boli povinní vypracovať a vy ste tak neurobili na základe „náзору“, že sa na vás DPIA nevzťahuje, malo by to rovnaký sankčný následok, ako keby ste svoje povinnosti bezprostredne porušili. Vždy je vhodnejšie poradiť sa s odborníkmi, ktorí budú vedieť spoľahlivo daný stav posúdiť. V tomto okamihu si dovoľíme nadviazať práve na text v úvode článku, kde sme hovorili o často komplikovanom posúdení toho, čo všetko môže byť osobným údajom. Pri samotnom hodnotení „pravdepodobnosti vysokého rizika pre práva a slobody dotknutých osôb“ je posúdenie zo strany podnikateľa o to viac komplikovanejšie. K hypotézam a dispozíciám prirodzene patrí aj sankcia za ich porušenie. A v tomto prípade nariadenie GDPR mimoriadne pritvrdzuje. V prípade absencie DPIA alebo jeho nesprávneho vypracovania hrozí prevádzkovateľovi pokuta až do 10 miliónov eur alebo do výšky 2 % celkového celosvetového obratu za predchádzajúci účtovný rok, v závislosti od toho, čo je vyššie.

Preto ak si nie ste dostatočne istí vašimi povinnosťami, je vhodnejšie uistiť sa a konzultovať stav vo vašej organizácii s odborníkmi, ktorí majú nielen vedomosť o právnom stave v danej oblasti, ale aj o technologických trendoch, vývoji judikatúry v oblasti ochrany osobných údajov, únikov dát, právnych konzekvencií a najlepšej aplikačnej praxe.

Poznámka redakcie: [§ 42 z. č. 18/2018 Z. z.](#)