UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ

2026

Právne aspekty ochrany osobných údajov

(metodika pre subjekty verejnej správy)

Projekt Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ (KCKB UPJŠ) financovaný Európskou úniou z prostriedkov Plánu obnovy a odolnosti Slovenskej republiky, kód projektu: 17R05-04-V01-00007.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

OBSAH

ÚVOD

Ochrana osobných údajov predstavuje jednu z kľúčových právnych a spoločenských výziev súčasnej digitálnej éry. Dynamický rozvoj informačných a komunikačných technológií, digitalizácia verejných aj súkromných služieb a expanzia dátovo orientovaných obchodných modelov zásadne menia spôsob, akým sú osobné údaje získavané, spracúvané a využívané. Osobné údaje sa pritom stávajú nielen predmetom právnej ochrany ako súčasť práva na súkromie a ochrany osobnosti jednotlivca, ale aj významným ekonomickým aktívom s rastúcou hodnotou v digitálnom hospodárstve. Tento dualizmus – ochrana základných práv jednotlivca na jednej strane a legitímne záujmy štátu a trhu na strane druhej – vytvára komplexné prostredie, v ktorom sa právna úprava ochrany osobných údajov musí neustále prispôsobovať technologickému a spoločenskému vývoju.

Právny rámec ochrany osobných údajov v európskom priestore je formovaný najmä Chartou základných práv Európskej únie, Dohovorom o ochrane ľudských práv a základných slobôd a sekundárnym právom Európskej únie, predovšetkým všeobecným nariadením o ochrane údajov (GDPR). Tieto právne nástroje reflektujú potrebu zabezpečiť vysokú úroveň ochrany práv dotknutých osôb, transparentnosť spracúvania a zodpovednosť subjektov, ktoré osobné údaje spracúvajú. Súčasne však čelia kritike v súvislosti s ich praktickou aplikovateľnosťou, administratívnou náročnosťou a schopnosťou reagovať na nové technologické fenomény, ako sú umelá inteligencia, veľké dátové súbory či platformové hospodárstvo.

Cieľom tohto dokumentu je poukázať na základné východiská a funkcie ochrany osobných údajov v súčasnom právnom poriadku, identifikovať hlavné aplikačné výzvy a kriticky zhodnotiť efektívnosť existujúceho regulačného rámca v kontexte rýchlo sa meniaceho digitálneho prostredia. Osobitná pozornosť bude venovaná vzťahu medzi ochranou osobných údajov ako súčasťou základných práv a legitímnymi ekonomickými a verejnými záujmami, ktoré spracúvanie údajov podmieňujú a formujú.

1 PREDSTAVENIE KC KB UPJŠ

Kompetenčné centrum kybernetickej bezpečnosti na Univerzite Pavla Jozefa Šafárika v Košiciach (KC KB UPJŠ) predstavuje kompetenčné centrum, v rámci ktorého sú realizované aktivity zamerané na vzdelávanie, výskum a expertnú činnosť v oblasti informačnej a kybernetickej bezpečnosti, ochrany dát, kyberkriminality a ochrany pred dezinformáciami. Súčasne KC KB UPJŠ realizuje medzinárodnú spoluprácu s akademickými partnermi zo zahraničia a poskytuje konzultácie pre možnosť prípravy a podania projektov v oblasti kybernetickej bezpečnosti.

Vytvorenie KC KB UPJŠ reflektuje viacero problémov, ktoré možno v súčasnosti identifikovať v oblasti informačnej a kybernetickej bezpečnosti (ďalej aj „KIB“):

- zvýšenie bezpečnostného povedomia relevantných subjektov zahŕňajúcich predovšetkým zamestnancov verejnej správy a študentov vysokoškolského a stredoškolského štúdia,
- vzdelávanie a výchova nových odborníkov pôsobiacich v tejto oblasti,
- výskum kybernetických hrozieb a identifikácia adekvátnych reakcií na tieto hrozby,
- zvýšenie operatívnej bezpečnosti v rámci verejnej správy poskytovaním expertných činností zo strany CSIRT tímu.

V rámci KC KB UPJŠ sa pripravoval študijný plán magisterského stupňa študijného programu aplikovaná informatika, ktorého jedna vetva sa zameriava na kybernetickú bezpečnosť. K tomuto študijnému plánu budú vytvorené, resp. modifikované viaceré predmety. Súčasne sa ako výstup kompetenčného centrá vytvára ponuka **vzdelávania** pre rôzne cieľové skupiny zamestnancov verejnej správy.

V kontexte projektu sa súčasne posilňuje **spolupráca so strednými školami**, najmä vo forme činnosti **KyberTímov**, ich vzdelávania a následného zapojenia do šírenia bezpečnostného povedomia medzi širokou verejnosťou.

V rámci vzdelávacích aktivít sa sumarizujú nové poznatky a skúsenosti z oblasti KIB, ale aj príbuzných oblastí. Tie sú aktuálne doplnené o rôzne formy zážitkového vzdelávania.

V rámci **výskumnej** činnosti dochádza v už existujúcich výskumných oblastiach k publikovaniu viacerých vedeckých výstupov a k vytvoreniu nových možných výskumných spoluprác na posilnenie výskumného a vývojového potenciálu KC KB UPJŠ.

Nemenej dôležitým výstupom projektu je doplnenie výbavy a vzdelávanie univerzitného CSIRT tímu a možnosť poskytovania **expertných činností** pre akreditované CSIRT tímy v SR za účelom rýchlejšej a adekvátnejšej reakcie na kybernetické bezpečnostné incidenty.

2 PRÁVO INFORMAČNÝCH A KOMUNIKAČNÝCH TECHNOLÓGIÍ

Právo informačných a komunikačných technológií predstavuje **súhrn právnych noriem, ktoré upravujú vzájomne nezávislé a vysoko špecializované právne oblasti, ktoré sa neustále rozvíjajú v dôsledku rýchleho vývoja a aplikácie nových technológií v praxi.** Zo strany zákonodarcu je často takmer nemožné predvídať uvedený vývoj a tomu prispôsobiť príslušnú právnu úpravu. Prijatiu akejkoľvek právnej úpravy v tejto oblasti tiež spravidla predchádza zdĺhavý a formalistický legislatívny proces, dôsledkom ktorého je právna neistota spôsobená nejednoznačnosťou možnosti aplikovať existujúcu právnu úpravu, ktorá pri jej prijímaní nezohľadňovala osobitosti vzťahov spadajúcich do rámca práva informačných a komunikačných technológií.

Je zrejmé, že technologický vývoj značne predstihuje vývoj právny. V prípade, ak sa zákonodarca predsa len odhodlá na prijatie novej právnej úpravy v tejto oblasti, jeho cieľom by malo byť vytvorenie takého právneho rámca, ktorý je dostatočne flexibilný a ktorý umožňuje aplikáciu prijatej legislatívy nielen na technológie existujúce v čase jej prijatia, ale aj na tie, ktorých vznik často nemožno v čase prijatia predpokladať. V tomto prípade možno hovoriť o aplikácii tzv. **princípu technologickej neutrality**, ktorý v kontexte tejto publikácie zjednodušene obmedzíme na snahu zákonodarcu prijať takú právnu úpravu, ktorá je technologicky neutrálna, tzn. ktorá sa neobmedzuje na konkrétnu technológiu, ale ktorá je použiteľná na akékoľvek novovznikajúce technológie bez potreby revízie príslušnej legislatívy. Jedným zo spôsobov, akým zákonodarca môže dosiahnuť prijatie technologicky neutrálnych právnych noriem, je využívanie všeobecných formulácií ustanovení právnych predpisov s otvoreným významom. Príkladom uvedeného je formulácia definície osobných údajov uvedená v § 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov, ktorá za osobný údaj zjednodušene považuje akúkoľvek informáciu, ktorá umožňuje priamu alebo nepriamu identifikáciu fyzickej osoby prostredníctvom identifikátora, a to bez ohľadu na technológiu použitú pri spracovaní predmetnej informácie.

3 OCHRANA OSOBNÝCH ÚDAJOV

Princípy ochrany osobných údajov vychádzajú z medzinárodných prameňov práva. Prvým významným dokumentom, ktorý ochranu osobných údajov pomenoval a systematicky spracoval, je Dohovor Rady Európy z 28. januára 1981 o ochrane jednotlivcov so zreteľom na automatizované spracovanie osobných údajov.[1]

Rôznorodosť právnych úprav oblasti ochrany osobných údajov jednotlivých členských štátov, ktorá bola pre túto dobu príznačná, mohla mať za následok vytváranie prekážok pri prenose osobných údajov v rámci spoločného vnútorného trhu. Z tohto dôvodu bolo nevyhnutné upraviť pravidlá a zásady pohybu osobných údajov v rámci Európskeho spoločenstva aj sekundárnym právnym aktom, a to sa zrealizovalo smernicou Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe týchto údajov.

Zásady ochrany osobných údajov sú priamo zakotvené aj v VI. Hlave Schengenského dohovoru a naviac individuálne a konkrétne aspekty spracúvania osobných údajov v súvislosti s prevádzkou Schengenského informačného systému sú obsahom aj IV. Hlavy Schengenského dohovoru. Schengenský dohovor sa v čl. 126 odvoláva na minimálny štandard odkazujúc na dodržiavanie zásad Dohovoru Rady Európy o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov

[1] K tomu tiež pozri Mates, P. – Janečková, E. – Bartík, V.: Ochrana osobních údaju. Praha: Leges, 2012, s. 9.

z 28. januára 1981, čo sa týka automatizovaného spracúvania osobných údajov prenášaných podľa Schengenského dohovoru.[2]

Elektronické spracúvanie osobných údajov a elektronická komunikácia spôsobujú, že sa mení ponímanie osobných údajov. Kedysi bol osobný údaj chápaný ako pomerne zložitá množina údajov, ktorú tvoril dátum narodenia, rodné číslo, meno a priezvisko, bydlisko atď., avšak dnes sa ponímanie množiny osobných údajov značne rozšírilo.[3] Uvedené vychádza aj z judikatúry, keď Najvyšší správny súd ČR konštatoval, že „*v podmienkach vyspelej spoločnosti, kedy väčšina ľudí disponuje elektronickými a inými médiami, je plná identita daná tým, že môžeme určitú osobu kontaktovať bez toho, aby sme museli poznať miesto jej aktuálneho pobytu a výklad pojmu osobný údaj nie je možné redukovať napríklad na znalosť rodného čísla, ale postačí len to, že máme číslo mobilného telefónu.*“[4]

V máji 2018 nadobudlo účinnosť Všeobecné nariadenie Európskeho parlamentu a Rady č. 2016/679 z 27. apríla 2016 o *ochrane* fyzických osôb pri spracúvaní *osobných údajov* a o voľnom pohybe takýchto *údajov* (General Data Protection Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) (ďalej len „GDPR“), ktoré so sebou prinieslo nielen sprísnenie podmienok pre nakladanie s osobnými údajmi, ale aj nové práva a povinnosti osôb, ktoré s osobnými údajmi nakladajú, zavedenie nových inštitútov a pod. Na základe GDPR bol v slovenskom legislatívnom konaní prijatý zákon č. 18/2018 Z.z. o ochrane osobných údajov, ktorý zrušil dovtedy platný zákon o ochrane osobných údajov. Nadobudol účinnosť 25.05.2018 rovnako ako GDPR. Zákonom o ochrane osobných údajov sa zároveň transponuje Smernica Európskeho parlamentu a rady (EÚ) č. 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 a o zrušení rámcového rozhodnutia Rady 2008/977/SVV do právneho poriadku Slovenskej republiky (ďalej len „smernica“).

Zhrnutie právnej úpravy:

Problematika ochrany osobných údajov je v rámci EÚ upravená v primárnom práve:

- čl. 6 a čl. 39 Zmluvy o Európskej únii
- čl. 16 Zmluvy o fungovaní Európskej únii
- čl. 8 Charty základných práv Európskej únie

Upravuje ju aj sekundárne právo v nasledovných dokumentoch:

- Nariadenie Európskeho parlamentu a rady (EÚ) č. 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)
- Smernica 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 a o zrušení rámcového rozhodnutia Rady 2008/977/SVV
- Smernice Európskeho parlamentu a Rady (EÚ) 2019/770 z 20. mája 2019 o určitých aspektoch týkajúcich sa zmlúv o dodávaní digitálneho obsahu a digitálnych služieb

[2]Porovnaj Schengenský dohovor dostupný na https://www.minv.sk/swift_data/source/policia/schengen/Schengensky%20dohovor.pdf

[3] Mates, P. – Janečková, E. – Bartík, V.: Ochrana osobních údaju. Praha: Leges, 2012, s. 30.

[4] Rozsudok Najvyššieho správneho súdu ČR sp.zn. 9 As 34/2008 – 73 a sp.zn. 1 As 98/2008 - 148.

V rámci SR je problematika ochrany osobných údajov upravená:

- Ústava SR
- Zákon č. 18/2018 Z.z. o ochrane osobných údajov

3.1 DEFINÍCIA OSOBNÝCH ÚDAJOV

V zmysle čl. 4 bod 1 GDPR sú **osobnými údajmi akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby** (ďalej len „dotknutá osoba"), pričom identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.[5] Môže sa teda jednať o údaje ako sú titul, meno, priezvisko, dátum narodenia, bydlisko, fotka, e-mailová adresa, kontaktné informácie, číslo bankového účtu, zdravotné informácie, ale aj počítačová IP adresa (okrem tzv. maskovanej IP adresy a IP adresy pridelenej k sieti využívanej viacerými používateľmi), súbory cookies, čo je dôležité pre určenie virtuálnej identity. Tieto údaje môžu v kombinácii s jedinečnými identifikátormi taktiež viesť k identifikácii fyzickej osoby. Osobnými údajmi môžu byť aj lokalizačné údaje získané napríklad prostredníctvom lokalizačných funkcií mobilných telefónov, či štítky na rádiofrekvenčnú identifikáciu. Ide o tzv. demonštratívny výpočet charakteristík určujúcich fyzickú osobu. Uvedená definícia osobných údajov nevyžaduje, aby išlo o konkrétnu identitu fyzickej osoby, ale postačuje, aby za splnenia daných podmienok bola osoba identifikovateľná. Miera, do akej sú určité identifikátory dostačujúce pre dosiahnutie identifikácie konkrétnej fyzickej osoby, závisí od komplexného posúdenia dostupných údajov v ich vzájomnej súvislosti a konkrétnej situácie.

Fyzickú osobu považujeme za určenú, keď na základe dostupných údajov je jednoznačne identifikovaná a odlíšená od ostatných osôb v danom informačnom systéme, v ktorom sa osobné údaje spracúvajú. V tomto prípade si treba uvedomiť, že nie každá informácia o fyzickej osobe, ktorá vyzerá ako osobný údaj, ním napokon aj je. Osobnými údajmi nebudú napríklad údaje určujúce právnickú osobu alebo fyzickú osobu podnikateľa, anonymné údaje a pod.[6]

GDPR zavádza tri druhy nových osobných údajov. Prvým sú **genetické údaje**. Do tejto skupiny osobných údajov patria tie, ktoré sa týkajú zdedených alebo nadobudnutých znakov osoby. Uvedené údaje sa týkajú najmä biologickej vzorky danej osoby.

GDPR ďalej zavádza kategóriu **biometrických údajov**. Ide o informácie týkajúce sa fyzických, fyziologických a behaviorálnych znakov osoby, ako sú napríklad vyobrazenia tváre alebo daktyloskopické údaje.

---

[5] Uvedeným sa tiež zaoberá KASL, F.: Internet věcí a ochrana dát v europském kontextu. In.: Revue pro právo a technologie [Online]. 2016, č. 13, s. 120 dostupné na https://journals.muni.cz/revue/article/view/5422/pdf

[6] K tomu pozri aj Metodické usmernenie č. 1/2013 k pojmu osobné údaje dostupné na https://dataprotection.gov.sk/uoou/sites/default/files/metodicke_usmernenie_c._1_2013_k_pojmu_osobne_udaje.pdf

Treťou skupinou osobných údajov sú tie, ktoré sa týkajú fyzického alebo duševného zdravia.[7] Na základe toho GDPR zaraďuje určité osobné údaje do **osobitných kategórií**. Ide napríklad o údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské presvedčenie, genetické a biometrické údaje či údaje týkajúce sa zdravia.

Je potrebné rozlišovať aj formu osobných údajov, ktorá môže byť rôzna. Môže ísť o grafickú, fotografickú, papierovú, či elektronickú podobu.

3.2 SPRACÚVANIE OSOBNÝCH ÚDAJOV

V zmysle GDPR *je spracúvaním osobných údajov potrebné rozumieť každú spracovateľskú operáciu alebo niekoľko na seba nadväzujúcich operácií (nadväznosť v čase nie je podstatná), ktoré prevádzkovateľ alebo sprostredkovateľ vykonáva na splnenie určitého vymedzeného účelu, systematicky, a to bez ohľadu na spôsob a využité prostriedky (alebo ich kombináciu) spracúvania*. Spracúvanie môže byť vykonávané rôznymi spôsobmi, formou ľudskej činnosti, automatizovane, ide teda o charakteristiku toho, ako sú jednotlivé spracovateľské operácie u prevádzkovateľa alebo sprostredkovateľa vykonávané, technicky nastavené.

3.3 ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV

Zásady spracúvania osobných údajov sú uvedené v zákone č. 18/2018 o ochrane osobných údajov v ustanoveniach § 6 až 12. Ide o tieto zásady:

a) zásada zákonnosti
b) zásada obmedzenia účelu
c) zásada minimalizácie osobných údajov
d) zásada správnosti
e) zásada minimalizácie uchovávania
f) zásada integrity a dôvernosti
g) zásada zodpovednosti

Zásada zákonnosti

Zásada zákonnosti spracovania osobných údajov znamená, že **osobné údaje možno spracúvať len spôsobom ustanoveným zákonom a v jeho medziach tak, aby nedošlo k porušeniu základných práv a slobôd dotknutých osôb**, najmä k porušeniu ich práva na zachovanie ľudskej dôstojnosti alebo k iným neoprávneným zásahom do ich práva na ochranu súkromia.

Nie každé spracúvanie osobných údajov bude znamenať porušenie ich ochrany. GDPR, ako aj právna úprava SR po vzore GDPR obsahuje výpočet prípadov, kedy pôjde o zákonné spracúvanie osobných údajov a v prípade takéhoto spracúvania nedôjde k porušeniu ich ochrany. Vo vzťahu k právnym základom spracúvania stanovuje zákon o ochrane osobných údajov tieto **prípady zákonného spracúvania:**

a) spracúvanie na základe súhlasu dotknutej osoby,
b) spracúvanie bez súhlasu dotknutej osoby na účely nevyhnutné na plnenie zmluvy, ak zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzavretím zmluvy,
c) spracúvanie nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa,

[7] Pozri dôvodovú správu k zákonu č. 18/2018 Z.z. o ochrane osobných údajov dostupnú na http://www.epi.sk/dovodova-sprava/dovodova-sprava-k-zakonu-c-18-2018-z-z.htm

d) spracúvanie nevyhnutné, na ochranu životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby,
e) spracúvanie nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi,
f) spracúvanie nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobu dieťa, pričom tento právny základ sa nevzťahuje na spracúvanie vykonávané orgánmi verejnej moci pri výkone ich úloh,
g) spracúvanie nevyhnutné na účely akademické, umelecké, literárne alebo na účely informovania v masovokomunikačných prostriedkoch,
h) prevádzkovateľ, ktorý je zamestnávateľom dotknutej osoby, je oprávnený sprístupniť, poskytovať alebo zverejniť jej osobné údaje v rozsahu titul, meno, priezvisko, pracovné, služobné alebo funkčné zaradenie, odborný útvar, miesto výkonu práce, telefónne číslo, faxové číslo alebo elektronická pošta na pracovisko a identifikačné údaje zamestnávateľa, ak je to potrebné v súvislosti s plnením pracovných, služobných alebo funkčných povinností dotknutej osoby. Sprístupnenie, poskytovanie alebo zverejnenie osobných údajov nemôže narušiť vážnosť, dôstojnosť a bezpečnosť dotknutej osoby,
i) prevádzkovateľ môže spracúvať genetické údaje, biometrické údaje a údaje týkajúce sa zdravia aj na právnom základe uvedenom v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná,
j) právne základy uvedené v súvislosti so spracúvaním osobitnej kategórie osobných údajov (rasový a etnický pôvod, politické názory, náboženské a filozofické presvedčenie alebo členstvo v odborových organizáciách, genetické údaje, biometrické údaje na individuálnu identifikáciu fyzickej osoby, údaje týkajúce sa zdravia, údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby).

Zásada obmedzenia účelu

Spracúvané osobné údaje majú byť primerané, relevantné a obmedzené na zoznam alebo rozsah osobných údajov nevyhnutný vzhľadom na účel, na ktorý sa spracúvajú. Účel je základným obmedzujúcim faktorom najmä vo vzťahu k zoznamu alebo rozsahu spracúvaných osobných údajov a vo vzťahu k dobe spracúvania, ako aj uchovávania spracúvaných osobných údajov. Účel má byť vymedzený dostatočne jasne a určito, aby z neho bolo jasné, aké spracovateľské operácie na základe neho budú a nebudú prebiehať, alebo aké spracovateľské operácie dotknutá osoba môže očakávať, že s jej osobnými údajmi na základe jeho vymedzenia môžu prebiehať. Spracúvať osobné údaje na iný účel, než na ktorý boli získané je zakázané, ibaže by tento iný účel úzko súvisel s pôvodným účelom spracúvania, bol s ním zlučiteľný.

*Z***ásada minimalizácie osobných údajov**

Spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracovávajú. Zásada minimalizácie údajov obmedzuje každého prevádzkovateľa spracovávať údaje v určitom rozsahu. Tento rozsah je determinovaný primeranosťou, relevantnosťou a obmedzením na nevyhnutný rozsah, ktorý je daný účelom spracúvania.

Zásada správnosti

Uvedená zásada znamená, že **možno spracúvať len správne, úplné a podľa potreby aktualizované osobné údaje vo vzťahu k účelu spracúvania**; nesprávne a neúplné osobné údaje je prevádzkovateľ povinný blokovať a bez zbytočného odkladu opraviť alebo doplniť; nesprávne a

neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné, prevádzkovateľ zreteľne označí a bez zbytočného odkladu zlikviduje.

Zásada integrity a dôvernosti

Osobné údaje musia byť spracúvané spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných údajov, náhodnou stratou osobných údajov, výmazom osobných údajov alebo poškodením osobných údajov. Prijaté bezpečnostné opatrenia musia byť adekvátne spracúvaným osobným údajom, a to tak po technickej, personálnej, ako aj po organizačnej stránke.

Zásada zodpovednosti

Zásada zodpovednosti znamená, že prevádzkovateľ a sprostredkovateľ musia vedieť preukázať, že splnili zákonné požiadavky počas celej doby spracúvania osobných údajov.

K zásadám, ktoré sú zákonne vymedzené možno priradiť aj **zásadu transparentnosti** uvedenú v GDPR. V zmysle bodu 58 si zásada transparentnosti vyžaduje, aby všetky informácie určené verejnosti alebo dotknutej osobe boli stručné, ľahko prístupné a ľahko pochopiteľné, formulované jasne a jednoducho, a navyše ak je to vhodné, ľahko zrakovo vnímateľné.

3.4 SUBJEKTY V OBLASTI OCHRANY OSOBNÝCH ÚDAJOV

Vo všeobecnosti možno identifikovať pri ochrane osobných údajov dva subjekty. Na jednej strane vzťahu s určitými právami a povinnosťami je **prevádzkovateľ** a na strane druhej rovnako s určitými právami a povinnosťami je **dotknutá osoba**.

Vzťah medzi prevádzkovateľom a dotknutou osobou je primárnym vzťahom pri ochrane osobných údajov dotknutej osoby. Na tento primárny vzťah sa môžu upínať sekundárne vzťahy, a teda do primárneho vzťahu vstupujú vedľajšie subjekty, napr. **sprostredkovateľ**, **subdodávateľ**, **tretia strana**, **príjemca**. Ochrana osobných údajoch je vždy minimálne o dvoch subjektoch, o prevádzkovateľovi, ktorý osobné údaje spracúva a o dotknutej osobe, ktorá tieto osobné údaje vlastní.

Prevádzkovateľ

Pojem prevádzkovateľ používa zákon č. 18/2018 Z.z. o ochrane osobných údajov ako aj nariadenie GDPR.

Prevádzkovateľom je podľa § 4 ods. 2 písm. b) „*každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene*.“

Na to, aby sme mohli hovoriť o vzťahu medzi prevádzkovateľom a dotknutou osobou, musia byť splnené viaceré znaky, a to:

a) vymedzenie **účelu a prostriedkov** spracúvania osobných údajov,
b) objektom spracovávania sú **osobné údaje,** a nie akékoľvek údaje, teda ak prevádzkovateľ zhromažďuje údaje, ktoré nemajú charakter osobných údajov, nespadajú pod osobitný režim,
c) spracovávanie osobných údajov **vo vlastnom mene.**

Vyššie uvedené znaky musia byť naplnené **súčasne a kumulatívne**. To znamená, že ak chýba jeden z týchto znakov, nejedná sa o prevádzkovateľa podľa zákona o ochrane osobných údajov (môže ísť o jednorazové náhodné zbieranie údajov, pre súkromné účely, etc.).

Prevádzkovateľ nesie zodpovednosť za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov, pričom je povinný tento súlad preukázať na požiadanie Úradu na ochranu osobných údajov. GDPR zmenilo koncepčné nazeranie na povinnosti prevádzkovateľa a zakotvilo predpoklady pre **objektívnu zodpovednosť prevádzkovateľa**. Prevádzkovateľ ako profesionál nesie zodpovednosť za zákonný spôsob nakladania s osobnými údajmi.

Zákon prevádzkovateľovi ukladá široké **spektrum povinností**:

- povinnosť prijať vhodné technické (bezpečnostné) a organizačné opatrenia: špecificky navrhnutá alebo štandardná ochrana osobných údajov („*privacy by design*“ alebo „*privacy by default*“);
- povinnosť ustanoviť zodpovednú osobu;
- informačná povinnosť vo vzťahu k dotknutej osobe (povinnosť poskytnúť dotknutej osobe ustanovené informácie);
- povinnosť viesť záznamy o spracovateľských činnostiach, za ktoré je prevádzkovateľ zodpovedný;
- povinnosť spolupracovať s úradom pri výkone jeho činností a úloh;
- oznamovacia povinnosť týkajúca sa bezpečnostných incidentov (dozorujúcemu orgánu, t. j. úradu a dotknutej osobe).

Povinnosť prijať vhodné technické a organizačné opatrenia

Prijatie vhodných technických a organizačných opatrení je spojené s povinnosťou prevádzkovateľa zabezpečiť spracúvanie osobných údajov takým spôsobom, ktorý zaručuje **primeranú bezpečnosť osobných údajov**, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením.

Vhodné technické a organizačné opatrenia a ich aplikáciu Nariadenie GDPR i zákon o ochrane osobných údajov spája s kvalitatívnou a kvantitatívnou stránkou spracúvania údajov, to znamená, že závisia od povahy, rozsahu, kontextu a účelov spracúvania.

Technické opatrenia – činnosti smerujúce k minimalizovaniu rizík prostredníctvom nasadenia prostriedkov technologickej povahy.

Organizačné opatrenia – činnosti smerujúce k minimalizovaniu rizík pri zbere dát prostredníctvom zmien procesov a úpravou dokumentácie. V rámci organizačných opatrení treba osobitne uviesť aj personálne opatrenia, t. j. opatrenia vo vzťahu ku zamestnancom – vyškolenie zamestnancov, ktorí prichádzajú do kontaktu s údajmi.

V súvislosti s prijatím technických a organizačných opatrení Nariadenie GDPR zaviedlo novinku, a to tzv. privacy by design a privacy by default.

Ochrana údajov v súlade s **princípom by design** znamená špecificky navrhnutú ochranu osobných údajov a dotknutých osôb zohľadňujúcu celý životný cyklus zhromažďovaných údajov.

Špecificky navrhnutá ochrana osobných údajov spočíva v prijatí primeraných technických a organizačných opatrení, najmä vo forme pseudonymizácie, v účinnom zavedení primeraných záruk

ochrany osobných údajov a dodržiavaní základných zásad ochrany osobných údajov podľa § 6-12 zákona.

Prevádzkovateľ je povinný pri špecificky navrhnutej ochrane osobných údajov zohľadniť najnovšie poznatky ochrany osobných údajov, náklady na vykonanie opatrení na ochranu údajov, povahy, rozsah, kontext a účel spracúvania osobných údajov a riziká spracúvania osobných údajov s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie osobných údajov predstavuje pre práva dotknutej osoby.

Privacy by default znamená povinnosť štandardne a trvalo udržateľným spôsobom vykonávať ochranu údajov vo všetkých procesoch a spracovateľských operáciách v čase samotného spracúvania. To znamená, že prevádzkovateľ prijme primerané technické a organizačné opatrenia na zabezpečenie spracúvania osobných údajov len na konkrétny účel, so zámerom minimalizácie množstva získaných údajov a bez možnosti štandardného prístupu neobmedzeného počtu fyzických osôb k týmto údajom.

Informačná a oznamovacia povinnosť prevádzkovateľa

Informačnú povinnosť prevádzkovateľa možno vo vzťahu k dotknutej osobe chápať vo viacerých rovinách.

V prvom rade, ak je spracúvanie osobných údajov založené na súhlase dotknutej osoby, prevádzkovateľ je povinný si takýto súhlas zaobstarať. Súhlas dotknutej osoby je jedným z právnych základov pre zákonnosť spracúvania osobných údajov. Je však nevyhnutné, aby samotnému súhlasu predchádzalo splnenie si informačnej povinnosti zo strany prevádzkovateľa. Prevádzkovateľ je povinný informovať dotknutú osobu jasným, zrozumiteľným spôsobom a v ľahko dostupnej podobe a tak, aby súhlas bol odlíšiteľný od iných skutočností.

Prevádzkovateľ je povinný na požiadanie dotknutú osobu **informovať**:

1. pri získavaní osobných údajov je povinný oznámiť:
    - identifikačné údaje a kontaktné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený;
    - kontaktné údaje zodpovednej osoby, ak je určená;
    - účel spracúvania osobných údajov, na ktorý sú osobné údaje určené, ako aj právny základ spracúvania osobných údajov;
    - identifikáciu príjemcu alebo kategóriu príjemcu, ak existuje;
    - informáciu o prenose údajov do tretej krajiny alebo medzinárodnej organizácií;
    - dobe uchovávania osobných údajov, ak to nie je dostatočne možné, tak o kritériách jej určenia.
2. pri získavaní údajov je dotknutú osobu povinný **informovať o osobitných právach** súvisiacich s jeho osobnými údajmi:
    - práve požadovať prístup k osobným údajom;
    - práve na opravu osobných údajov;
    - práve na výmaz osobných údajov alebo o práve na obmedzenie spracúvania osobných údajov;
    - práve namietať spracúvanie osobných údajov;
    - práve na prenosnosť osobných údajov;
    - práve odvolať kedykoľvek súhlas;
    - práve podať návrh na začatie konania o konanie osobných údajov;
    - práve byť informovaný o existencii automatizovaného individuálneho rozhodovania vrátane profilovania – v týchto prípadoch je prevádzkovateľ povinný poskytnúť dotknutej osobe informáciu o použitom postupe, ako aj o význame automatizovaného

rozhodovania a predpokladaných dôsledkoch takéhoto spracúvania osobných údajov pre dotknutú osobu.

Prevádzkovateľ je povinný bez zbytočného odkladu **oznámiť** dotknutej osobe **porušenie ochrany osobných údajov**, ak takéto porušenie ochrany osobných údajov môže viesť k vysokému riziku pre práva fyzickej osoby.

Oznamovaciu povinnosť má prevádzkovateľ aj vo vzťahu k Úradu na ochranu osobných údajov, ktorému je povinný oznámiť porušenie ochrany osobných údajov najneskôr do 72 hodín po tom, ako sa o ňom dozvedel. Túto povinnosť nemá len v tom prípade, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby.

Sankcie za porušenie povinností

Sankcie predstavujú zákonom predvídaný spôsob trestu za nedodržanie povinností, ktoré zákonodarca ukladá všetkým, ktorí spracúvajú osobné údaje. Nová európska úprava priniesla zmeny aj v oblasti trestania za nedodržanie povinností.

Príslušný orgán môže uložiť pokutu **prevádzkovateľovi** až do výšky 10 000 000 Eur, alebo ak ide o podnik do 2 % celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia za neplnenie alebo porušenie zákonom alebo Nariadením GDPR ustanovených povinností:

a) osobitné povinnosti prevádzkovateľa pri získavaní súhlasu pri poskytovaní služieb informačnej spoločnosti podľa § 15,
b) povinnosti pri spracúvaní osobných údajov bez potreby identifikácie podľa § 18,
c) všeobecné povinnosti prevádzkovateľa podľa § 31 až 35,
d) povinnosť viesť záznamy o spracovateľských činnostiach podľa § 37,
e) povinnosti týkajúce sa bezpečnosti osobných údajov, vrátane povinnosti oznámiť porušenie ochrany osobných údajov dotknutej osobe a úradu podľa § 39 až 41,
f) povinnosti v súvislosti s posúdením vplyvu na ochranu osobných údajov a predchádzajúcej konzultácie podľa § 42 až 43,
g) povinnosti v súvislosti s určením zodpovednej osoby podľa § 44 až 45,
h) povinnosť zachovávať mlčanlivosť podľa § 79.

Sankcie môžu byť uložené aj iným subjektom než prevádzkovateľovi, a to sprostredkovateľovi za porušenie obdobných povinností ako prevádzkovateľ, keďže jeho pozícia v procese spracúvania osobných údajov je obdobná pozícii samotného prevádzkovateľa. Sankcie môžu byť uložené aj certifikačnému subjektu alebo monitorujúcemu subjektu, a to za porušenie povinností, ktoré im zveruje zákon.

Pokutu až do výšky 20 000 000 Eur môže úrad uložiť **každému, kto:**

a) nesplnil alebo porušil niektorú zo základných zásad spracúvania osobných údajov – napr. porušenie zásady zákonnosti, zásadu minimalizácie osobných údajov, etc.;
b) nesplnil alebo porušil niektoré z práv dotknutej osoby – napr. porušenie informačnej povinnosti voči dotknutej osobe;
c) nesplnil alebo porušil niektorú z povinností pri prenose osobných údajov príjemcovi v tretej krajine alebo medzinárodnej organizácii;
d) nesplnil alebo porušil niektorú z povinností zákonného spracúvania osobných údajov;

e) nesplnil úradom uložené opatrenie na nápravu a lehotu na vykonanie nariadeného opatrenia.[8]

Spoloční prevádzkovatelia

Spoločnými prevádzkovateľmi sú dvaja alebo viacerí prevádzkovatelia, ktorí si dohodou určia účel a prostriedky spracúvania osobných údajov. V dohode sú zároveň povinní transparentne určiť zodpovednosť každého z nich za plnenie povinností a úloh v súlade so zákonom. V dohode musí byť určené kontaktné miesto pre dotknutú osobu.

Sprostredkovateľ

Sprostredkovateľ je subjekt, ktorý sa môže, ale zároveň aj nemusí vyskytnúť v konkrétnej reťazi vzťahov pri zabezpečovaní ochrany osobných údajov. Už z označenia tohto subjektu vyplýva, že jeho funkcia je „*niečo*" sprostredkovať, pričom však z podstaty inštitútu vyplýva, že sprostredkovanie je len možnosť, a nie povinnosť. Teda, povedané inými slovami prevádzkovateľ sa môže rozhodnúť, či využije alebo nevyužije prostredníka/sprostredkovateľa pri zabezpečovaní ochrany osobných údajov. Závisí to nepochybne najmä od možnosti a schopností prevádzkovateľa postarať sa o spracúvanie osobných údajov sám.

Sprostredkovateľ spracúva osobné údaje v mene prevádzkovateľa, ktorý rozhoduje o účele a dôvode spracúvania. Vzťah medzi prevádzkovateľom a sprostredkovateľom je vzťahom obchodným, keďže sprostredkovateľ vykonáva tieto činnosti pre prevádzkovateľa ako profesionál – odborník. Sprostredkovateľskú zmluvu upravuje § 642 a nasl. Obchodného zákonníka, i keď označenie tejto zmluvy nemusí byť priamo sprostredkovateľská. V praxi sú frekventovanejšie označenia ako napríklad zmluva o spracúvaní osobných údajov. **Zmluva o spracúvaní osobných údajov** sa spravidla uzatvára ako sekundárny sprievodný právny vzťah, to znamená, že dôvodom zmluvného vzťahu prevádzkovateľa a sprostredkovateľa nemusí byť priamo ochrana osobných údajov, ale vyplýva z hlavného záväzkového vzťahu. V praxi sa častokrát ustanovenia sprostredkovateľskej zmluvy môžu subsumovať do ustanovení hlavnej zmluvy.

Za sprostredkovateľa sa nepovažuje zamestnanec prevádzkovateľa. Ak tento nakladá s osobnými údajmi, tak je to v mene prevádzkovateľa, ako keby s nimi nakladal prevádzkovateľ sám. Následne sa vzťah tohto zamestnanca a prevádzkovateľa spravuje pri zabezpečovaní adekvátnej ochrany spracovávaných údajov uzatvorenou pracovnou zmluvou a príslušnými právnymi predpismi. Ak príslušný zamestnanec poruší svoje povinnosti a týmto dôjde k porušeniu ochrany osobných údajov dotknutej osoby, je toto porušenie pričítateľné samotnému prevádzkovateľovi, a nie konkrétnemu zamestnancovi. Postihnuteľnosť jeho konania (alebo nekonania) sa bude následne riešiť podľa pravidiel pracovného práva.

Medzi **povinnosti sprostredkovateľa** zaraďujeme:

a) povinnosť spracúvať osobné údaje len na základe písomných pokynov prevádzkovateľa – táto povinnosť je úzko spätá so zodpovednosťou oboch strán, t. j. prevádzkovateľa i sprostredkovateľa. Na vymedzenie deliacej čiary medzi zodpovednosťou prevádzkovateľa a sprostredkovateľa je potrebné, aby boli všetky pokyny prevádzkovateľa udelené sprostredkovateľovi jasné, presné, určité a zdokumentované.[9] Zodpovednosť na strane

[8] Prevzaté: Pohorelá, P., Ukladanie pokút podľa GDPR. Dostupné: https://www.podnikajte.sk/zakonne-povinnosti-podnikatela/pokuty-podla-gdpr. Citované: 28.2.2019

[9] Hudecová, Cyprichová, Makatura a kol., Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. Bratislava, Eurokódex, 2018, s. 319 a nasl.).

sprostredkovateľa vzniká jednoznačne vtedy, ak spracúva osobné údaje nad rámec dohody s prevádzkovateľom.;

b) povinnosť zabezpečiť, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovajú mlčanlivosť – v prípade, ak sprostredkovateľ spracúva osobné údaje prostredníctvom ďalších osôb, najmä svojich zamestnancov, je potrebné, aby boli zaviazané zachovávať dôvernosť informácií, ku ktorým majú v súvislosti so spracovávaním údajov prístup.;
c) povinnosť prijať primerané technické a organizačné opatrenia na zaistenie bezpečnosti spracúvania osobných údajov;
d) povinnosť dodržiavať podmienky zapojenia ďalšieho sprostredkovateľa – sprostredkovateľ je oprávnený zapojiť ďalší medzičlánok do procesu spracovávania údajov, t. j. ďalšieho sprostredkovateľa len so súhlasom prevádzkovateľa.

Za porušenie svojich povinností je sprostredkovateľ sankcionovateľný obdobne ako prevádzkovateľ. Vzťah medzi prevádzkovateľom a sprostredkovateľom sa riadi osobitnou zmluvou, čiže nedodržanie jednak zákonných povinností alebo povinností nad rámec zákona dohodnutých v zmluve, je sankcionovateľné.

Dotknutá osoba

Dotknutou osobou je **každá fyzická osoba, ktorej osobné údaje sa spracúvajú**. To znamená, že dotknutou osobou nemôže byť právnická osoba.

GDPR upravuje tieto základné práva dotknutých osôb:

a) právo na poskytnutie informácií
b) právo na prístup k údajom
c) právo na opravu
d) právo na obmedzenie spracúvania
e) právo „na zabudnutie“
f) právo na prenosnosť údajov
g) právo namietať spracúvanie na účely priameho marketingu a profilovanie
h) právo na súdny prostriedok nápravy
i) právo na náhradu škody

Právo na poskytnutie informácií

Toto právo dotknutej osoby súvisí s informačnou povinnosťou prevádzkovateľa. GDPR zakotvuje právny rámec informačnej povinnosti prevádzkovateľa na poskytovanie informácii dotknutej osobe, ktoré sa týkajú spracovania jej osobných údajov. Uvedené údaje sa musia poskytnúť v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme tak, aby aj osoba bez vzdelania porozumela uvedeným informáciám. Prevádzkovateľ, ktorý získava osobné údaje dotknutej osoby je povinný ju informovať napríklad o svojej totožnosti, pričom je povinný poskytnúť aj svoje kontaktné údaje, resp. kontaktné údaje na svojho zástupcu. Ďalej je povinný poskytnúť jej údaje o oprávnených záujmoch, ak je spracovanie nevyhnutné na účely oprávnených záujmov. Poskytuje jej tiež informáciu o príjemcoch týchto údajov, ak existujú, prípadne aj informáciu o tom, či prevádzkovateľ zamýšľa preniesť osobné údaje do tretej krajiny. Prevádzkovateľ je povinný poskytnúť aj údaje o účele spracúvania, informácie o predpokladanej dobe uchovávania údajov a pod. Dôležitou poznámkou pri informačnej povinnosti je, že sa neviaže len na okamih získavania osobných údajov. Prevádzkovateľ je povinný oznámiť dotknutým osobám každú zmenu, a zabezpečiť túto povinnosť od získania až po výmaz osobných údajov.

Právo na prístup k údajom

Dotknutá osoba by mala mať právo na prístup k osobným údajom, ktoré boli o nej získané, a uvedené právo aj jednoducho a v primeraných intervaloch uplatňovať, aby si bola vedomá zákonnosti spracúvania a mohla si ju overiť. K tomu patrí aj právo dotknutých osôb na prístup k údajom týkajúcim sa ich zdravia, napríklad k údajom v ich lekárskych záznamoch obsahujúcich informácie ako diagnóza, výsledky vyšetrení, posudky ošetrujúcich lekárov a akákoľvek poskytnutá terapia alebo uskutočnené zákroky. Každá dotknutá osoba by preto mala mať právo vedieť a byť informovaná najmä o účeloch spracúvania osobných údajov, podľa možnosti o dobe spracúvania osobných údajov, o príjemcoch osobných údajov, o postupe v každom automatickom spracúvaní osobných údajov a aspoň v prípadoch, v ktorých sa spracúvanie opiera o profilovanie, o následkoch takéhoto spracúvania. Ak je to možné, prevádzkovateľ by mal môcť poskytnúť prístup na diaľku k bezpečnému systému, ktorý by dotknutej osobe zabezpečil priamy prístup k jej osobným údajom.

Právo na opravu

Právo dotknutej osoby na opravu je uvedené v čl. 16 GDPR. V zmysle tohto článku má dotknutá osoba právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účely spracúvania má dotknutá osoba právo na doplnenie neúplných osobných údajov, a to aj prostredníctvom poskytnutia doplnkového vyhlásenia. *Právom na opravu by však nemal byť napríklad dotknutý obsah svedeckej výpovede.*

Právo na obmedzenie spracúvania

Uvedené právo je upravené v čl. 18 GDPR ako aj v ustanovení § 24 zákona o ochrane osobných údajov. *Fyzická osoba by mala mať právo na obmedzenie spracúvania, ak napadne správnosť osobných údajov a nemožno určiť ich správnosť či nesprávnosť, alebo keď je potrebné osobné údaje uchovať na účely dokazovania. Namiesto vymazania osobných údajov by sa spracúvanie malo obmedziť najmä vtedy, keď sa v osobitnom prípade možno odôvodnene domnievať, že vymazanie by mohlo ovplyvniť oprávnené záujmy dotknutej osoby. V takomto prípade by sa obmedzené údaje mali spracúvať len na účely, ktoré zabránili ich vymazaniu. Metódy na obmedzenie spracúvania osobných údajov by okrem iného mohli zahŕňať presunutie vybraných údajov do iného systému spracúvania, napríklad na účely archivácie, alebo zamedzenie prístupu k nim. V automatizovaných informačných systémoch by sa obmedzenie spracúvania malo v zásade zabezpečiť technickými prostriedkami. Skutočnosť, že spracúvanie osobných údajov je obmedzené, by sa v systéme mala vyznačiť tak, aby bolo jednoznačné, že spracúvanie osobných údajov je obmedzené. Takáto oprava alebo vymazanie osobných údajov alebo obmedzenie spracúvania by sa mali oznámiť príjemcom, ktorým sa údaje poskytli, a príslušným orgánom, od ktorých nesprávne údaje pochádzajú. Príslušné orgány by takisto mali upustiť od ďalšieho šírenia takýchto údajov.*

„Obmedzenie“ znamená, že osobné údaje dotknutej osoby môžu byť, s výnimkou ukladania, spracúvané s jej súhlasom len pri zriaďovaní, výkone alebo obhajobe právnych nárokov, na ochranu práv inej fyzickej alebo právnickej osoby alebo z dôvodov verejného záujmu EÚ alebo členského štátu EÚ. Ak sa obmedzenie zruší, musí byť dotknutá osoba vopred informovaná.

Príkladom uvedeného je situácia, ak nová banka na domácom trhu ponúka ponuky na úver na kúpu domu. Kupujete nový dom a rozhodnete sa zmeniť banku. Vyzvete „starú“ banku, aby zatvorila všetky účty, a požiadate o vymazanie všetkých vašich osobných údajov. Stará banka však podlieha právnym predpisom, ktoré nariaďujú bankám, aby uchovávali všetky podrobnosti o zákazníkoch počas

desiatich rokov. Stará banka je zo zákona povinná ukladať vaše údaje, ale aj napriek tomu môžete požiadať o obmedzenie údajov, aby ste zabezpečili, že sa „náhodne“ nepoužijú na neželané účely[10].

Právo „na zabudnutie“ alebo právo na vymazanie

Významným právom, ktoré súvisí s ochranou osobných údajov, je aj právo byť zabudnutý alebo právo na vymazanie, ktoré je upravené v čl. 17 GDPR.

V zmysle tohto článku má dotknutá osoba právo dosiahnuť u prevádzkovateľa vymazanie osobných údajov, ktoré sa jej týkajú, a to bez zbytočného odkladu. Prevádzkovateľ je povinný vymazať tieto osobné údaje v prípade, ak:

a) tieto osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali,
b) dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie vykonáva a ak neexistuje iný právny základ pre spracúvanie,
c) dotknutá osoba namieta voči spracúvaniu podľa čl. 21 ods. 1 GDPR a neprevažujú žiadne oprávnené dôvody na spracúvanie,
d) osobné údaje sa spracúvali nezákonne,
e) osobné údaje musia byť vymazané, aby sa splnila zákonná povinnosť podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha,
f) osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti podľa článku 8 ods. 1 (súhlas dieťaťa v súvislosti so službami informačnej spoločnosti)

Nariadenie zároveň určuje aj prípady, kedy **nebude možné vyhovieť dotknutej osobe** a takáto osoba nebude môcť úspešne uplatniť právo na zabudnutie, a to napríklad ak spracúvanie jej osobných údajov bude potrebné na uplatnenie práva na slobodu prejavu a na informácie, z dôvodov verejného záujmu v oblasti verejného zdravia, na účely archivácie vo verejnom záujme, na účely vedeckého a historického výskumu alebo napríklad na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

Právo na prenosnosť údajov

Právo na prenosnosť údajov je upravené v čl. 20 GDPR ako aj v ustanovení § 26 zákona o ochrane osobných údajov. Vychádzajúc z dôvodovej správy k zákonu o ochrane osobných údajov bolo toto právo zavedené s cieľom posilniť kontrolu nad vlastnými osobnými údajmi dotknutej osoby. Uplatniť toto právo je možné v prípade, že sa spracúvanie osobných údajov vykonáva u prevádzkovateľa automatizovanými prostriedkami spracúvania, možnosť získať jej osobné údaje, ktoré poskytla prevádzkovateľovi v štruktúrovanom a interoperabilnom formáte a preniesť ich k ďalšiemu prevádzkovateľovi, a to bez toho, aby prvý prevádzkovateľ, ktorému ich poskytla, jej v tom akokoľvek bránil alebo ju v tomto práve obmedzoval.

Uvedené platí v prípadoch, ak spracúvanie osobných údajov týkajúcich sa dotknutej osoby:

a) je založené na súhlase so spracúvaním osobných údajov poskytnutom samotnou dotknutou osobou alebo

[10] Pozri: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/when-should-i-exercise-my-right-restriction-processing-my-personal-data_sk)

b) ak je spracúvanie osobných údajov založené na zmluvnom vzťahu, ktorého je dotknutá osoba zmluvnou stranou alebo
c) je vykonávané u prevádzkovateľa automatizovanými prostriedkami spracúvania.

Uplatňovaním práva na prenosnosť osobných údajov nie je dotknuté právo dotknutej osoby požadovať výmaz jej osobných údajov a obmedzenie tohto práva na výmaz.

Právo na prenosnosť údajov nemá viesť k vymazaniu osobných údajov dotknutej osoby, ktoré poskytla na účely plnenia zmluvy, v takom rozsahu a počas takého obdobia, ako sú tieto osobné údaje potrebné na plnenie danej zmluvy. Právo na prenosnosť osobných údajov dotknutej osoby sa uplatňuje na tie jej osobné údaje, na ktorých spracúvanie poskytla dotknutá osoba súhlas alebo ak je spracúvanie potrebné na plnenie zmluvy. Toto právo na prenosnosť osobných údajov sa neuplatní, ak je spracúvanie založené na inom právnom základe, než je súhlas alebo zmluva. Zo samotnej povahy uvedeného práva vyplýva, že by sa nemalo uplatňovať voči prevádzkovateľom, ktorí spracúvajú osobné údaje týkajúce sa dotknutej osoby pri výkone ich verejných úloh, alebo sa nebude uplatňovať, ak je spracúvanie osobných údajov potrebné na plnenie zákonnej povinnosti, ktorá sa na prevádzkovateľa vzťahuje, alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi. Ak je to technicky možné, mala by mať dotknutá osoba právo na prenos osobných údajov priamo od jedného prevádzkovateľa k druhému prevádzkovateľovi.

Právo na prenosnosť údajov by sa malo vždy dotknúť len konkrétnej dotknutej osoby, ktorá si ho uplatňuje, čo znamená, že jeho výkonom nemajú byť dotknuté práva iných osôb.

Právo namietať spracúvanie na účely priameho marketingu a profilovanie

Ďalším právom dotknutej osoby je právo namietať spracúvanie na účely priameho marketingu a profilovanie. Ak sa osobné údaje spracúvajú na účely priameho marketingu, dotknutá osoba má právo kedykoľvek namietať proti spracúvaniu svojich osobných údajov vrátane profilovania. Ak dotknutá osoba namieta voči spracúvaniu na účely priameho marketingu, prevádzkovateľ už jej osobné údaje na tieto účely nesmie spracúvať.

Profilovanie dotknutých osôb je definované v GDPR, a to v čl. 4 ods. 4 ako *„akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom.“*

Ako príklady profilovania dotknutých osôb možno uviesť:

- spracúvanie osobných údajov na účely tzv. behaviorálnej reklamy, ktorá je založená na predpokladoch záujmov dotknutej osoby v dôsledku jej online správania (prezeranie určitých stránok, likes, lokalizačné služby cez technológie);
- spracúvanie osobných údajov poisťovňou na účely analýzy poistného rizika alebo identifikovanie potenciálnych poistných podvodov;
- spracúvanie osobných údajov veriteľom (napr. bankou alebo iným oprávneným subjektom) pri preverovaní bonity záujemcu o úver (napr. prostredníctvom údajov z elektronických registrov údajov o spotrebiteľských úveroch);
- vylúčenie uchádzača o zamestnanie v dôsledku aplikovania plne automatizovaného vyhodnocovania prijatých životopisov v elektronickej forme, ktoré sa postupne začína využívať vo väčších agentúrach v prvej fáze obsadzovania pracovného miesta na odfiltrovanie nevhodných uchádzačov pri väčších počtoch prijatých životopisov.

Najčastejším príkladom profilovania je spracúvanie osobných údajov na účely tzv. behaviorálnej reklamy. Uvedené využívajú obchodníci za účelom marketingu, reklamy a ponuky tovarov. Čo sa týka

ďalších príkladov profilovania, ktoré sme uviedli vyššie, v tomto prípade profilovanie naráža na právne normy regulujúce ochranu osobných údajov. V zmysle GDPR by dotknutá osoba by mala mať právo nepodliehať rozhodnutiu hodnotiacemu osobné aspekty, ktoré sa jej týkajú, založenému výlučne na automatizovanom spracúvaní a ktoré má právne účinky, ako je napríklad automatické zamietnutie online žiadosti o úver alebo elektronické postupy prijímania pracovníkov bez akéhokoľvek ľudského zásahu, musia byť ustanovené primerané záruky ochrany práv dotknutej osoby, najmä právo na overenie rozhodnutia nie automatizovaným spôsobom zo strany príslušného orgánu

Okrem toho zákonná úprava uvádza, že **rozhodnutia založené na profilovaní sa nesmú zakladať na osobitných kategóriách osobných údajov** (napr. informáciách o rasovej, etnickej alebo náboženskej príslušnosti); výnimky v tomto prípade predstavuje verejný záujem a súhlas dotknutej osoby.

V zmysle § 66 ods. 3 zákon č. 18/1918 o ochrane osobných údajov **je zakázané**:

- také profilovanie, ktoré vedie k diskriminácii osôb na základe osobitných kategórií osobných údajov,
- profilovanie, ktoré nie je realizované zákonným spôsobom.

Aj keď je profilovanie inak zákonné a môže byť v mnohých prípadoch nápomocné, dotknutá osoba má právo vzniesť kedykoľvek námietku. Na základe námietky dotknutej osoby k profilovaniu, ktoré je inak podľa GDPR povolené a legálne, sa musí spracúvanie skončiť, pokiaľ prevádzkovateľ nepreukáže presvedčivé oprávnené dôvody na spracúvanie, ktoré majú prednosť pred záujmami, právami a slobodami dotknutej osoby.

Právo na súdny prostriedok nápravy

V zmysle čl. 79 Nariadenia, bez toho, aby bol dotknutý akýkoľvek dostupný správny alebo mimosúdny prostriedok nápravy vrátane práva na podanie sťažnosti dozornému orgánu, každá dotknutá osoba má právo na účinný súdny prostriedok nápravy, ak sa domnieva, že v dôsledku spracúvania jej osobných údajov v rozpore s platnými právnymi predpismi došlo k porušeniu jej práv. Návrh na začatie konania proti prevádzkovateľovi alebo sprostredkovateľovi sa podáva na súdoch členského štátu, v ktorom má prevádzkovateľ alebo sprostredkovateľ prevádzkareň. Návrh na začatie takéhoto konania možno podať aj na súdoch členského štátu, v ktorom má dotknutá osoba svoj obvyklý pobyt, pokiaľ prevádzkovateľom alebo sprostredkovateľom nie je orgán verejnej moci členského štátu konajúci v rámci výkonu verejnej moci.

Dotknutá osoba má právo poveriť neziskový subjekt, organizáciu alebo združenie, ktoré boli riadne zriadené v súlade s právom členského štátu, ktorých ciele podľa stanov sú vo verejnom záujme a ktoré pôsobia v oblasti ochrany práv a slobôd dotknutých osôb, pokiaľ ide o ochranu ich osobných údajov, aby podali sťažnosť v jej mene, aby v jej mene uplatnili práva podľa článkov 77, 78 a 79 GDPR a aby v jej mene uplatnili právo na náhradu škody podľa článku 82 GDPR, ak to umožňuje právo členského štátu.

Právo na náhradu škody

Každá osoba (nielen dotknutá osoba), ktorá utrpela majetkovú alebo nemajetkovú ujmu v dôsledku porušenia GDPR, má právo na náhradu utrpenej škody od prevádzkovateľa alebo sprostredkovateľa.

Prevádzkovateľ, ktorý sa zúčastnil na spracúvaní, je zodpovedný za škodu spôsobenú spracúvaním, ktoré bolo v rozpore s GDPR. Sprostredkovateľ zodpovedá za škodu spôsobenú spracúvaním, len ak neboli splnené povinnosti, ktoré sa GDPR ukladajú výslovne sprostredkovateľom, alebo ak konal nad rámec alebo v rozpore s pokynmi prevádzkovateľa, ktoré boli v súlade so zákonom.

Prevádzkovateľ alebo sprostredkovateľ je zbavený zodpovednosti podľa odseku 2, ak sa preukáže, že nenesie žiadnu zodpovednosť za udalosť, ktorá spôsobila škodu. Ak sa na tom istom spracúvaní zúčastnil viac než jeden prevádzkovateľ alebo sprostredkovateľ alebo prevádzkovateľ aj sprostredkovateľ spoločne a sú zodpovední za škodu spôsobenú spracúvaním, každý z nich zodpovedá za celú škodu, aby sa dotknutej osobe zabezpečila účinná náhrada.

S poslednými dvoma právami, t. j. právo na súdny prostriedok nápravy a právo na náhradu škody súvisí možnosť dotknutej osoby takpovediac brániť sa pred porušením ochrany osobných údajov, resp. žiadať o nápravu po zistení porušenia. Jednou z možností, ktorú predpokladá zákonodarca je aj možnosť podať sťažnosť dozornému orgánu. Uvedenú možnosť predpokladá čl. 77 GDPR, v zmysle ktorého „*bez toho, aby boli dotknuté akékoľvek iné správne alebo súdne prostriedky nápravy, má každá dotknutá osoba právo podať sťažnosť dozornému orgánu, najmä v členskom štáte svojho obvyklého pobytu, mieste výkonu práce alebo v mieste údajného porušenia, ak sa domnieva, že spracúvanie osobných údajov, ktoré sa jej týka, je v rozpore s týmto nariadením*“. Následne, dozorný orgán, ktorému sa sťažnosť podala je povinný informovať sťažovateľa o pokroku a výsledku sťažnosti vrátane možnosti podať súdny prostriedok nápravy podľa čl. 78 GDPR.

V každom členskom štáte, je pre úsek kontroly dodržiavania predpisov na ochranu osobných údajov, zriadený Úrad na ochranu osobných údajov (ďalej len „Úrad“). Úrad okrem iných povinností prešetruje aj sťažnosti dotknutých osôb, ktoré sa domnievajú, že postupom prevádzkovateľa alebo sprostredkovateľa došlo k porušeniu práv fyzických osôb pri spracúvaní ich osobných údajov. Uvedené je aj účelom konania o ochrane osobných údajov. Úrad je v prípade zistenia nedostatkov oprávnený uložiť opatrenia na nápravu, prípadne sankcie.

Zodpovedná osoba

Zákonodarca stanovuje podmienky kedy je prevádzkovateľ povinný ustanoviť zodpovednú osobu a kto môže resp. nemôže byť zodpovednou osobou. V zmysle § 44 ods. 1 Prevádzkovateľ a sprostredkovateľ sú povinní určiť zodpovednú osobu, ak

a) spracúvanie osobných údajov vykonáva orgán verejnej moci alebo verejnoprávna inštitúcia okrem súdov pri výkone ich súdnej právomoci,
b) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah alebo účel vyžadujú pravidelné a systematické monitorovanie dotknutej osoby vo veľkom rozsahu, alebo
c) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií osobných údajov podľa § 16 vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 vo veľkom rozsahu.

Zákon stanovuje aj **úlohy zodpovednej osoby**, a to:

a)poskytuje informácie a poradenstvo prevádzkovateľovi alebo sprostredkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa tohto zákona, osobitných predpisov alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná, týkajúcich sa ochrany osobných údajov,

b) monitoruje súlad s týmto zákonom, osobitnými predpismi alebo medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, týkajúcimi sa ochrany osobných údajov a s pravidlami prevádzkovateľa alebo sprostredkovateľa súvisiacimi s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy osôb, ktoré sú zapojené do spracovateľských operácií a súvisiacich auditov ochrany osobných údajov,

c)poskytuje na požiadanie poradenstvo, ak ide o posúdenie vplyvu na ochranu osobných údajov a monitorovanie jeho vykonávania podľa § 42,

d)spolupracuje s úradom pri plnení svojich úloh,

e)plní úlohy kontaktného miesta pre úrad v súvislosti s otázkami týkajúcimi sa spracúvania osobných údajov vrátane predchádzajúcej konzultácie podľa § 43 a podľa potreby aj konzultácie v iných veciach.

Príjemca a tretia strana

Príjemcom je každý, komu sa osobné údaje **poskytnú** bez ohľadu na to, či je treťou stranou. Príjemcom je každý, komu boli osobné údaje poskytnuté alebo sprístupnené. Príjemcom môže byť aj tretia strana.

Príjemcom však **nie je** orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je SR viazaná. To znamená, že príjemcom nie sú ústredné orgány štátnej správy, ministerstvá, ani samotný Úrad na ochranu osobných údajov nie je príjemcom. Tieto subjekty sú v pozícií tretích strán.

Príjemcom sú napríklad zdravotné poisťovne, ktorým sa osobné údaje poskytujú na účely úhrady poskytnutých služieb z verejného zdravotného poistenia. **Príjemcom** údajov môžu byť aj zmluvní partneri prevádzkovateľa na osobitné účely (napr. právne služby, audítorské služby, služby v oblasti informačných technológií, etc.).

Treťou stranou je každý, kto nie je dotknutou osobou – prevádzkovateľom, sprostredkovateľom alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje. Pôjde napríklad o orgán štátnej správy, územnej samosprávy, iný orgán verejnej moci, fyzické a právnické osoby, ktorým prevádzkovateľ poskytuje osobné údaje a ktoré tieto údaje ďalej spracúvajú vo vlastnom informačnom systéme.

ZÁVER

Predložený dokument poukázal na základné definičné východiská ochrany osobných údajov, na jej normatívne zakotvenie v právnom poriadku Európskej únie a vnútroštátnych právnych úpravách, ako aj na kľúčové zásady spracúvania osobných údajov a práva dotknutých osôb. Tieto prvky tvoria základný rámec zabezpečujúci rovnováhu medzi ochranou súkromia jednotlivca a legitímnymi potrebami spracúvania údajov v modernom digitálnom prostredí.

Z analýzy vyplýva, že právna úprava ochrany osobných údajov, reprezentovaná najmä všeobecným nariadením o ochrane údajov (GDPR), poskytuje komplexný a systematický mechanizmus ochrany práv jednotlivcov a zodpovednosti prevádzkovateľov. Zásady zákonnosti, transparentnosti, minimalizácie údajov či zodpovednosti vytvárajú normatívny základ, ktorý by mal zabezpečiť spravodlivé a bezpečné spracúvanie osobných údajov. Súčasne však praktická aplikácia týchto pravidiel poukazuje na pretrvávajúce výzvy, najmä pokiaľ ide o interpretáciu niektorých pojmov, administratívnu náročnosť plnenia povinností a efektívne uplatňovanie práv dotknutých osôb v praxi.

Možno konštatovať, že ochrana osobných údajov už nemožno vnímať len ako izolovanú právnu disciplínu, ale ako integrálnu súčasť širšieho systému ochrany základných práv a fungovania digitálnej ekonomiky. Jej ďalší vývoj bude nevyhnutne ovplyvnený technologickým pokrokom, rastúcim významom dát a požiadavkou na zabezpečenie dôvery verejnosti v spracúvanie osobných údajov. V tomto kontexte zostáva kľúčovou úlohou právnej teórie aj praxe hľadať rovnováhu medzi efektívnou ochranou jednotlivca a umožnením legitímneho a inovatívneho využívania údajov, ktoré je nevyhnutné pre fungovanie súčasnej spoločnosti.

POUŽITÉ ZDROJE

[1] ADAMOVÁ, Z. a kol.: Princípy európskeho zmluvného práva. Bratislava: IURA EDITION 2009,
[2] FEKETE, I.: Občiansky zákonník. Veľký komentár. 1.diel. Bratislava: Eurokódex, 2011
[3] FRIMMEL M., *Elektronický obchod*, 1.vydanie, 2002, Praha: Prospektum
[4] HUČKOVÁ,R.: Nové mechanizmy uplatňovania práv spotrebiteľov. In: Studia Iuridica Cassoviensia, Roč. 4, č. 1 (2016)
[5] HUDECOVÁ, CYPRICHOVÁ, MAKATURA a kol., Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. Bratislava, Eurokódex, 2018
[6] HUSOVEC, M. *Injunctions against Intermediaries in the European Union. Accountable but not Liable?* 2017: Cambridge University Press
[7] HUSOVEC, M. Zodpovednosť na internete podľa českého a slovenského práva. Praha: CZ.NIC, z. s. p. o., 2014
[8] KARAS, V. - KRÁLIK, A. Právo Európskej únie. Praha: C. H. Beck, 2012
[9] KASL, F.: Internet věcí a ochrana dát v europském kontextu. In.: Revue pro právo a technológie [Online]. 2016, č. 13, dostupné z https://journals.muni.cz/revue/article/view/5422/pdf
[10] MATES, P. – JANEČKOVÁ, E. – BARTÍK, V.: Ochrana osobních údaju. Praha: Leges, 2012
[11] MAISNER, M. a kol.: Základy softwarového práva. Praha: Wolters Kluwer Česká republika, 2011
[12] PATTYNOVÁ, J. - SUCHÁNKOVÁ, L. - ČERNÝ, J. a kol.: Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světe. Komentář. Praha: Leges, 2018
[13] POHORELÁ, P., Ukladanie pokút podľa GDPR. Dostupné z https://www.podnikajte.sk/zakonne-povinnosti-podnikatela/pokuty-podla-gdpr.
[14] PURTOVA, N. The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. In: Law, Innovation and Technology, roč. 2018, č. 10:1
[15] SCHWARCZ, J. – STEC, A.: Ochrana osobných údajov. In.: SUCHOŽA, J. , HUSÁR, J., HUČKOVÁ, R. (eds.): Právo, obchod, ekonomika V. Košice: Univerzita P.J.Šafárika v Košiciach, 2015
[16] Rozsudok Súdneho dvora vo veci C-210/16 Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388
[17] Rozsudok Súdneho dvora zo dňa 1. októbra 2019 vo veci C-673/17 Planet49, ECLI:EU:C:2019:801
[18] Rozsudok Súdneho dvora z 24. novembra 2011 vo veci C-70/10 Scarlet Extended, ECLI:EU:C:2011:771
[19] Rozsudok Súdneho dvora z 19. októbra 2016 vo veci C-582/14 Breyer. ECLI:EU:C:2016:779
[20] Rozsudok Súdneho dvora vo veci C-352/85 Bond van Adverteerders/Holandské kráľovstvo, ECLI:EU:C:1988:196
[21] Rozsudok Súdneho dvora vo veci C-291/13 Papasavvas, ECLI:EU:C:2014:2209
[22] Uznesenie Súdneho Dvora zo dňa 19. februára 2009 vo veci C-557/07, LSG – Gesellschaft zur Wahrnehmung von Leistungsschutzrechten, ECLI:EU:C:2009:107
[23] Rozsudok Súdneho dvora zo dňa 12. júla vo veci C-324/09, L'Oréal a i. ECLI:EU:C:2011:474
[24] Rozsudok Súdneho dvora zo dňa 16. februára 2012 vo veci C-360/10, SABAM, ECLI:EU:C:2012:85
[25] Rozsudok Súdneho dvora zo dňa 15. septembra 2016 vo veci C-484/14, Mc Fadden, ECLI:EU:C:2016:689
[26] Rozsudok Súdneho dvora zo dňa 7. júla 2016 vo veci C-494/15, Tommy Hilfiger Licencing a i. ECLI:EU:C:2016:528
[27] Rozsudok Súdneho dvora vo veci C-101/01 Lindqvist, ECLI:EU:C:2003:596
[28] Rozsudok Súdneho dvora z 13. mája 2014 vo veci C-131/12 Google Spain a Google, ECLI:EU:C:2014:317

[29] Rozsudok Súdneho dvora z 23. marca 2010 v spojených veciach C-236/08 až C-238/08 Google France a Google, ECLI:EU:C:2010:159, bod 111.