Ochrana fyzických osôb pri spracúvaní osobných údajov/GDPR
Veľký komentár

**Mgr. Irena Hudecová, Mgr. Anna Cyprichová,
Ing. Ivan Makatura a kolektív**

NARIADENIE O OCHRANE FYZICKÝCH OSÔB PRI SPRACÚVANÍ OSOBNÝCH ÚDAJOV/GDPR

Veľký komentár

2. zväzok

2. aktualizované vydanie

Strach zo zmeny je nepriateľom úspechu.

Bhagwan Maurya

Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR
2. zväzok, 2. aktualizované vydanie

2. vydanie komentára aktualizované k polovici februára 2020

Žilina, august 2020

ISBN 978-80-8155-095-9

www.eurokodex.sk

Predslov k 1. vydaniu

Milí čitatelia,

dňa 25. mája 2018 sa začalo uplatňovať Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov známe aj pod skratkou GDPR. Časy, kedy sme boli zvyknutí na to, že „nás" sa týkajú iba slovenské právne predpisy, sa stali minulosťou. Nariadenie ako právny akt EÚ má všeobecnú platnosť, je záväzné vo svojej celistvosti a priamo uplatniteľné vo všetkých členských štátoch EÚ. Svojou podstatou predstavuje právnu normu s vyššou právnou silou ako zákony Slovenskej republiky.

Nariadenie predstavuje bezpochyby jeden z kľúčových predpisov pre všetky subjekty pôsobiace v Európskej únii alebo zacielené na trh Európskej únie. Jeho cieľom je vrátiť dotknutým osobám kontrolu nad spracúvaním ich osobných údajov a odstrániť prekážky voľného pohybu osobných údajov v EÚ. Zavádza nielen harmonizované pravidlá ochrany osobných údajov, ale aj možnosť dozorných orgánov ukladať vysoké pokuty, ktoré boli vo väčšine prípadov príčinou toľkého záujmu venovanému tejto novej právnej úprave.

Dosah Nariadenia je obrovský. Bez akéhokoľvek preháňania môžeme povedať, že tento právny akt EÚ sa vzťahuje takmer na každého. A nemám tým na mysli iba veľké korporácie či finančné inštitúcie, telekomunikačných operátorov, dodávateľov energií či nemocnice. Aplikuje sa aj na lekárov, psychológov, advokátov, notárov, exekútorov, súdy, ministerstvá, obce a mestá, školy, škôlky, lekárne, e-shopy, cestovné kancelárie, personálne agentúry, účtovníkov, mzdárov, SBS, reklamné agentúry a mnoho ďalších podnikateľov z oblasti výroby či služieb. Výnimkou nie sú ani neziskové subjekty, politické strany či cirkvi. Veď kto dnes už len nespracúva osobné údaje?

Nariadenie vychádza z pravidiel obsiahnutých v Smernici o ochrane osobných údajov, ktorá bola základom právnej úpravy ochrany osobných údajov vyše 22 rokov. Tieto pravidlá sú vo viacerých smeroch podrobnejšie rozpracované, zohľadňujúc doterajšie názory pracovnej skupiny WP29, ako aj postoje a vyjadrenia Súdneho dvora EÚ či Európskeho súdu pre ľudské práva. Napriek tomu sa však mnohým z vás nová právna úprava spája s radom nezodpovedaných otázok, a to i napriek skutočnosti, že Nariadeniu bola v posledných dvoch rokoch venovaná nepretržitá pozornosť v médiách, na rôznych odborných fórach i konferenciách.

S cieľom objasniť zmysel a podstatu pravidiel ochrany osobných údajov obsiahnutých v Nariadení a tým vám pomôcť nastaviť ich správnu aplikáciu v praxi sme pre vás pripravili tento podrobný komentár. Komentár je jedinečným zhrnutím názorov, rád a dlhoročných praktických skúseností štyroch odborníkov z Úradu na ochranu osobných údajov SR spolu s odborníkmi z komerčného prostredia špecializujúcimi sa na ochranu osobných údajov, bezpečnosť informačných systémov a zastupovanie klientov v súvisiacich správnych a súdnych konaniach.

Komentár vám ponúka odborný a praktický pohľad na všetky dôležité výkladové aj aplikačné problémy:

— vysvetľuje sledovaný cieľ a účel Nariadenia, postupy pre správne určenie právneho základu spracúvania, plnenie povinností prevádzkovateľov a sprostredkovateľov vrátane uplatnenia certifikačných mechanizmov a kódexov správania,
— obsahuje praktickú stránku zabezpečenia súladu spracúvania osobných údajov s Nariadením, postup prevádzkovateľov pri získavaní súhlasu dotknutých osôb (v prípadoch, keď je potrebný), pri uplatnení existujúcich alebo nových práv dotknutých osôb,
— kontrola dodržiavania Nariadenia vrátane pravidiel vzťahujúcich sa na ukladanie sankcií je podrobne rozobraná odborníkmi z Úradu na ochranu osobných údajov SR s dlhoročnou praxou,
— bezpečnostným opatreniam a ochrane informačných systémov sa venuje dlhoročný expert a súdny znalec pre odvetvie bezpečnosti a ochrany informačných systémov,
— podmienky prenosov osobných údajov mimo krajín EÚ, vzájomný vzťah práva na ochranu osobných údajov s právom na slobodu prejavu, s právom na prístup verejnosti k úradným

dokumentom, s právami zamestnancov pri spracúvaní ich osobných údajov alebo záväzkom profesijnej mlčanlivosti spolu s prostriedkami správnej a súdnej nápravy je vysvetlený advokátkou z renomovanej advokátskej kancelárie G. Lehnert, k. s., s dlhoročnými skúsenosťami s poskytovaním poradenstva klientom v týchto oblastiach.

V snahe čo najviac reagovať na praktické problémy sme do komentára zahrnuli aj vyše 150 názorných príkladov a 150 relevantných záverov z judikatúry Súdneho dvora EÚ či Európskeho súdu pre ľudské práva. Pri jeho tvorbe sme zohľadňovali aj všetky najnovšie stanoviská pracovnej skupiny WP29.

Moja nesmierna vďaka patrí všetkým spoluautorom, ktorí napriek hektickému obdobiu, ktoré s príchodom Nariadenia prežívali, venovali dielu maximum svojho času a pozornosti. Špeciálne by som chcela poďakovať Aničke Cyprichovej za jej čas, neúnavnú energiu, prístup a nesmierne hladkú a efektívnu spoluprácu. Touto cestou by som rada vyjadrila svoje poďakovanie aj celému tímu ľudí z vydavateľstva, ktorí robili všetko pre to, aby sa komentár dostal čo najskôr k vám. Osobitné poďakovanie patrí našim rodinám, rodičom, manželom, manželkám, priateľom a deťom, ktorí nás pri tvorbe tak vytrvalo podporovali.

Komentár bol písaný pre vás všetkých, či už ste v pozícii osoby podieľajúcej sa na implementácii Nariadenia u prevádzkovateľa či sprostredkovateľa, alebo v role dotknutej osoby, ktorá má záujem dozvedieť sa viac o svojich právach. Pretože každý z nás sa v súkromnom živote stávame súčasťou procesu, v ktorom sú o nás spracúvané najrozličnejšie, často veľmi citlivé osobné údaje. Je prospešné a užitočné poznať svoje práva a nastaviť si mantinely zásahov do svojho súkromia tam, kde je to možné, na základe vlastného uváženého rozhodnutia. V neposlednom rade tento komentár slúži aj ako sprievodca pre tých, ktorí sú možno zmätení množstvom často protichodných alebo aj nesprávnych informácií a mýtov o Nariadení a jeho dôsledkoch.

Na záver by som vám všetkým chcela zaželať veľa šťastia pri implementovaní a uplatňovaní jednotlivých požiadaviek Nariadenia. Nariadenie prichádza so zmysluplnou myšlienkou chrániť súkromie nás všetkých. Do akej miery sa mu to podarí, závisí od každého z nás.

Irena Hudecová, hlavná autorka

Predslov k 2. vydaniu

Milí čitatelia,

oslovujeme vás takmer po 2 rokoch od vydania prvého komentára, ktorý bol v priebehu roka vypredaný. Veľmi nás teší váš záujem o našu publikáciu a nesmierne si vážime dôveru, ktorú nám tým vyjadrujete. O to väčšiu snahu a motiváciu sme mali rozšíriť komentár o ďalšie informácie, ktoré by vám mohli pomôcť pri riešení vašich konkrétnych situácií.

V prvom vydaní sme sa snažili priblížiť vám rozdiely, ktoré Nariadenie prináša v porovnaní s dovtedy platnými predpismi v oblasti ochrany osobných údajov, vysvetliť vám naše vnímanie jednotlivých ustanovení, ktoré sme pre lepšie pochopenie doplnili viac ako 150 praktickými prípadmi a výňatkami relevantnej judikatúry. Naším hlavným cieľom pri písaní druhého vydania bolo vytvoriť pre vás komplexný komentár, ktorý bude jedinečným zhrnutím našich znalostí a skúseností s aplikáciou Nariadenia, ako aj postojov, názorov a vyjadrení tých najdôležitejších inštitúcií, ktorých rozhodnutia a usmernenia zásadným spôsobom prispievajú k výkladu jednotlivých ustanovení Nariadenia. V tomto vydaní komentára sú preto zapracované relevantné **stanoviská Európskeho výboru pre ochranu údajov, judikatúra Súdneho dvora EÚ a Európskeho súdu pre ľudské práva** k problematike ochrany osobných údajov, ako aj najnovšie **rozhodnutia dozorných orgánov**. Relevantné závery uvedených súdov sú pritom pre väčšiu prehľadnosť spracované v texte samotného komentára, zatiaľ čo v časti judikatúry sú pri jednotlivom článku Nariadenia uvedené iba vybrané ustanovenia rozsudku relevantné vo vzťahu k problematike posudzovanej v danom článku.

Po viac ako 2 rokoch uplatňovania predpisu vo viac ako 29 štátoch sme sa snažili pomôcť nám všetkým zodpovedať otázku, aké prípady vnímajú dozorné orgány jednotlivých členských krajín ako porušenie Nariadenia a aké **sankcie**, resp. **správne pokuty** ukladajú. Do druhého vydania komentára sme doplnili aj **prehľadný zoznam všetkých zverejnených black listov a návrhov white listov**, ktorý nielen odzrkadľuje pohľad príslušného dozorného orgánu na rizikovosť danej spracovateľskej operácie, ale môže byť užitočnou pomôckou aj pre vás v prípadoch posudzovania vašej povinnosti vykonať posúdenie vplyvu na ochranu údajov.

Právo na ochranu osobných údajov nie je absolútnym právom. V praxi sa často dostáva do konfliktu s inými, v demokratickej spoločnosti rešpektovanými právami, ako napr. slobodou prejavu a právom na informácie, právom verejnosti na prístup k úradným dokumentom. Právo na ochranu osobných údajov rovnako zohráva veľmi významnú úlohu v oblasti zamestnania, kde je potrebné vybalansovať na jednej strane snahu zamestnávateľa čo najviac monitorovať svojho zamestnanca s právom zamestnanca na rešpektovanie jeho súkromného života a korešpondencie. S cieľom pomôcť vám správne nastaviť strety uvedených práv a objasniť mantinely prípustného zásahu do práva na ochranu osobných údajov, sme naše odporúčania doplnili o podrobne spracované najvýznamnejšie rozhodnutia, ktoré v tomto smere Súdny dvor EÚ a Európsky súd pre ľudské práva vydali.

Vzhľadom na skutočnosť, že počas finalizácie prác na 2. vydaní komentára sa na Slovensku rozšírila pandémia spôsobená koronavírusom SARS-CoV-2, ktorá má neočakávané dopady na život a spôsob fungovania každého z nás, rozhodli sme sa náš komentár doplniť ešte o **špeciálnu prílohu**, ktorej cieľom je vyjadriť náš názor na otázky, ktoré vás v tomto čase najviac zaujímajú a sú úzko prepojené s ochranou súkromia a spracúvaním osobných údajov. Do prílohy sme zahrnuli naše **stanovisko na meranie telesnej teploty zamestnanca a pravidlá pre prácu z domu**.

Z dôvodu rozsiahlosti aktualizácie sme 2. vydanie komentára rozdelili do dvoch zväzkov, a to pri zachovaní pôvodnej postupnosti článkov Nariadenia.

Prvý zväzok obsahuje komentár k všeobecným ustanoveniam a zásadám Nariadenia, ako aj k právam dotknutých osôb. Tieto dojednania a komentár k nim predstavujú základ pre správne a legálne nastavenie spracúvania osobných údajov. Nájdete tu predmet a ciele Nariadenia vrátane stručného prehľadu histórie ochrany osobných údajov a súvisiacej právnej úpravy, vymedzenie jeho

pôsobnosti – vecnej aj územnej, vysvetlenie vzťahu Nariadenia a slovenského zákona o ochrane osobných údajov, ďalej podrobne rozpracované zásady spracúvania, ktoré predstavujú základné pravidlá akéhokoľvek spracúvania osobných údajov, jednotlivé právne základy ako nevyhnutný predpoklad zákonnosti spracúvania, osobitné podmienky vyjadrenia súhlasu dotknutej osoby, spracúvanie osobitných kategórií osobných údajov, ako aj údajov týkajúcich sa uznania viny za trestné činy a priestupky a práva dotknutých osôb. Značnú časť prvého zväzku obsahuje komentár k právam dotknutých osôb (podmienky splnenia informačnej povinnosti, právo na prístup k údajom, právo na opravu, vymazanie, právo namietať, podmienky pre automatizované individuálne rozhodovanie vrátanie profilovania a iné) a k ich aplikácii v praxi prevádzkovateľov. Práve prvý zväzok obsahuje **množstvo praktických príkladov spracúvania osobných údajov**, ktoré slúžia ako názorná pomôcka aplikácie pravidiel Nariadenia. Súčasťou 1. zväzku je aj **špeciálna príloha súvisiaca s pandémiou**.

Druhý zväzok upravuje postavenie prevádzkovateľa, sprostredkovateľa a zodpovednej osoby, podmienky kladené Nariadením na zabezpečenie bezpečnosti spracúvania osobných údajov, okolnosti, za ktorých sa vyžaduje posúdenie vplyvu na ochranu osobných údajov (vrátane zoznamu všetkých zverejnených black listov a návrhov white listov), právnu úpravu kódexov správania a certifikácie, podmienky pre realizáciu prenosov osobných údajov do tretích krajín alebo medzinárodným organizáciám, postavenie a úlohy dozorných orgánov, zabezpečenie ich spolupráce a pravidiel konzistentnosti vrátane ukladania sankcií (s uvedením prehľadu sankcií dozorných orgánov členských štátov uložených podľa Nariadenia), prostriedky nápravy neoprávnených zásahov do práva na ochranu osobných údajov, a na záver podmienky stretu práva na ochranu súkromia s inými právami (teda s právom na slobodu prejavu a právom na informácie, právom na prístup verejnosti k úradným dokumentom, ďalej možnosti zásahu do povinnosti profesijnej mlčanlivosti, podmienky spracúvania rodného čísla, osobných údajov zamestnancov ich zamestnávateľmi vrátane rôznych foriem monitorovania, spracúvanie v oblasti archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu alebo štatistické účely, pravidlá ochrany údajov cirkví, spracúvanie osobných údajov v oblasti elektronických komunikácii, nastavenie cookies a iné). Druhý zväzok obsahuje rozsiahlu judikatúru Súdneho dvora EÚ a Európskeho súdu pre ľudské práva, vďaka ktorej sa čitateľ bude jasnejšie orientovať v problematike ochrany osobných údajov v osobitných situáciách zahrnutých v druhom zväzku komentára.

Komentár je rozdelený do dvoch zväzkov, ktoré uceleným spôsobom riešia problematiku v nich obsiahnutú. Vzhľadom na skutočnosť, že Nariadenie predstavuje jeden celok a v niektorých prípadoch nebolo možné vyhnúť sa previazanosti jednotlivých článkov, a tým aj zväzkov komentára, pre správne pochopenie problematiky odporúčame pracovať s oboma zväzkami.

Moja vďaka patrí všetkým spoluautorom, ktorí si pri svojich pracovných povinnostiach našli čas spracovať pre vás ďalšie zaujímavé informácie. Zároveň ma veľmi teší, že aj pri tomto vydaní sa podarilo zostaviť funkčný a spolupracujúci tím. Špeciálne poďakovanie patrí môjmu synovi Adamovi pre jeho pochopenie a podporu a pani Lucii Mikulovskej za jej ľudský prístup, čas a energiu, ktorú dielu pri jazykovej úprave venovala. Osobitné poďakovanie patrí našim rodinám, rodičom, manželom, manželkám, priateľom a deťom, ktorí nám boli pri tvorbe oporou.

Osobné údaje sa v dnešnej dobe stávajú čoraz častejším a vzácnejším platidlom. Preto vám všetkým na záver zo srdca želám, aby ste si sami stanovili ich hodnotu alebo pomohli túto hodnotu stanoviť aj tým, ktorým na vlastnom súkromí záleží.

Irena Hudecová, hlavná autorka

o autoroch

Mgr. Irena Hudecová

Štúdium na Právnickej fakulte v Bratislave dokončila v roku 2004. V roku 2003 úspešne absolvovala výberový európsky program organizovaný Erasmovou univerzitou v Rotterdame v spolupráci so 7 ďalšími európskymi univerzitami zameraný na problematiku EÚ z ekonomického a právneho hľadiska. V tom istom roku absolvovala niekoľkomesačnú stáž v Haagu v Medzinárodnom centre športového práva. V roku 2007 úspešne zložila advokátske skúšky. Irena sa špecializuje na problematiku ochrany osobných údajov. V tejto oblasti má niekoľkoročné skúsenosti, a to tak z pozície advokátky, ako aj kontrolórky Úradu na ochranu osobných údajov SR. Podieľala sa na príprave Nariadenia aj tvorbe nového zákona o ochrane osobných údajov. Zastupovala Úrad na ochranu osobných údajov SR na medzinárodných stretnutiach a pracovných zasadnutiach WP29. V roku 2017 sa ako členka kontrolného tímu vybraného Európskou komisiou zúčastnila medzinárodnej kontroly Schengenského informačného systému iného členského štátu EÚ. V tom istom roku na základe nominácie od Európskej komisie školila zástupcov Úradu na ochranu osobných údajov v Macedónsku, ako správne nastaviť skúšky pre zodpovednú osobu a overiť ich kvalifikáciu. V roku 2019 obhajovala stanovisko a postup Úradu na ochranu osobných údajov SR v prípadnom prvom spore úradu s iným dozorným orgánom pred Európskym výborom pre ochranu údajov. Irena pravidelne prednáša na odborných fórach a konferenciách.

Mgr. Anna Cyprichová

Vyštudovala Právnickú fakultu Univerzity Komenského v Bratislave (1998). Profesijnú kariéru začala v advokátskej kancelárii G. Lehnert, k. s., ako advokátsky koncipient (predtým komerčnoprávny čakateľ) a neskôr spolupracujúci advokát. V roku 2003 prešla do korporátnej sféry k významnému telekomunikačnému operátorovi na pozíciu senior právnika. V súčasnosti pôsobí ako advokátka spolupracujúca s advokátskou kanceláriou G. Lehnert, k. s. S manželom a troma deťmi býva v Bratislave.

Vo svojej profesijnej činnosti sa podieľala na poskytovaní komplexného právneho poradenstva pri mnohých významných projektoch a transakciách, najmä v oblasti nastavenia rôznych cloudových služieb a služieb spojených so spracúvaním osobných údajov veľkého množstva dotknutých osôb. Vo svojej praxi riešila tiež právne nastavenie dokumentácie a procesov spracúvania osobných údajov dotknutých osôb prevádzkovateľmi, ako aj úpravu zmluvných vzťahov medzi prevádzkovateľmi a sprostredkovateľmi vrátane cezhraničného spracúvania a prenosov do tretích krajín.

Ing. Ivan Makatura

Vyštudoval odbor aplikovaná informatika na Fakulte elektrotechniky a informatiky Technickej univerzity v Košiciach. Neskôr absolvoval postgraduálne štúdium na Znaleckom ústave elektrotechniky a informatiky Slovenskej technickej univerzity v Bratislave. Je držiteľom mnohých profesijných certifikácií v oblasti informačnej bezpečnosti a riadenia rizika. Kvalifikovaný bezpečnostný manažér s dlhoročnou praxou vo funkcii riaditeľa odboru bezpečnosti v bankách, v IT priemysle od roku 1993. V súčasnosti je generálnym riaditeľom Kompetenčného a certifikačného centra kybernetickej bezpečnosti. V minulosti bol vedúcim konzultantom IBM Security Services so zameraním na oblasť informačnej bezpečnosti a ochranu osobných údajov. Pracovne pôsobí aj ako súdny znalec v odvetví Bezpečnosť a ochrana informačných systémov a tiež ako certifikovaný audítor kybernetickej bezpečnosti. V role člena technickej komisie Úradu pre normalizáciu a metrológiu SR sa spolupodieľa na implementácii noriem ISO do sústavy Slovenských technických noriem. Je známym prednášajúcim na slovenských i medzinárodných konferenciách a vzdelávacích aktivitách, ako aj autorom mnohých článkov s témou informačnej bezpečnosti a ochrany osobných údajov. Pracuje aj ako predseda Asociácie kybernetickej bezpečnosti a člen rady ISACA Slovensko.

Ing. Beata Pčolová

Na Úrade na ochranu osobných údajov Slovenskej republiky pôsobí 14 rokov. V rámci problematiky osobných údajov sa venuje prešetrovaniu podozrení z porušovania zákona v konaniach o ochrane osobných údajov a nadväzne ukladaniu pokút za zistené porušenia zákona. V minulosti sa zúčastňovala výkonu kontrol spracúvania osobných údajov.

Mgr. Barbora Jarottová Bujňáková

Vyštudovala Právnickú fakultu Univerzity Komenského v Bratislave. Na Úrade na ochranu osobných údajov Slovenskej republiky pôsobí tretí rok ako zamestnankyňa Odboru správnych konaní, kde sa venuje predovšetkým konaniam o ochrane osobných údajov s cezhraničným prvkom a spolupráci medzi dozornými orgánmi. Tiež sa venuje problematike kódexov správania.

Mgr. Viliam Mizák

Problematike ochrany osobných údajov sa ako zamestnanec Úradu na ochranu osobných údajov SR venuje viac než 10 rokov, z toho 5 rokov v pozícii inšpektora úradu. V minulosti participoval na príprave súvisiacich všeobecne záväzných právnych predpisov, ktoré nadväzne aplikoval v praxi. Jeho skúsenosti získané v rámci kontrol zameraných na spracúvanie osobných údajov sa vzťahujú na rozsiahle spektrum informačných systémov a ich prevádzkovateľov.

JUDr. Juraj Mičura

Venuje sa problematike ochrany osobných údajov. Na Úrade na ochranu osobných údajov Slovenskej republiky pôsobí od roku 2013, pričom ako vedúci zamestnanec riadi prvostupňový správny orgán, v ktorého kompetencii je plnenie úloh najmä v oblasti konania o ochrane osobných údajov. Spolupodieľal sa na príprave nového zákona o ochrane osobných údajov.

Zoznam autorov...

Komentár k Nariadeniu Európskeho parlamentu a Rady (EÚ) 2016/679
spracoval autorský kolektív Mgr. Ireny Hudecovej:

Mgr. Irena Hudecová

články 1 – 3, článok 4 body 1 – 3, body 6 – 11, body 13 – 15, bod 17, bod 21, body 24 – 25, články 5 – 8, článok 9, články 10 – 11, články 13 –21, články 23 - 35, články 37 – 43, články 52 – 54, články 57 – 58, článok 60, článok 68, článok 74, články 82 -86, článok 95, článok 99

Mgr. Anna Cyprichová

článok 4 bod 4, bod 15, bod 16, body 18 – 23, bod 26, článok 3, článok 12, článok 22, článok 23, články 44 – 51, články 55 – 56, článok 59, články 63 – 67, články 69 – 81, článok 83, články 85 – 98

Ing. Ivan Makatura

článok 4 bod 5 a bod 12, články 24 – 25, články 32 – 36, článok 42

Ing. Beata Pčolová

článok 4 bod 1, články 12 – 14, článok 21, články 60 – 62

Mgr. Barbora Jarottová Bujňáková

článok 83

Mgr. Viliam Mizák

článok 9

JUDr. Juraj Mičura

článok 83

Judikatúru k jednotlivým článkom Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 spracovali Mgr. Irena Hudecová a Mgr. Anna Cyprichová.

Špeciálnu prílohu týkajúcu sa spracúvania osobných údajov v súvislosti s pandémiou spôsobenou koronavírusom pripravili Irena Hudecová, Anna Cyprichová a Ivan Makatura.

Prehľad použitých skratiek

Charta	Charta základných práv Európskej únie
ZFEÚ	Zmluva o fungovaní Európskej únie
Dohovor alebo EDĽP	Oznámenie č. 209/1992 Zb. Oznámenie Federálneho ministerstva zahraničných vecí o dojednaní Dohovoru o ochrane ľudských práv a základných slobôd a Protokolov na tento Dohovor nadväzujúcich (Dohovor o ochrane ľudských práv a základných slobôd zo 4. novembra 1950)
Dohovor 108	Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (Rady Európy)
Dohovor 108+	Modernizovaný Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (Rady Európy)
Listina práv a slobôd	Ústavný zákon č. 23/1991 Zb., ktorým sa uvádza Listina základných práv a slobôd
Ústava SR	Ústavný zákon č. 460/1992 Z. z. Ústava Slovenskej republiky v znení neskorších predpisov
Zákonník práce	Zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov
Smernica o ochrane osobných údajov	Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Ú. v. ES L 281, 23.11.1995, s. 31)
Nový zákon o ochrane osobných údajov	Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 221/2019 Z. z., ktorým sa mení a dopĺňa zákon č. 177/2018 Z. z. o niektorých opatreniach na znižovanie administratívnej záťaže využívaním informačných systémov verejnej správy a o zmene a doplnení niektorých zákonov (zákon proti byrokracii) a ktorým sa menia a dopĺňajú niektoré zákony
Zákon č. 122/2013 Z. z.	Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Vyhláška 164/2013	Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení v znení vyhlášky č. 117/2014 Z. z.
Zákon č. 428/2002 Z. z.	Zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov
Policajná smernica	Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 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 z 27. apríla 2016
Nariadenie č. 45/2001	Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi spoločenstva a o voľnom pohybe takýchto údajov (Ú. v. ES L 8, 12.1.2001, s. 1)
Nariadenie 2018/1725	Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES

Smernica 2000/31/ES	Smernica Európskeho parlamentu a Rady 2000/31/ES z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode) (Ú. v. ES L 178, 17. 7. 2000, s. 1)
Smernica 2002/58/ES	Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31. 7. 2002, s. 37) v znení neskorších zmien
Občiansky zákonník	Zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov
Obchodný zákonník	Zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov
Živnostenský zákon	Zákon č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov
Trestný zákon	Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov
Zákon o štátnej službe	Zákon č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov
Zákon o advokácii	Zákon o advokácii a o zmene a doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov
Dohoda o EHP	Dohoda o Európskom hospodárskom priestore
Zákon o súdoch	Zákon č. 757/2004 Z. z. o súdoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Správny poriadok	Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov
Zákon o slobodnom prístupe k informáciám	Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov
Správny súdny poriadok	Zákon č. 162/2015 Z. z. Správny súdny poriadok v znení neskorších predpisov
Civilný sporový poriadok	Zákon č. 160/2015 Z. z. Civilný sporový poriadok v znení neskorších predpisov
Zákon o ochrane utajovaných skutočností	Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Zákon o správnych poplatkoch	Zákon č. 145/1995 Z. z. o správnych poplatkoch v znení neskorších predpisov
Zákon o účtovníctve	Zákon č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov.
Zákon o dani z príjmov	Zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov.
Zákon o elektronických komunikáciách	Zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov
Školský zákon	Zákon č. 245/2008 Z. z. o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Úrad	Úrad na ochranu osobných údajov Slovenskej republiky
ESĽP	Európsky súd pre ľudské práva
SDEÚ/alebo Súdny dvor EÚ	Súdny dvor Európskej únie
OECD	Organizácia pre hospodársku spoluprácu a rozvoj

EHP	Európsky hospodársky priestor
Pracovná skupina WP29 WP29 Pracovná skupina	Pracovná skupina zriadená podľa čl. 29 Smernice o ochrane osobných údajov
Posúdenie vplyvu DPIA	Posúdenie vplyvu na ochranu údajov
Usmernenia WP29 týkajúce sa posúdenia vplyvu	Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“, prijaté 4. apríla 2017, v znení naposledy revidovanom a prijatom 4. októbra 2017, WP 248 rev. 01
Európsky výbor pre ochranu údajov Výbor EDPB	Európsky výbor pre ochranu údajov
Nariadenie o IMI	Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1024/2012 z 25. októbra 2012 o administratívnej spolupráci prostredníctvom informačného systému o vnútornom trhu a o zrušení rozhodnutia Komisie 2008/49/ES
Zmluvy	Zmluva o Európskej únii a Zmluva o fungovaní Európskej únie
Zákon o kybernetickej bezpečnosti	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 373/2018 Z. z., ktorým sa mení a dopĺňa zákon č. 371/2014 Z. z. o riešení krízových situácií na finančnom trhu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony
Zákon o bezpečnosti a ochrane zdravia pri práci	Zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Zákon o ochrane, podpore a rozvoji verejného zdravia	Zákon č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Stanovisko k transparentnosti	Stanovisko WP29 k transparentnosti (WP 260 rev. 01) prijaté dňa 29. novembra 2017, naposledy revidované a prijaté 11. apríla 2018
ECB	Európska centrálna banka
ECA	Európsky dvor audítorov
EUIPO	Úrad Európskej únie pre duševné vlastníctvo
EFSA	Európsky úrad pre bezpečnosť potravín
REA	Výkonná agentúra pre výskum
EACEA	Výkonná agentúra pre vzdelávanie, audiovizuálny sektor a kultúru
IMI	Informačný systém o vnútornom trhu
EZVO	Európske združenie voľného obchodu

Obsah

KAPITOLA IV
Prevádzkovateľ a sprostredkovateľ

Oddiel 1
Všeobecné povinnosti

Článok 24
Zodpovednosť prevádzkovateľa

1. S ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb prevádzkovateľ prijme vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie sa vykonáva v súlade s týmto nariadením. Uvedené opatrenia sa podľa potreby preskúmajú a aktualizujú.

2. Ak je to primerané vzhľadom na spracovateľské činnosti, opatrenia uvedené v odseku 1 zahŕňajú zavedenie primeraných politík ochrany údajov zo strany prevádzkovateľa.

3. Dodržiavanie schválených kódexov správania uvedených v článku 40 alebo schválených certifikačných mechanizmov uvedených v článku 42 sa môže použiť ako prvok na preukázanie splnenia povinností prevádzkovateľa.

Súvisiace ustanovenia: recitály 74, 75, 76, 77 a 83

Komentár k článku 24

Recitál 74: Mali by sa stanoviť povinnosti a zodpovednosť prevádzkovateľa v súvislosti s akýmkoľvek spracúvaním osobných údajov, ktoré vykonáva sám alebo ktoré sa vykonáva v jeho mene. Prevádzkovateľ by mal byť najmä povinný prijať primerané a účinné opatrenia a vedieť preukázať súlad spracovateľských činností s týmto nariadením vrátane účinnosti opatrení. V uvedených opatreniach by sa mala zohľadniť povaha, rozsah, kontext a účel spracúvania a riziko pre práva a slobody fyzických osôb.

Recitál 75: 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 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.

Recitál 76: 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.

Recitál 77: Usmernenie na vykonanie primeraných opatrení a preukázanie súladu prevádzkovateľom alebo sprostredkovateľom, najmä pokiaľ ide o identifikáciu rizika súvisiaceho so

spracúvaním, na jeho posúdenie so zreteľom na pôvod, povahu, pravdepodobnosť a závažnosť, a na identifikáciu najlepších postupov na zmiernenie rizika by mohlo byť poskytnuté najmä prostredníctvom schválených kódexov správania, schválenej certifikácie, usmernení vypracovaných výborom alebo pokynov poskytnutých zodpovednou osobou. Výbor môže vydať aj usmernenia pre spracovateľské operácie, v súvislosti s ktorými sa nepovažuje za pravdepodobné, že by viedli k vysokému riziku pre práva a slobody fyzických osôb, a uviesť, aké opatrenia môžu byť v takýchto prípadoch na vyriešenie takého rizika dostatočné.

Recitál 83: S cieľom zachovať bezpečnosť a predchádzať spracúvaniu v rozpore s týmto nariadením by prevádzkovateľ alebo sprostredkovateľ mali posúdiť riziká súvisiace so spracúvaním a prijať opatrenia na zmiernenie týchto rizík, ako napríklad šifrovanie. Týmito opatreniami by sa mala zaistiť primeraná úroveň bezpečnosti vrátane dôvernosti, pričom by sa mali zohľadniť najnovšie poznatky a náklady na vykonanie opatrení v súvislosti s rizikami a povahou osobných údajov, ktoré sa majú chrániť. Pri posudzovaní rizika v oblasti bezpečnosti údajov by sa mali zohľadniť riziká spojené so spracúvaním osobných údajov, ako sú napríklad náhodné alebo nezákonné zničenie, strata, zmena, neoprávnené poskytnutie prenášaných, uchovávaných alebo inak spracúvaných osobných údajov alebo neoprávnený prístup k nim, ktoré by mohli viesť k ujme na zdraví, majetkovej alebo nemajetkovej ujme.

Zodpovednosť je natoľko frekventovaným slovom, že azda ani niet takej oblasti ľudskej činnosti alebo sociálnej roly, kde by sa neodvolávalo na zodpovednosť. **Zodpovednosť** (angl. liability) má v práve oveľa užší význam ako v bežnom jazyku. Vo všeobecnosti sa pod výrazom zodpovednosť rozumie povinnosť starostlivosti o inú osobu alebo vec, prípadne starostlivosti o stav alebo o vzťah tak, aby nenastala ujma. Toto chápanie zodpovednosti je zodpovednosť v pôvodnom zmysle slova (angl. responsibility). Terajšie chápanie právnej zodpovednosti znamená najmä povinnosť niesť sankčné následky za vlastné konanie. Ak by neexistoval inštitút právnej zodpovednosti, nebolo by možné stanoviť, čo je to delikt, a teda ani stanoviť následnú sankciu za delikt. Bolo by zložité vymedziť povinnosť, t. j. nevyhnutnosť správať sa určitým spôsobom.

Regulácia je zvyčajne vykonávaná prostredníctvom právnych prepisov, ktoré stanovujú určité pravidlá správania sa subjektov práva. Vhodne nastavené pravidlá a ich efektívne vynucovanie majú smerovať k takému stavu na trhu, kedy sa dosiahne požadované správanie zúčastnených subjektov. V regulácii je preto práve snaha o dosiahnutie žiaduceho správania subjektov zrejmým zámerom stanovenia zodpovednosti.

Stanovenie objektívnej zodpovednosti prevádzkovateľa je cieľom článku 24 Nariadenia. Článok 24 stanovuje prevádzkovateľovi nasledujúce základné povinnosti:

- **prijať vhodné technické a organizačné opatrenia** (t. j. zaviesť ochranné procedúry a mechanizmy),
- prostredníctvom prijatých opatrení **zaistiť spracúvanie v súlade s Nariadením,**
- podľa potreby prijaté **opatrenia preskúmavať a aktualizovať** (t. j. prispôsobovať účinnosť opatrení priebežne sa vyvíjajúcim podmienkam spracovateľského prostredia).

Článok 24 upravuje aj:

- zavedenie **politiky ochrany údajov** (najmä ako integrálnu súčasť organizačných opatrení, avšak aj s cieľom zaistiť dokumentovanie prijatých technických a organizačných opatrení),
- **dodržiavať kódexy správania**, ak sa prevádzkovateľ zaviazal ich dodržiavať (uvedené v článku 40),
- **dodržiavať vydané certifikáty** (uvedené v článku 42), pokiaľ sa ich prevádzkovateľ rozhodol použiť ako prvok na preukázanie súladu s požiadavkami Nariadenia.

K ods. 1

Právna úprava povinnosti prevádzkovateľa prijať vhodné technické a organizačné opatrenia vychádza z jednej zo základných zásad spracúvania, a to konkrétne zo zásady integrity a dôvernosti, ktorá je odvodená zo základných atribútov bezpečnosti informácií, ktorými sú dôvernosť, celistvosť (integrita) a dostupnosť. Pri dodržaní týchto cieľov sú osobné údaje spracúvané takým spôsobom, ktorý zaručí primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením. Úprava zodpovednosti prevádzkovateľa za súlad s požiadavkami Nariadenia vychádza zo zásady zodpovednosti (článok 5 ods. 2). Cieľom tejto úpravy je zabezpečiť, aby prevádzkovatelia, ktorí majú skutočný vplyv na

spracúvanie osobných údajov, niesli za toto spracúvanie zodpovednosť spojenú s postihom v prípade porušenia svojich povinností vyplývajúcich z Nariadenia.

Nariadenie výslovne uvádza, že prevádzkovateľ je povinný prijať vhodné technické a organizačné opatrenia s ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb. Je teda povinný zohľadniť:

- povahu spracúvania (napr. či spracúvanie zahŕňa osobitné kategórie osobných údajov alebo osobné údaje týkajúce sa uznania viny za trestné činy a priestupky, spôsob použitia nových technológií, či zahŕňa automatizované individuálne rozhodovanie s právnymi účinkami vrátane profilovania),
- rozsah spracúvania (napr. počet dotknutých osôb, počet osobných údajov, počet kategórií osobných údajov, objem osobných údajov na regionálnej, vnútroštátnej alebo nadnárodnej úrovni),
- kontext spracúvania (vrátane právneho základu spracúvania, identity prevádzkovateľa, dobrovoľnosti alebo povinnosti poskytnúť osobné údaje, kategórií dotknutých osôb a pod.),
- účely spracúvania (napr. či sa v súvislosti s účelom spracúvania predpokladá dopad na dotknutú osobu alebo nie) a
- riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb (napr. diskriminácia, krádež totožnosti, finančná strata, ujma na zdraví, akékoľvek hospodárske alebo sociálne znevýhodnenie, bránenie dotknutej osobe využiť svoje právo a iné). Na vysvetlenie pojmu riziko pre práva a slobody fyzických osôb si Vás dovoľujeme odkázať na komentár k článku 32.

Ak je jednou zo základných povinností prevádzkovateľa prijať vhodné technické a organizačné opatrenia, je na začiatok nutné vysvetliť význam pojmu opatrenie, ktoré sa v kontexte Nariadenia na tomto mieste spomína po prvýkrát.

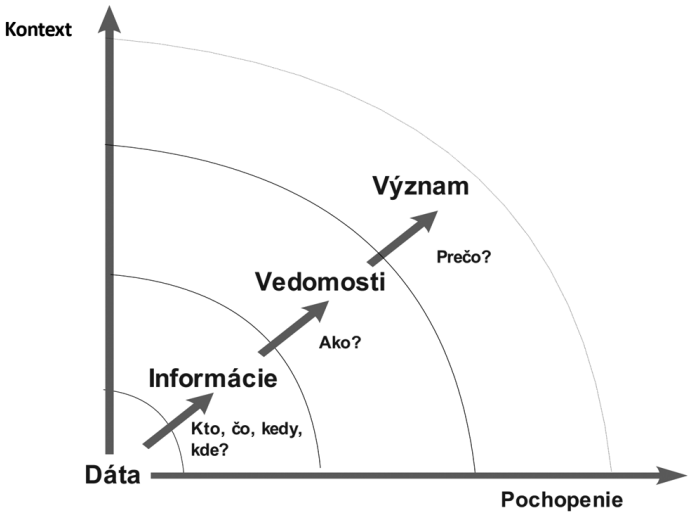
Slovo **„opatrenie“** je synonymom pre zákrok na dosiahnutie istého cieľa, výsledku a pod. Nariadenie pojednáva o ochrane osobných údajov. V odbornej oblasti ochrany citlivých informačných aktív (čo, samozrejme, osobné údaje sú) je cieľom, výsledkom dosiahnutie stavu, alebo priblíženie sa stavu, v ktorom je možné vyhlásiť, že osobné údaje sú chránené, teda že sú spracúvané bezpečným spôsobom.

Pojem **„bezpečnosť“** (z angl. „security“) pochádza z latinského securitas (sine cura + tutus). Tieto výrazy vo všeobecnosti znamenajú istotu, pokoj, ochranu, zabezpečenie, nespornosť. V každom význame týchto slov ide o stav, v ktorom sú chránené aktíva a objekty vo vlastníctve nejakého subjektu. Tento výraz môže byť vykladaný dynamicky alebo staticky – teda buď ako určitý momentálny stav, alebo naopak ako bežiaci proces, kontinuálne prebiehajúca spoločenská činnosť. Na výsledný stav môžeme nahliadať dvoma spôsobmi:

- objektívna bezpečnosť – daná skutočnou absenciou ohrozenia,
- subjektívna bezpečnosť – ako dôsledok absencie vnímania ohrozenia.

Slovo bezpečnosť je preto značne široký pojem, ktorému zvykne byť v rôznych oblastiach ľudskej činnosti pripisovaný rôzny význam. V prostredí hrozieb pôsobiacich na informačné aktíva má tento výraz svoj špecifický význam. Nech už ale vnímame bezpečnosť v kontexte ktorejkoľvek spoločenskej oblasti, máme na mysli určitý status bezpečnosti, t. j. **objektívne opísateľný stav relatívneho bezpečia pred hrozbami a rizikami.** V prípade Nariadenia je to stav relatívneho bezpečia pred hrozbami a rizikami, ktoré pôsobia na údaje, v tomto prípade osobné údaje. Na pochopenie toho, čo znamená bezpečnosť osobných údajov, je potrebné najprv vysvetliť pojmy „údaje“ (alebo tiež „dáta“, nemyslíme tým teraz osobné údaje) a „informácie“. Reprezentácia hierarchického vzťahu medzi dátami a informáciami je už mnoho rokov súčasťou teoretickej informatiky. Aj keď nie je úplne jasné, kedy a kým boli tieto vzťahy prvýkrát prezentované, hierarchia je zakotvená v použití skratky DIKW ako skráteného opisu vzťahu medzi dátami a informáciami a ich postupnej transformácie až k vedomostiam a pochopeniu ich významu. DIKW pyramída (alebo tiež informačná pyramída) je skratkou z anglických slov Data – Information – Knowledge – Wisdom (Dáta – Informácie – Vedomosti – Význam).

Schéma č. 1 Vzťah medzi dátami a informáciami



ÚDAJE sa stávajú informáciami až vtedy, ak nadobudnú určitý význam, zmysel a najmä hodnotu. Informácia je pochopením vzťahu medzi časťami dát. Hodnotu informácií určuje výhradne ich vlastník, teda ten subjekt, pre koho informácie nadobúdajú aktuálny alebo potenciálny význam. Táto zásada je mimoriadne dôležitá najmä v kontexte hodnotenia rizík, ktoré na tieto informácie pôsobia. Pokiaľ teda informácie sú dátami, ktoré nadobudli vlastníka, kontext a následne aj hodnotu, potom aj hodnotu rizika pôsobiaceho na informácie má správne určiť ich vlastník – teda subjekt, pre ktorý zníženie kvality, zničenie, odcudzenie alebo strata príslušných informácií znamená stratu tejto aktuálnej alebo potenciálnej hodnoty. Pojem „informačná bezpečnosť" znamená bezpečie týchto informácií, resp. zaručenie bezpečnosti týchto informácií. Rozdiel medzi pojmami „údaj" a „informácia" podčiarkuje aj názov, akým sú osobné údaje označované napr. v USA, tu sa totiž v správnom kontexte používa výraz „personally identifiable information" (identifikovateľné osobné informácie). Bezpečnosť informácií je stav, v ktorom sú informácie považované za bezpečné. Je to časť informačného manažmentu bez ohľadu na fyzikálny stav dát, bez ohľadu na ich formát, bez ohľadu na spôsob ich interpretácie a bez ohľadu na médium, prostredníctvom ktorého sú dáta uchovávané a prenášané. Z uvedeného dôvodu je pre informačnú bezpečnosť výstižnejšou a rovnako platnou definíciou manažment hrozieb a rizík, ktoré pôsobia na informačné aktíva. Alebo inými slovami – manažment hrozieb a rizík, ktoré pôsobia na údaje.

Opatrenia (z angl. „measures", alebo „controls") možno v spojitosti s ochranou osobných údajov chápať ako prostriedky, praktiky, procedúry a mechanizmy, ktoré je potrebné implementovať, dodržiavať, kontinuálne preverovať a v prípade potreby aktualizovať, to všetko s cieľom zabezpečiť primeranú úroveň ochrany osobných údajov. Bezpečnostné opatrenia je prevádzkovateľ aj sprostredkovateľ povinný prijať preto, aby chránil osobné údaje pred náhodným alebo úmyselným (v niektorých prípadoch i nezákonným) zničením, stratou, zmenou, neoprávneným poskytnutím alebo neoprávneným prístupom k nim. Tým sú nepriamo opísané základné atribúty informačnej bezpečnosti, dôvernosť, dostupnosť a integrita, ktoré sú v kontexte ochrany osobných údajov spomenuté v čl. 32 Nariadenia.

Bezpečnostné opatrenia môžu prevádzkovateľovi alebo sprostredkovateľovi pomôcť najmä chrániť pred určitou hrozbou, znížiť zraniteľnosť, obmedziť vplyv nechcenej udalosti, odhaliť malígnu udalosť alebo umožniť zotavenie alebo odškodnenie. Ich prijatím je napr. neoprávneným osobám znemožnený nedovolený prístup k osobným údajom, manipulácia s technickými zariadeniami určenými na spracovanie osobných údajov a manipulácia s nosičmi osobných údajov a naopak – oprávneným osobám je zaistený prístup k osobným údajom v rozsahu potrebnom na plnenie ich povinností.

Primárne sa bezpečnostné opatrenia rozdeľujú na **technické opatrenia** a **organizačné opatrenia**. Vzhľadom na svoje špecifiká sa niekedy z organizačných opatrení ešte ďalej vyčleňujú tzv. **personálne opatrenia** (napr. primeraná odborná príprava personálu, ktorý má stály alebo pravidelný prístup k osobným údajom v oblasti ochrany údajov), i keď Nariadenie tento pojem explicitne nepoužíva.

Technické opatrenia sú aktivity smerujúce ku zníženiu rizík pomocou nasadenia prostriedkov fyzickej a technologickej povahy, zatiaľ čo **organizačné opatrenia** sú aktivity smerované na zníženie operačných rizík pomocou zmien procesov a úpravou dokumentácie.

Aj Nariadenie správne uvádza, že opatrenia majú byť prijaté s ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb. Pre rozhodnutie o spôsobe ochrany je najprv potrebné zmapovať si informačné procesy. Tak ako v medicíne nie je možné bez diagnózy stanoviť spôsob liečby, v informačnej bezpečnosti nie je možné genericky stanoviť opatrenia bez poznania procesov (účelov spracúvania, kategórií osobných údajov, právnych základov a pod.), bez poznania jestvujúcej architektúry konkrétneho prostredia, bez znalosti spracovateľských operácií, bez znalosti klasifikácie dát a najmä – bez znalosti hrozieb a rizík. Preto vymenovanie príkladov technických a organizačných opatrení by nedávalo zmysel, pokiaľ by tieto neboli mapované na konkrétne ciele ochrany v kontexte konkrétnych spracovateľských operácií.

Nasledujúcu tabuľku predkladáme len ako hrubý príklad niektorých vybraných typov opatrení výhradne za účelom približného znázornenia niektorých z množstva dostupných možností ochrany osobných údajov. Implementácia akýchkoľvek opatrení a najmä ich účinnosť je samozrejme zásadným spôsobom závislá od posúdenia povahy, rozsahu, kontextu a účelov spracúvania, ako aj rizík s ich rôznou pravdepodobnosťou a rôznym potenciálnym dopadom (závažnosťou) pre práva a slobody fyzických osôb.

V nasledujúcej tabuľke sú v tejto publikácii po prvýkrát spomenuté oblasti bezpečnosti (tzv. bezpečnostné domény). Netreba si ich mýliť s opatreniami. Rozdelenie bezpečnostných domén súvisí predovšetkým s rozdelením špecializácií a zodpovedností v oblasti ochrany aktív, zatiaľ čo opatrenia súvisia s povahou reakcie na identifikované riziká.

Tabuľka č. 1: Príklady technických opatrení

Cieľ, ktorý má byť dosiahnutý	**Príklad opatrenia v oblasti**	
	Informačná bezpečnosť	**Fyzická bezpečnosť**
Privacy by Design (Špecificky navrhnutá ochrana údajov)	Bezpečný vývoj softvéru, postupy bezpečného obstarávania systémov, návrh procesov v súlade s požiadavkou PbD	–
Integrita a dôvernosť informácií	Sieťové firewally, segmentácia počítačovej siete, virtualizácia a vyhradenie spracovateľského prostredia (tzv. sandboxing)	
	Sledovanie siete, analýza správania, analýza anomálií	
Dôvernosť informácie	Mechanizmy kontroly práv a prístupov (tzv. manažment identít)	Elektronické zabezpečovacie systémy, systémy kontroly vstupov
	Použitie kryptografických riešení, najmä šifrovanie osobných údajov, pseudonymizácia osobných údajov	Bezpečnostné dvere, mreže, trezory, bezpečnostné skrine a pod. vrátane ich umiestnenia v zabezpečených priestoroch prevádzkovateľa
	Pseudonymizácia osobných údajov (iným spôsobom ako použitím kryptografických mechanizmov)	
Nepopierateľnosť informácie	Použitie kryptografických riešení, najmä digitálneho (elektronického) podpisu	Postupy na overenie vlastnoručného podpisu

Cieľ, ktorý má byť dosiahnutý	Príklad opatrenia v oblasti	
	Informačná bezpečnosť	Fyzická bezpečnosť
Integrita, dôvernosť a dostupnosť informácií	Ochrana proti malware, automatická analýza zraniteľnosti, zaznamenávanie udalostí v systémoch (logovanie)	Zaznamenávanie vstupu do chránených objektov, systémy kontroly vstupov
Vysoká dostupnosť informácií	Migrované sieťové úložiská dát	
Obnova dostupnosti informácií	Záložné kópie dát	Geograficky alebo metropolitne oddelené dátové centrá
Stála dostupnosť informácií (kontinuita)	Zdroje záložného elektrického napájania, prevádzkový monitoring	Požiarne poplachové systémy, dohľadové systémy

Tabuľka č. 2.: Príklady organizačných opatrení

Cieľ, ktorý má byť dosiahnutý	Príklad opatrenia
Dôvernosť informácií, Privacy by Default (štandardná ochrana údajov)	Poučenie o povinnostiach pri spracúvaní osobných údajov a zodpovednosti za ich porušenie
	Oddelenie právomocí (angl. Segregation of Duties), princíp komisionálnosti pri schvaľovaní transakcií
	Pravidlá výkonu kontroly vstupu do objektov a chránených priestorov, správa kľúčov, kľúčové režimy, vymedzenie fyzického perimetra objektov, určenie kategórií chránených priestorov a bezpečnostných úschovných objektov
	Vzdelávanie, zvyšovanie povedomia
	Určenie postupov likvidácie osobných údajov
	Pravidlá manipulácie s fyzickými nosičmi osobných údajov mimo chránených priestorov
	Pravidlá používania prenositeľných IT prostriedkov (napr. notebookov)
	Postupy pri údržbe alebo oprave IT prostriedkov
	Politika čistého stola
Integrita, dôvernosť a dostupnosť informácií	Postup pri ukončení pracovného pomeru (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušení zákonnej alebo zmluvnej povinnosti mlčanlivosti)
	Prideľovanie prístupových práv a úrovní prístupu (rolí) oprávnených osôb a správa hesiel
	Režim zastupovania oprávnených osôb
	Režim údržby a upratovania chránených priestorov
	Pravidlá mobilného spracovania a vzdialeného prístupu do technickej infraštruktúry prevádzkovateľa
Integrita a dostupnosť informácií	Vedenie zoznamu aktív a jeho aktualizácia, riadenie zmien
Oznámenie porušenia ochrany osobných údajov	Postup pri ohlasovaní a riešení bezpečnostných incidentov a zistených zraniteľností
	Organizácia tímu reakcie na bezpečnostné incidenty
Privacy by Design (Špecificky navrhnutá ochrana údajov)	Definovanie bezpečnostných požiadaviek v zmluvách
	Pravidlá pre bezpečný vývoj softvéru, pravidlá testovania systémov pred ich nasadením do produkcie
	Pravidlá výberu dodávateľov a audit služieb poskytovaných tretími stranami

Požiadavka, aby implementované opatrenia boli podľa potreby preskúmavané a aktualizované, vyplýva z princípu riadenia životného cyklu systémov, ktorý je uvedený v komentári k čl. 25.

K ods. 2

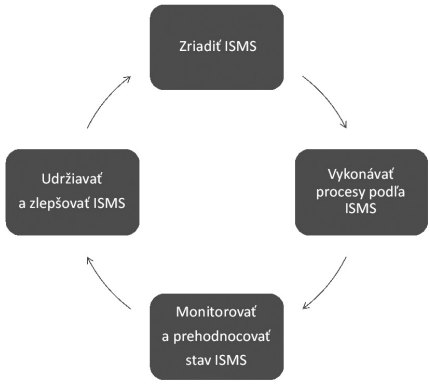
Bezpečnosť nie je konečný stav, ale iteratívny proces, na ktorý vplývajú mnohé okolnosti. Tento iteratívny prístup vyplýva z podstaty systému riadenia informačnej bezpečnosti, ktorý je založený na tzv. Demingovom cykle (skratkou „PDCA"). Systém PDCA predstavuje efektívny, univerzálny postup pre zlepšovanie kvality výrobkov, služieb a procesov. Zlepšovaním kvality sa zaoberal už v 50-tych rokoch americký fyzik a matematik W. E. Deming, dodnes sa udeľuje Demingova cena za kvalitu.

PDCA je skratka pozostávajúca zo 4 začiatočných písmen anglických slov:

- Plan – Plánuj
- Do – Vykonaj
- Check – Overuj (Kontroluj)
- Act – Konaj (Zlepšuj)

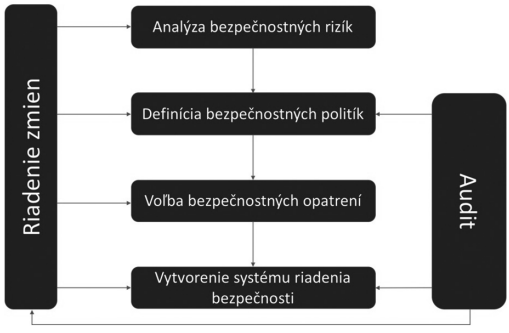
Nepretržitosť v uplatňovaní systému riadenia informačnej bezpečnosti (ISMS) je zrejmá z nasledujúcej schémy.

Schéma č. 2 Demingov cyklus v riadení informačnej bezpečnosti



Spôsob, akým prevádzkovateľ zaručí požadovanú úroveň bezpečnosti, je determinovaný rozhodnutím o primeranej množine bezpečnostných opatrení. Je však zrejmé, že primeranú úroveň bezpečnosti je možné efektívne dosiahnuť zásadne iba kombináciou technických a organizačných opatrení. Aj zo všeobecnej schémy procesu je zrejmé, že v informačnej bezpečnosti predchádza implementácii opatrení (myslené je technických opatrení) analýza rizík a návrh bezpečnostných politík.

Schéma č. 3 Generický proces informačnej bezpečnosti



Nariadenie vyžaduje, aby opatrenia zahŕňali aj zavedenie primeraných politík ochrany údajov, ak je to primerané vzhľadom na spracovateľské činnosti. Je úplne relevantné, ak Nariadenie požaduje, aby bola pred nasadzovaním opatrení opäť hodnotená primeranosť. Najmä vzhľadom na to, že spracovateľské prostredie sa priebežne mení a je možné očakávať, že medzi návrhom opatrení a ich implementáciou typicky ubehne určité obdobie. O tom, čo je primerané opatrenie a ako zvážiť „primeranosť" opatrení, píšeme v komentári k čl. 32.

Bezpečnostné politiky, t. j. bezpečnostná dokumentácia, sú typickou súčasťou organizačných opatrení. Pokiaľ sa má prevádzkovateľ zamyslieť nad tým, ako by mala byť navrhnutá vhodná štruktúra dokumentácie, je možné jej štruktúru rozdeliť na tri rôzne úrovne prispôsobené príslušnej úrovni riadenia:

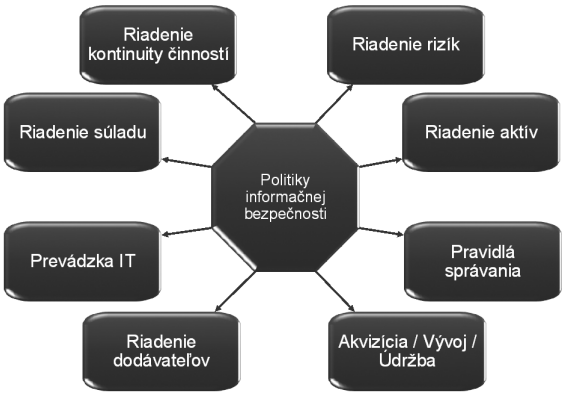
- strategické,
- taktické,
- operatívne.

Odporúčaný rámec bezpečnostnej dokumentácie podľa zaužívaných metodík

Úroveň riadenia	Typ dokumentu	Obsah
1. Strategická	Politika	**Politiky** určujú celkové smerovanie organizácie. Prostredníctvom politík sa stanovujú všeobecné požiadavky, zákazy a zásady správania sa v príslušnej oblasti bezpečnosti informácií.
2. Taktická	Štandard	**Štandardy** interpretujú politikami určené ciele a zásady už v konkrétnych situáciách. Stanovujú hlavné zodpovednosti, povinné aktivity, ako aj explicitné pravidlá, ktoré sú navrhnuté na podporu a vynútenie dodržiavania politík. Prostredníctvom štandardov sa zvyčajne prenášajú konkrétne politiky do praxe.
3. Operatívna	Procedúra	**Procedúry** implementujú podrobnosti o tom, ako dodržiavať politiky a štandardy. Procedúry sú súhrnom predpísaných krokov na vykonanie politík prostredníctvom konkrétneho súhrnu pracovných aktivít.
	Návod	**Návody** sú dodatočné (nepovinné) dokumenty na podporu politík, štandardov a procedúr. Sú to všeobecné usmernenia ku konkrétnym okolnostiam prostredníctvom odpovedí na otázky typu: „čo robiť“ a „ako to urobiť“. Medzi návody patrí aj technická dokumentácia a schémy IT architektúry.
	Konfigurácie	**Konfigurácie** (angl. baseline) sú pravidlá závislé od konkrétnej technickej platformy, typicky akceptované naprieč celým odvetvím. Konfigurácie poskytujú najefektívnejšie prístupy k špecifickej implementácii politík, opisujú nastavenia prostredia a spôsob jeho obsluhy vrátane opisu ovládacích prvkov a rozhraní.

Vyššie uvedený rámec bezpečnostnej dokumentácie je len odporúčaním v zmysle dobrej praxe, avšak pre niektoré špecifické subjekty, tzv. prevádzkovateľov základných služieb sa zákonom o kybernetickej bezpečnosti zavádza povinnosť udržiavať určitú štruktúru a obsah bezpečnostnej dokumentácie. Cieľom takto navrhnutej štruktúry je predovšetkým udržanie prehľadu o implementovaných organizačných opatreniach a zároveň schopnosť prevádzkovateľa reagovať na zmenné podmienky spracovateľského prostredia prípadnou zmenou príslušnej časti dokumentácie.

Schéma č. 4 Typická množina bezpečnostných politík



Príklad: Prevádzkovateľ, ktorý prevádzkuje množstvo informačných technológií s heterogénnou aplikačnou architektúrou, rozhodol o implementácii riešenia pre manažment identít (Identity & Access Management System, IAM) s cieľom zaistiť centrálne prideľovanie prístupov do všetkých prevádzkovaných systémov. Až po nasadení systému do produkčnej prevádzky si prevádzkovateľ uvedomil, že okrem systému IAM je zrejme potrebný aj vlastník tohto procesu, ktorý by bol primárne zodpovedný za rozhodovanie o úrovniach prístupových práv, o potrebe prístupov do systémov a napríklad aj o spôsobe overovania trvajúcej potreby prístupu do systémov. Takéto všeobecné rozhodnutie o procese a spôsobe riadenia procesu sa v organizáciách typicky vykonáva prostredníctvom bezpečnostných politík. V tomto prípade technické opatrenie (implementovaný systém IAM) nebolo sprevádzané príslušným organizačným opatrením. Výsledkom je, že opatrenia ako celok nemôžu byť pre dotknutú organizáciu efektívne.

Príklad z praxe: **Pokuta 500 000 GBP uložená spoločnosti DSG Retail Ltd.** po tom, čo sa spoločnosťou prevádzkovaná sieť POS terminálov stala cieľom kybernetického bezpečnostného incidentu. Podľa výsledkov analýzy útočník nainštaloval škodlivý kód na 5390 termináloch spoločnosti DSG v období od júla 2017 do apríla 2018 a následne pravdepodobne aj počas ďalšieho obdobia až do reálneho odhalenia útoku zhromažďoval osobné údaje. Zlyhanie spoločnosti v ochrane vlastných systémov pred známymi hrozbami umožnilo neoprávnený prístup k údajom o platobných kartách 5,6 milióna zákazníkov a k iným osobným údajom približne 14 miliónov zákazníkov vrátane celých mien, PSČ, e-mailových adries a záznamov o neúspešných autorizáciách transakcií. Ako dôvod incidentu boli po forenznej analýze identifikované nasledujúce nedostatky: neadekvátny proces nasadzovania softvérových záplat, nedostatočná segmentácia počítačovej siete a úplná absencia procesu rutinného hodnotenia technických zraniteľností.

V danom prípade je dostatočne preukázateľné, že v spoločnosti DSG Reatial Ltd. nebola uplatnená dobrá prax informačnej bezpečnosti a nebola splnená požiadavka článku 24 ods. 1 Nariadenia, podľa ktorého prevádzkovateľ prijme vhodné technické a organizačné opatrenia.

Príklad z praxe: **Pokuta 80 000 GBP uložená londýnskej realitnej agentúre Life at Parliament View Ltd.** za zverejnenie 18 610 záznamov s osobnými údajmi zákazníkov počas obdobia od marca 2015 do februára 2017.

Bezpečnostný incident nastal, keď spoločnosť migrovala databázu zo svojho servera ku dodávateľovi IT služieb, pričom po skončení migrácie neboli vypnuté niektoré štandardné funkcionality nového databázového systému, najmä možnosť anonymnej autentifikácie používateľa. Toto zlyhanie v konečnom dôsledku znamenalo, že nebolo správne nasadené riadenie prístupov, čo následne umožnilo komukoľvek získať plný prístup ku všetkým údajom uloženým v databáze. Kompromitované údaje zahŕňali výpisy z bankových účtov, mzdové údaje, kópie pasov, dátumy narodenia a adresy nájomcov a prenajímateľov.

Je možné konštatovať, že v danom prípade je dostatočne preukázateľné, že v spoločnosti nebola uplatnená dobrá prax informačnej bezpečnosti a nebola splnená požiadavka článku 24 ods. 1 Nariadenia, podľa ktorého prijaté technické a organizačné opatrenia sa podľa potreby preskúmajú a aktualizujú. Zároveň došlo k porušeniu zásady „privacy by default“ uvedenej v článku 25 ods 1. Nariadenia, podľa ktorej prevádzkovateľ aj v čase samotného spracúvania prijme primerané technické a organizačné opatrenia.

K ods. 3

Pre bližšie informácie ohľadom využívania schválených kódexov správania a vydaných certifikátov ako prvkov na preukázanie súladu pozri komentár k článku 40 a 42.

Článok 25

Špecificky navrhnutá a štandardná ochrana údajov

1. So zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie predstavuje pre práva a slobody fyzických osôb, prevádzkovateľ v čase určenia prostriedkov spracúvania aj v čase samotného spracúvania prijme primerané technické a organizačné opatrenia, ako je napríklad pseudonymizácia, ktoré sú určené na účinné zavedenie

zásad ochrany údajov, ako je minimalizácia údajov, a začlení do spracúvania nevyhnutné záruky s cieľom splniť požiadavky tohto nariadenia a chrániť práva dotknutých osôb.

2. Prevádzkovateľ vykoná primerané technické a organizačné opatrenia, aby zabezpečil, že štandardne sa spracúvajú len osobné údaje, ktoré sú nevyhnutné pre každý konkrétny účel spracúvania. Uvedená povinnosť sa vzťahuje na množstvo získaných osobných údajov, rozsah ich spracúvania, dobu ich uchovávania a ich dostupnosť. Konkrétne sa takýmito opatreniami zabezpečí, aby osobné údaje neboli bez zásahu fyzickej osoby štandardne prístupné neobmedzenému počtu fyzických osôb.

3. Schválený certifikačný mechanizmus podľa článku 42 sa môže použiť ako prvok na preukázanie súladu s požiadavkami uvedenými v odsekoch 1 a 2 tohto článku.

Súvisiace ustanovenia: recitál 78

Komentár k článku 25

Recitál 78: 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.

K ods. 1 a 2

Nariadenie v niekoľkých ustanoveniach zakotvuje povinnosť prevádzkovateľa prijať vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie sa vykonáva v súlade s Nariadením. Zatiaľ čo článok 24 rieši otázku voľby a následného prijatia bezpečnostných opatrení v nadväznosti na povahu, rozsah, kontext a účely spracúvania, ako aj riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, článok 25 upravuje, kedy má prevádzkovateľ tieto primerané technické a organizačné opatrenia implementovať. Cieľom čl. 25 je stanoviť, v ktorej časti životného cyklu informácie klasifikovanej ako „osobný údaj" je prevádzkovateľ povinný prijať tieto opatrenia.

Na pochopenie tohto článku je najprv nutné vysvetliť, čo je to **ŽIVOTNÝ CYKLUS INFORMÁCIE** alebo tiež **ŽIVOTNÝ CYKLUS VÝVOJA SYSTÉMOV.**

Každý pracovný proces predstavuje určitý **SYSTÉM,** v zmysle súhrnu aktivít a prvkov, medzi ktorými existujú isté vzťahy a ich usporiadania do organizovaného celku, resp. mechanizmu, metodiky, sústavy s koordinovanou činnosťou alebo sústavy ustálených úkonov.

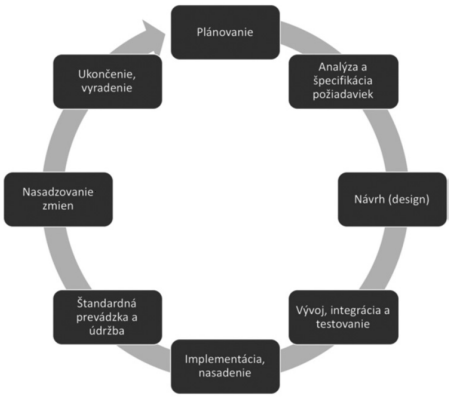
Vývoj a využívanie každého systému prechádza určitými etapami, ktoré sa pri jeho návrhu, nasadení, bežnom vykonávaní (prevádzke), zmenách, údržbe, rozvoji a inovácii cyklicky opakujú. Postupnosť týchto logicky na seba nadväzujúcich, opakujúcich sa vývojových etáp systémov sa nazýva **ŽIVOTNÝ CYKLUS.** Najčastejšie sú spomínané nasledujúce základné etapy životného cyklu systému, životného cyklu procesu alebo životného cyklu informácie:

- **Špecifikácie**, požiadavky a potreby vedúce k rozhodnutiu o vzniku (vytvorení informácie, spustení návrhu systému, resp. vybudovaní procesu);
- **Návrh** (design) budúceho procesu, systému, alebo dátovej štruktúry;

- **Vývoj** systému „na mieru“, integrácia, prípadne prispôsobenie jestvujúceho systému novým požiadavkám podľa návrhu a podľa špecifikácií;
- **Implementácia**, inštalácia, nasadenie, zavedenie alebo oživenie systému;
- **Výkon** procesu, štandardná prevádzka a údržba systému;
- **Zmeny** jestvujúceho, bežiaceho procesu (systému), rozvoj a inovácie podľa aktuálnych potrieb;
- **Nahradenie** systému novým v prípade zastaranosti, nesúladu alebo nízkej efektivity;
- **Ukončenie** procesu, vyradenie systému z prevádzky, dôveryhodné a úplné zničenie informácií.

Tento cyklický proces sa dá znázorniť aj graficky v postupnosti krokov.

Schéma č. 5 Životný cyklus procesu, systému, informácie



Na vysvetlenie požiadavky článku 25 je opätovne nutné zdôrazniť, že výraz „životný cyklus“ je v informačnom manažmente používaný ako v kontexte životného cyklu informácie, tak procesu, alebo aj systému. V softvérovom inžinierstve je na tento princíp zaužívaný pojem životný cyklus vývoja systémov (z anglického „Systems development life cycle“, so skratkou **„SDLC“**).

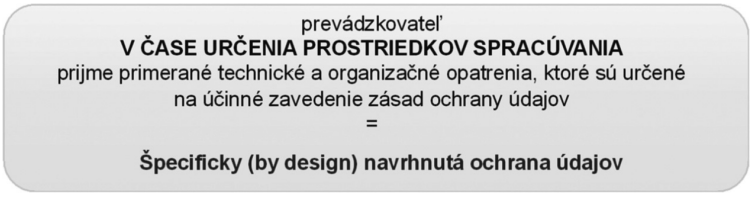
V súvislosti so zodpovednosťou prevádzkovateľa za súlad s Nariadením zakotvuje zákonodarca povinnosť prevádzkovateľa prijať špecificky navrhnutú ochranu údajov (angl. Privacy by design), ako aj štandardnú ochranu údajov (angl. Protection by default alebo Privacy by default). Požiadavka článku 25 nie je ničím iným, než požiadavkou na prijatie primeraných technických a organizačných opatrení, ktoré sú určené na účinné zavedenie zásad ochrany údajov v dvoch na seba nadväzujúcich fázach životného cyklu. Tými dvomi časťami sú:

- v čase určenia prostriedkov spracúvania,
- v čase samotného spracúvania.

K výkladu pojmu prostriedky spracúvania pozri komentár k článku 4 bod 2.

Súkromie **„BY DESIGN“** znamená špecificky zabudovať ochranu súkromia už v tej fáze životného cyklu, keď dochádza k návrhu aplikácie, procesu, činnosti alebo riadenia daného systému či obchodného procesu. Povinnosť prevádzkovateľa aplikovať špecificky navrhnutú ochranu údajov znamená špecificky zabudovať zásady spracúvania osobných údajov, a teda právo na ochranu osobných údajov v predstihu pred budúcim spracúvaním, a to už v návrhu aplikácie, služby a produktu, ktoré budú určené alebo založené na spracúvaní osobných údajov. Túto povinnosť má prevádzkovateľ v čase určovania prostriedkov spracúvania, t. j. v čase, keď ešte žiadne osobné údaje nespracúva, iba aplikáciu, službu alebo produkt práve navrhuje.

Schéma č. 6 Špecificky navrhnutá ochrana údajov



Recitál 78 správne uvádza, že zásady špecificky navrhnutej ochrany údajov a štandardnej ochrany údajov by sa mali zohľadniť aj v súvislosti s obstarávaním služieb a produktov. To znamená, že proces obstarania systému, aplikácie alebo produktu od tretej strany je nutné viesť takým spôsobom, aby keď začne proces spracúvania osobných údajov pomocou produktu alebo služby tretej strany, boli od prvej chvíle výkonu spracovateľskej činnosti zohľadnené požiadavky na ochranu práv dotknutých osôb. Táto požiadavka je aj súčasťou medzinárodných noriem v oblasti informačnej bezpečnosti.

Cieľom týchto povinností je zabezpečiť, aby prostriedky spracúvania osobných údajov boli vyvíjané alebo obstarané spôsobom, ktorý umožní budúcu ochranu osobných údajov, keďže v opačnom prípade by nebolo možné zabezpečiť aplikáciu zásad ochrany osobných údajov počas samotného spracúvania.

V praxi to znamená, že akékoľvek činnosti a kroky prevádzkovateľa, ktoré súvisia s ochranou osobných údajov (napr. interné projekty, vývoj produktov, vývoj softvéru, obstaranie systému alebo produktu), musia zohľadňovať ochranu osobných údajov už v štádiu samotnej prípravy danej činnosti, t. j. ešte pred jej zavedením či spustením. Projektový manažér, oddelenie IT musia v spolupráci s osobou zaoberajúcou sa problematikou osobných údajov (či už je to zodpovedná osoba alebo iný zamestnanec) zabezpečiť, aby boli zásady spracúvania implementované do každého návrhu v prvých fázach životného cyklu spracúvania.

Súkromie **„BY DEFAULT“** oproti súkromiu „by design“ znamená štandardne a trvalo udržateľným spôsobom vykonávať ochranu údajov vo všetkých obchodných procesoch a spracovateľských operáciách v čase samotného spracúvania. Je však potrebné zdôrazniť, že toto ustanovenie platí aj vo vzťahu k existujúcemu spracúvaniu, ktoré ku dňu uplatňovania Nariadenia prevádzkovateľ vykonáva, t. j. táto povinnosť sa teda vzťahuje na nové spracúvania, ako aj v deň začatia uplatňovania tohto Nariadenia existujúce spracúvania.

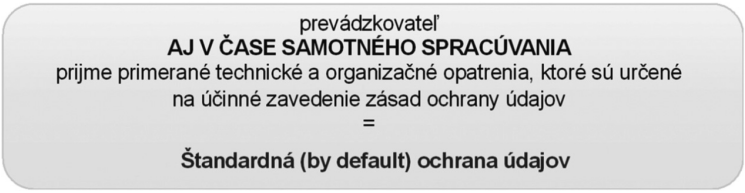
V rámci štandardnej ochrany osobných údajov je prevádzkovateľ povinný prijať primerané technické a organizačné opatrenia, aby zabezpečil, že v čase spracúvania osobných údajov sa štandardne spracúvajú len tie osobné údaje, ktoré sú nevyhnutné pre každý konkrétny účel spracúvania. Tieto bezpečnostné opatrenia musia zabezpečiť, že prevádzkovateľ získava iba osobné údaje nevyhnutné na dosiahnutie účelu spracúvania, osobné údaje sa spracúvajú iba v nevyhnutnom rozsahu, po dobu potrebnú na dosiahnutie účelu spracúvania a sú dostupné pre oprávneného používateľa a systém vo chvíli, keď je to potrebné a požadované.

Prečo je dôležité minimalizovať spracúvané osobné údaje? Okrem skutočnosti, že ide o základné povinnosti prevádzkovateľa vyplývajúce zo zásad spracúvania upravených v článku 5, predstavuje minimalizácia aj najlepšiu prax pri znižovaní rizika neoprávneného prístupu k osobným údajom a eliminácii ostatných bezpečnostných hrozieb. Pri získavaní osobných údajov by si prevádzkovateľ mal vždy položiť niekoľko základných otázok pre každý typ osobných údajov, ktorý plánuje spracúvať, najmä:

- Je dotknutá osoba informovaná o tom, ktoré osobné údaje o nej prevádzkovateľ získava a spracúva?
- Na aký účel a akým spôsobom plánuje prevádzkovateľ tieto osobné údaje spracúvať?
- Existuje spôsob, ako dosiahnuť príslušný účel aj bez toho, aby bolo nutné získavať osobné údaje?
- Je možné dosiahnuť príslušný účel aj s menším objemom osobných údajov, resp. s menším rozsahom atribútov osobných údajov?
- Na akú dobu bude potrebné uchovávať osobné údaje na dosiahnutie príslušného účelu spracúvania?

Odpoveď na tieto otázky umožní prevádzkovateľovi pochopiť, ktoré osobné údaje sú na dosiahnutie účelu potrebné a ktoré naopak nebudú potrebné v žiadnej etape životného cyklu spracúvania – a teda ktoré osobné údaje nepotrebuje získať a ktoré, ak už boli získané, je potrebné vymazať.

Schéma č. 7 Štandardná ochrana údajov



Prevádzkovateľ je povinný prijať také technické a organizačné opatrenia, ktoré sú účinné na zavedenie a udržateľnosť zásady:

- zákonnosti, spravodlivosti a transparentnosti,
- obmedzenia účelu,
- minimalizácie údajov,
- správnosti,
- minimalizácie uchovávania,
- integrity, dôvernosti a dostupnosti.

Vo vzťahu k špecificky navrhnutej ochrane údajov je prevádzkovateľ povinný prijať primerané technické a organizačné opatrenia, ktoré sú určené na účinné zavedenie zásad spracúvania osobných údajov. Pritom je povinný zohľadniť najnovšie poznatky, náklady na vykonanie opatrení, ako aj povahu spracúvania. Tieto poznatky musia zahŕňať napríklad:

- dostupnosť a spôsob použitia nových technológií,
- možné uplatnenie alebo naopak vyhnutie sa výlučne automatizovanému rozhodovaniu s právnymi účinkami vrátane profilovania,
- či je spracúvanie vykonávané aj neautomatizovanými prostriedkami,
- rozsah spracúvania (napr. počet dotknutých osôb, počet osobných údajov, počet kategórií osobných údajov, objem osobných údajov na regionálnej, vnútroštátnej alebo nadnárodnej úrovni),
- kontext spracúvania (vrátane právneho základu spracúvania, identity prevádzkovateľa, dobrovoľnosti alebo povinnosti poskytnúť osobné údaje, kategórií dotknutých osôb a pod.),
- účely spracúvania (napr. či sa v súvislosti s účelom spracúvania predpokladá dopad na dotknutú osobu alebo nie) a riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb (napr. diskriminácia, krádež totožnosti, finančná strata, ujma na zdraví, akékoľvek hospodárske alebo sociálne znevýhodnenie, bránenie dotknutej osobe využiť svoje právo a iné...).

Recitál 78 stanovuje, že bezpečnostné opatrenia by mali okrem iného pozostávať z minimalizácie spracúvania osobných údajov, podľa možnosti aj zo 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.

V tejto súvislosti myslí Nariadenie nielen na prevádzkovateľov, ale aj dodávateľov produktov, služieb a aplikácií a vyzýva ich, aby pri vypracovaní, navrhovaní, výbere a používaní aplikácií, služieb a produktov, ktoré sú založené na spracúvaní osobných údajov alebo spracúvajú osobné údaje, zohľadnili právo na ochranu údajov, aby prevádzkovatelia a sprostredkovatelia mohli plniť svoje povinnosti týkajúce sa ochrany údajov.

V rámci štandardnej ochrany osobných údajov je prevádzkovateľ povinný prijať primerané technické a organizačné opatrenia, aby zabezpečil, že v čase spracúvania osobných údajov sa spracúvajú len tie osobné údaje, ktoré sú nevyhnutné pre konkrétny účel spracúvania. Tieto bezpečnostné opatrenia zabezpečia, že prevádzkovateľ získava iba osobné údaje nevyhnutné na dosiahnutie účelu spracúvania, osobné údaje sa spracúvajú iba v nevyhnutnom rozsahu, po dobu potrebnú na dosiahnutie účelu spracúvania a sú dostupné pre oprávneného používateľa a systém vo chvíli, keď je to potrebné a požadované.

Ak vyššie uvedené ciele aplikujeme na životný cyklus informácie, procesu alebo systému, znamená to, že zabudovanie ochrany súkromia **V ČASE URČENIA PROSTRIEDKOV SPRACÚVANIA** je aplikácia princípov informačnej bezpečnosti vo fázach: Plánovanie – Analýza a špecifikácia požiadaviek – Návrh (design) – Vývoj podľa špecifikácií – Integrácia a testovanie – Implementácia, nasadenie a **V ČASE SAMOTNÉHO SPRACÚVANIA** je aplikácia princípov informačnej bezpečnosti vo fázach: Štandardná prevádzka a údržba – Nasadzovanie zmien – Ukončenie a vyradenie.

V grafickom znázornení by sa táto požiadavka dala vyjadriť nasledujúcim spôsobom:

Schéma č. 8 Špecificky navrhnutá a štandardná ochrana údajov z pohľadu životného cyklu

K ods. 3

Jedným z prvkov preukázania splnenia povinnosti uplatňovať špecificky navrhnutú aj štandardnú ochranu osobných údajov je certifikát podľa článku 42.

Článok 26

Spoloční prevádzkovatelia

1. Ak dvaja alebo viacerí prevádzkovatelia spoločne určia účely a prostriedky spracúvania, sú spoločnými prevádzkovateľmi. Transparentne určia svoje príslušné zodpovednosti za plnenie povinností podľa tohto nariadenia, najmä pokiaľ ide o vykonávanie práv dotknutej osoby, a svoje povinnosti poskytovať informácie uvedené v článkoch 13 a 14, a to formou vzájomnej dohody, pokiaľ nie sú príslušné zodpovednosti prevádzkovateľov určené právom Únie alebo právom členskému štátu, ktorému prevádzkovatelia podliehajú. V dohode sa môže určiť kontaktné miesto pre dotknuté osoby.

2. V dohode uvedenej v odseku 1 sa náležite zohľadnia príslušné úlohy spoločných prevádzkovateľov a ich vzťahy voči dotknutým osobám. Základné časti dohody sa poskytnú dotknutým osobám.

3. Bez ohľadu na podmienky dohody uvedenej v odseku 1 môže dotknutá osoba uplatniť svoje práva podľa tohto nariadenia u každého prevádzkovateľa a voči každému prevádzkovateľovi.

Súvisiace ustanovenia: recitál 79, článok 4 bod 7, článok 82

Komentár k článku 26

Recitál 79: Ochrana práv a slobôd dotknutých osôb, ako aj povinnosti a zodpovednosť prevádzkovateľov a sprostredkovateľov, a to aj v súvislosti s monitorovaním zo strany dozorných orgánov a ich opatreniami, si vyžaduje jasné rozdelenie povinností podľa tohto nariadenia vrátane prípadov, v ktorých prevádzkovateľ určuje účely a prostriedky spracúvania spoločne s inými prevádzkovateľmi, alebo v prípadoch, v ktorých sa spracovateľská operácia vykonáva v mene prevádzkovateľa.

K ods. 1 a 2

Nariadenie upravuje situáciu, keď účely a prostriedky spracúvania určia dvaja alebo viacerí prevádzkovatelia. V takom prípade hovoríme o spoločných prevádzkovateľoch. Hoci tento pojem Smernica o ochrane osobných údajov ani zákon č. 122/2013 Z. z. nepoznal, obidva uvedené predpisy takúto situáciu predpokladali, keďže prevádzkovateľa definovali ako subjekt, ktorý sám alebo **spoločne s inými určí účel a prostriedky spracúvania** osobných údajov. V tomto smere teda nejde o novinku, ale o doplnenie pravidiel týkajúcich sa spracúvania vykonávaného viacerými prevádzkovateľmi.

Pre posúdenie, či viaceré subjekty vystupujú v postavení spoločných prevádzkovateľov, je rozhodujúce, či spoločne určili účel a prostriedky spracúvania, bez ohľadu na to, v akom rozsahu sa na určení každý z nich podieľal. Ak má nejaký subjekt objektívny vplyv na spracúvanie osobných údajov, ak sa podieľal na určení účelu a prostriedkov spracúvania, považuje sa za prevádzkovateľa, bez ohľadu na to, či to zmluva určuje alebo nie. Pod účelom spracúvania osobných údajov rozumieme konkrétny dôvod, prečo sa osobné údaje spracúvajú. Vyplýva buď zo slobodného rozhodnutia spoločných prevádzkovateľov, alebo z právneho predpisu Únie či členského štátu. Účel spracovania musí byť v súlade so zásadou obmedzenia účelu konkrétne určený, výslovne uvedený, legitímny a v prípade ďalšieho spracúvania zlučiteľný s pôvodným účelom spracúvania (bližšie k účelu pozri komentár k článku 5 ods. 1 písm. b). Určenie prostriedkov spracúvania osobných údajov nám pomáha odpovedať na otázku, ako stanovený účel dosiahneme. Pojem prostriedky spracúvania osobných údajov je veľmi široký a zahŕňa všetky technické aj organizačné prostriedky, ktoré prevádzkovatelia pri spracúvaní osobných údajov použijú (napr. hardvér, softvér, ktorý sa na spracúvanie použije, listinná kartotéka a pod.). Nie je pritom potrebné, aby mali prevádzkovatelia tieto prostriedky vo svojom vlastníctve (napr. kamery, softvér) alebo v držbe. K pojmu spoločný prevádzkovateľ pozri bližšie komentár k článku 4 bod 7 a rozsudok Súdneho dvora EÚ vo veci Tietosuojavaltuutettu uvedený v časti judikatúra k čl. 4. Spoloční prevádzkovatelia môžu spracúvať osobne údaje súčasne alebo aj po sebe vo viacerých fázach. Na spoločných prevádzkovateľov sa vzťahujú ustanovenia Nariadenia týkajúce sa prevádzkovateľa.

Existencia spoločných prevádzkovateľov môže vyplývať buď z ich slobodného rozhodnutia, alebo z práva Únie či členského štátu, ktorému prevádzkovatelia podliehajú. V takom prípade môže toto právo určiť aj prostriedky spracúvania. Najdôležitejšie je zabezpečiť, aby boli všetky práva, povinnosti a zodpovednosť spoločných prevádzkovateľov za ich plnenie jasne a transparentne určené, a to najmä pokiaľ ide o povinnosť poskytnúť dotknutým osobám informácie podľa článku 13 a 14 (ak sa na nich nevzťahuje výnimka z tejto povinnosti podľa článku 13 ods. 4 alebo 14 ods. 5 alebo obmedzenie prijaté v súlade s čl. 23) a povinnosti vyplývajúce zo žiadosti dotknutej osoby uplatňujúcej si svoje práva (právo na prístup, právo na opravu, právo na vymazanie, právo na obmedzenie spracúvania, právo na prenosnosť, právo namietať, právo týkajúce sa automatizovaného individuálneho rozhodovania vrátane profilovania podľa článku 22). V prípade, ak nie sú príslušné zodpovednosti spoločných prevádzkovateľov určené právom Únie alebo právom členského štátu, ktorému prevádzkovatelia podliehajú, sú spoloční prevádzkovatelia povinní uzatvoriť dohodu, v ktorej si upravia svoj vzájomný vzťah, t. j. v ktorej si transparentne medzi sebou rozdelia povinnosti vyplývajúce z Nariadenia a s tým súvisiacu zodpovednosť za ich plnenie. Nariadenie síce nevyžaduje písomnú formu dohody, ale vzhľadom na zásadu zodpovednosti, ako aj presné rozdelenie zodpovednosti za porušenie povinností spojené s prípadnou náhradou škody spôsobenej dotknutej osobe odporúčame dohodu písomne zdokumentovať. Existencia spoločnej zodpovednosti neznamená nevyhnutne rovnakú zodpovednosť spoločných prevádzkovateľov za to isté spracovanie osobných údajov. Spoloční prevádzkovatelia môžu byť, naopak, zapojení do tohto spracovania v rôznych fázach a stupňoch, takže mieru zodpovednosti každého z nich treba hodnotiť z hľadiska všetkých relevantných okolností konkrétnej veci. Okrem toho spoluzodpovednosť viacerých subjektov za to isté spracovanie nepredpokladá, aby mal každý z nich prístup k dotknutým osobným údajom.[359)]

V súlade so zásadou transparentnosti sú základné časti dohody, t. j. identifikáciu spoločných prevádzkovateľov a rozdelenie povinností a zodpovednosti za ich plnenie, spoloční prevádzkovatelia povinní poskytnúť dotknutým osobám, a to v stručnej, ľahko dostupnej a ľahko pochopiteľnej forme. V tomto smere odporúčame, aby dohoda prehľadným spôsobom určovala, ktorý prevádzkovateľ zodpovedá za vybavenie žiadosti dotknutej osoby uplatňujúcej si konkrétne právo dotknutej osoby, napr. právo na prenosnosť údajov. Dohoda môže určiť aj kontaktné miesto pre dotknuté osoby. V prípade, 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, sú spoloční prevádzkovatelia povinní vykonať pred spracúvaním posúdenie vplyvu na ochranu osobných údajov, ktoré by malo obsahovať určenie, ktorý prevádzkovateľ je zodpovedný za prijatie konkrétneho bezpečnostného opatrenia.

359) Rozsudok Súdneho dvora EÚ z 10. júla 2018 vo veci C-25/17, Tietosuojavaltuutettu.

Na to, aby mohli spoloční prevádzkovatelia využívať zásadu jednotného kontaktného miesta, mali by určiť, ktorá prevádzkareň spoločných prevádzkovateľov bude mať právomoc presadzovať vykonanie rozhodnutí o účeloch a prostriedkoch spracúvania vo vzťahu ku všetkým spoločným prevádzkovateľom. Táto prevádzkareň sa potom bude považovať za hlavnú prevádzkareň. Určenie hlavnej prevádzkarne môže byť súčasťou vyššie spomínanej dohody spoločných prevádzkovateľov.

Vo veci Fashion ID[360)] Súdny dvor EÚ konštatoval, že fyzickú alebo právnickú osobu, ktorá ovplyvňuje na svoje vlastné účely spracovanie osobných údajov a v dôsledku toho sa podieľa na určovaní účelov a prostriedkov tohto spracovania, možno považovať za prevádzkovateľa. Spoluzodpovednosť viacerých subjektov za to isté spracovanie nepredpokladá, aby mal každý z nich prístup k dotknutým osobným údajom. Cieľom širokej definície pojmu „prevádzkovateľ" je zaručiť účinnú a úplnú ochranu dotknutých osôb, existencia spoločnej zodpovednosti však neznamená nevyhnutne rovnakú zodpovednosť rôznych subjektov za to isté spracovanie osobných údajov. Fyzická alebo právnická osoba môže byť prevádzkovateľom v spojení s inými osobami len za tie operácie spracovania osobných údajov, pri ktorých spoločne určuje účely a prostriedky spracovania. Naproti tomu a bez toho, aby bola v tejto súvislosti dotknutá prípadná občianskoprávna zodpovednosť stanovená vnútroštátnym právom, nemožno uvedenú fyzickú alebo právnickú osobu považovať za prevádzkovateľa za predchádzajúce alebo neskoršie operácie v postupe spracovania, pri ktorých neurčuje účely ani prostriedky. Súdny dvor EÚ v predmetnej veci konštatoval, že správcu internetovej stránky, ktorý umiestni na svojej stránke modul sociálnej siete umožňujúci prehliadaču návštevníka tejto stránky vyžiadať si obsah od dodávateľa uvedeného modulu a na tento účel prenesie tomuto dodávateľovi osobné údaje návštevníka, možno považovať za prevádzkovateľa. Táto zodpovednosť prevádzkovateľa je však obmedzená na operáciu alebo všetky operácie spracovania osobných údajov, pri ktorých skutočne určuje účely a prostriedky, t. j. operácie zberu a prenosu predmetných údajov.

K ods. 3

Bez ohľadu na to, ako si spoloční prevádzkovatelia v dohode rozdelili medzi sebou povinnosti vyplývajúce z Nariadenia (napr. kto je povinný osobné údaje opraviť, kto preniesť a pod.), dotknutá osoba môže uplatniť všetky svoje práva u každého prevádzkovateľa alebo akékoľvek svoje právo voči ktorémukoľvek prevádzkovateľovi. Dotknutá osoba teda nie je pri výkone svojich práv viazaná ani obmedzovaná dohodou spoločných prevádzkovateľov. Zákonodarca výslovne uvádza, že v prípade, ak sa na tom istom spracúvaní zúčastní viac ako jeden prevádzkovateľ a sú podľa článku 82 ods. 2 a 3 zodpovední za škodu spôsobenú spracúvaním, každý z nich zodpovedá za celú škodu, aby sa dotknutej osobe zabezpečila celá náhrada. Ak niektorý zo spoločných prevádzkovateľov zaplatil dotknutej osobe náhradu spôsobenej škody v plnej výške, má právo žiadať ostatných spoločných prevádzkovateľov zapojených do toho istého spracúvania tú časť náhrady škody, ktorá zodpovedá ich podielu zodpovednosti za škodu (k práve na náhradu škody pozri komentár k článku 82).

Dve alebo viac dcérskych spoločností sa rozhodnú vytvoriť spoločnú internetovú platformu s cieľom zefektívniť logistiku doručovania zásielok klientom dcérskych spoločností. Dohodnú sa na účele spracúvania osobných údajov, ako aj na prostriedkoch, ktoré sa majú použiť. V takomto prípade budú spoločnými prevádzkovateľmi v súvislosti so spracúvaním vykonávaným na dohodnutý účel prostredníctvom spoločnej internetovej logistickej platformy.

Cestovná agentúra, hotelový reťazec a letecká spoločnosť sa rozhodnú vytvoriť spoločnú internetovú platformu s cieľom zlepšiť svoju spoluprácu pri manažmente cestovných rezervácií. Dohodnú sa na dôležitých prvkoch prostriedkov, ktoré sa majú použiť, napríklad, aké údaje sa majú ukladať, ako sa budú prideľovať a potvrdzovať rezervácie a kto bude mať prístup k uloženým informáciám. Navyše sa rozhodnú spoločne využívať údaje o svojich zákazníkoch s cieľom vykonávať integrované marketingové akcie. V tomto prípade cestovná agentúra, letecká spoločnosť a hotelový reťazec budú mať spoločnú kontrolu nad spôsobom spracovania osobných údajov vlastných zákazníkov, a preto budú spoločnými prevádzkovateľmi v súvislosti s operáciami spracúvania týkajúcimi sa spoločnej internetovej rezervačnej platformy. Každý z nich si však zachová výlučnú kontrolu nad ostatnými činnosťami spracovania, napríklad činnosťami súvisiacimi s riadením ľudských zdrojov.[361)]

Inú situáciu predstavuje príklad, ak cestovná agentúra posiela osobné údaje svojich zákazníkov leteckej spoločnosti a hotelovému reťazcu s cieľom rezervácie miest v rámci cestovného balíka. Letecká spoločnosť a hotel potvrdia požadované voľné

360) Rozsudok Súdneho dvora EÚ z 29. júla 2019 vo veci C-40/17 Fashion ID GmbH & Co. KG proti Verbraucherzentrale NRW eV.

361) Usmernenie WP29 k pojmom „prevádzkovateľ" a „sprostredkovateľ" (WP 169) prijaté 16. februára 2010.

miesta a izby. Cestovná agentúra vystaví svojim zákazníkom cestovné dokumenty a poukážky. V tomto prípade sú cestovná agentúra, letecká spoločnosť a hotel traja rôzni prevádzkovatelia a všetci traja samostatne podliehajú povinnostiam ochrany údajov v súvislosti s vlastným spracovaním osobných údajov.[362)]

Spoločnými prevádzkovateľmi môžu byť aj advokáti, ak poskytujú právne služby v združení podľa § 13 zákona o advokácii.

Z judikatúry:

Rozsudok Súdneho dvora EÚ z 10. júla 2018 vo veci C-25/17, Tietosuojavaltuutettu (poznámka autorov: pre skutkové okolnosti prejednávanej veci pozri rozsudok v časti judikatúra k článku 4; rozsudok je podrobne spracovaný aj v judikatúre k čl. 91 Nariadenia)

66 Keďže cieľom tohto ustanovenia je prostredníctvom extenzívnej definície pojmu „prevádzkovateľ" zaručiť účinnú a úplnú ochranu dotknutých osôb, existencia spoločnej zodpovednosti neznamená nevyhnutne rovnakú zodpovednosť rôznych subjektov za to isté spracovanie osobných údajov. Tieto subjekty môžu byť naopak zapojené do tohto spracovania v rôznych fázach a stupňoch, takže mieru zodpovednosti každého z nich treba hodnotiť z hľadiska všetkých relevantných okolností prejednávanej veci (pozri v tomto zmysle rozsudok z 5. júna 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, body 28, 43 a 44).

69 Okrem toho spoluzodpovednosť viacerých subjektov za to isté spracovanie podľa tohto ustanovenia nepredpokladá, aby mal každý z nich prístup k dotknutým osobným údajom (pozri v tomto zmysle rozsudok z 5. júna 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, bod 38).

Rozsudok Súdneho dvora EÚ z 29. júla 2019 vo veci C-40/17 Fashion ID GmbH & Co. KG proti Verbraucherzentrale NRW eV (rozsudok je podrobne spracovaný v judikatúre k čl. 4 Nariadenia)

Článok 27

Zástupcovia prevádzkovateľov alebo sprostredkovateľov, ktorí nie sú usadení v Únii

1. Ak sa uplatňuje článok 3 ods. 2, prevádzkovateľ alebo sprostredkovateľ písomne určí zástupcu v Únii.

2. Povinnosť stanovená v odseku 1 tohto článku sa nevzťahuje na:

a) spracúvanie, ktoré je občasné, nezahŕňa vo veľkom rozsahu spracúvanie osobitných kategórií osobných údajov podľa článku 9 ods. 1 alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky podľa článku 10, a nie je pravdepodobné, že povedie k riziku pre práva a slobody fyzických osôb, pričom sa zohľadní povaha, kontext, rozsah a účely spracúvania, alebo

b) orgán verejnej moci či verejnoprávny subjekt.

3. Zástupca musí byť usadený v jednom z tých členských štátov, v ktorých sa nachádzajú dotknuté osoby, ktorých osobné údaje sa spracúvajú v súvislosti s ponukou tovaru alebo služieb pre nich, alebo ktorých správanie sa sleduje.

4. Prevádzkovateľ alebo sprostredkovateľ poverí zástupcu, aby sa naňho popri prevádzkovateľovi alebo sprostredkovateľovi alebo namiesto prevádzkovateľa alebo sprostredkovateľa obracali najmä dozorné orgány a dotknuté osoby, a to vo všetkých otázkach týkajúcich sa spracúvania na účely zabezpečenia súladu s týmto nariadením.

5. Určením zástupcu prevádzkovateľom alebo sprostredkovateľom nie sú dotknuté právne prostriedky nápravy, ktoré by sa mohli iniciovať proti samotnému prevádzkovateľovi alebo sprostredkovateľovi.

Súvisiace ustanovenia: recitály 75, 80, článok 3 ods. 2, článok 4 bod 17

Komentár k článku 27

Recitál 75: 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

362) Usmernenie WP29 k pojmom „prevádzkovateľ" a „sprostredkovateľ" (WP 169) prijaté 16. februára 2010.

údajov chránených profesijným tajomstvom, neoprávnenej reverznej pseudonymizácii alebo akémukoľvek inému závažnému hospodárskemu alebo sociálnemu znevýhodneniu; ak by dotknuté osoby mohli 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.

Recitál 80: Ak prevádzkovateľ alebo sprostredkovateľ, ktorý nie je usadený v Únii, spracúva osobné údaje dotknutých osôb, ktoré sa nachádzajú v Únii, pričom jeho spracovateľské činnosti súvisia s ponukou tovaru alebo služieb takýmto dotknutým osobám v Únii, bez ohľadu na to, či sa od dotknutej osoby vyžaduje platba, alebo so sledovaním ich správania sa, pokiaľ sa toto ich správanie uskutočňuje v Únii, prevádzkovateľ alebo sprostredkovateľ by mal určiť zástupcu okrem prípadov, keď spracúvanie, ktoré vykonáva, je občasné, nezahŕňa vo veľkom rozsahu spracúvanie osobitných kategórií osobných údajov alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky, a nie je pravdepodobné, že povedie k riziku pre práva a slobody fyzických osôb, pričom sa zohľadní povaha, kontext, rozsah a účely spracúvania, alebo keď je prevádzkovateľ orgánom verejnej moci alebo verejnoprávnym subjektom. Zástupca by mal konať v mene prevádzkovateľa alebo sprostredkovateľa a môže sa na neho obracať ktorýkoľvek dozorný orgán.

K ods. 1

Nariadenie zakotvuje povinnosť prevádzkovateľa alebo sprostredkovateľa určiť v prípade, ak sa na neho uplatňuje článok 3 ods. 2 Nariadenia, zástupcu v EÚ, a to písomne. Ide o situácie, keď prevádzkovateľ alebo sprostredkovateľ síce nie je usadený v EÚ, ale spracúva osobné údaje dotknutých osôb nachádzajúcich sa v EÚ, a to v súvislosti s ponukou tovaru alebo služieb týmto osobám v EÚ (v EÚ musia byť tovary aj služby ponúkané) alebo v súvislosti so sledovaním správania dotknutých osôb, pokiaľ ide o ich správanie na území EÚ. Zatiaľ čo odsek 1 tohto článku upravuje všeobecnú povinnosť prevádzkovateľa alebo sprostredkovateľa zástupcu určiť, odsek 2 obsahuje výnimky z tejto povinnosti. Povinnosť určiť zástupcu sa vzťahuje tak na prevádzkovateľa, ako aj na sprostredkovateľa. Ak sa na hociktorého z nich vzťahuje článok 3 ods. 2 Nariadenia a nie je splnená výnimka z tejto povinnosti podľa článku 27 ods. 2 Nariadenia, je daný subjekt povinný určiť v EÚ svojho zástupcu, bez ohľadu na to, či sa táto povinnosť vzťahuje aj na druhý subjekt, prípadne či druhý subjekt svoju povinnosť určiť zástupcu splnil. V prípade, keď sa táto povinnosť vzťahuje na prevádzkovateľa aj na sprostredkovateľa, určením zástupcu zo strany prevádzkovateľa nezaniká povinnosť sprostredkovateľa a naopak.

Povinnosť určiť zástupcu poznala aj Smernica o ochrane osobných údajov, ako aj zákon č. 122/2013 Z. z. Vzhľadom na odlišnú úpravu miestnej pôsobnosti zakotvenú v Smernici o ochrane osobných údajov oproti jej úprave uvedenej v Nariadení sa však táto povinnosť vzťahovala iba na prevádzkovateľa (nie aj na sprostredkovateľa), a to iba v prípade, ak nebol usadený na území EÚ, avšak na účely spracúvania osobných údajov dotknutých osôb používal úplne alebo čiastočne automatizované alebo iné ako automatizované prostriedky spracúvania umiestnené na území členského štátu, pričom tieto prostriedky neboli využívané výlučne na prenos osobných údajov cez územie členských štátov. K určeniu zástupcu podľa zákona č. 122/2013 Z. z. tak prišlo napr. v prípade zhromažďovania osobných údajov na území SR v súvislosti s Google Street View pre potreby prevádzkovateľa Google Inc. sídliaceho v USA.

Zmenou vymedzenia územnej pôsobnosti, ako aj aplikáciou tejto povinnosti na sprostredkovateľa dochádza k rozšíreniu prípadov obligatórneho určenia zástupcu prevádzkovateľa alebo sprostredkovateľa v EÚ v porovnaní s doterajšou úpravou obsiahnutou v Smernici o ochrane osobných údajov aj v zákone č. 122/2013 Z. z.

V zmysle článku 4 bod 17 sa zástupcom rozumie fyzická alebo právnická osoba usadená v EÚ, ktorú prevádzkovateľ alebo sprostredkovateľ písomne určil a ktorá ho zastupuje, pokiaľ ide o jeho povinnosti podľa tohto nariadenia. V tejto súvislosti treba uviesť, že povinnosť určiť zástupcu treba odlišovať od povinnosti prevádzkovateľa alebo sprostredkovateľa určiť zodpovednú osobu, a to aj napriek skutočnosti, že úlohou obidvoch osôb je spolupráca s dozorným orgánom, ako aj komunikácia s dotknutými osobami v súvislosti so všetkými otázkami týkajúcimi sa spracúvania ich osobných údajov, ako aj uplatňovania ich práv podľa Nariadenia. V praxi môžu nastať prípady, keď sa na prevádzkovateľa alebo sprostredkovateľa budú vzťahovať obidve povinnosti (t. j. povinnosť ustanoviť zástupcu aj zodpovednú osobu).

K ods. 2

Tento odsek upravuje výnimky z povinnosti prevádzkovateľa alebo sprostredkovateľa určiť svojho zástupcu v EÚ napriek tomu, že sa na nich čl. 3 ods. 2 Nariadenia vzťahuje. Prevádzkovateľ alebo sprostredkovateľ nie je povinný určiť svojho zástupcu v EÚ v prípade, ak je 1. orgánom verejnej moci alebo verejnoprávnym subjektom, alebo 2. v prípade, ak spracúvanie osobných údajov je občasné a nezahŕňa vo veľkom rozsahu spracúvanie osobitných kategórií osobných údajov alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky a zároveň nie je pravdepodobné, že povedie k riziku pre práva a slobody fyzických osôb, pričom sa zohľadní povaha, kontext, rozsah a účely spracúvania. Na uplatnenie výnimky v druhom prípade sa vyžaduje, aby boli všetky podmienky splnené kumulatívne. To znamená, že prevádzkovateľ alebo sprostredkovateľ je povinný určiť zástupcu v EÚ aj v prípade, ak napr. spracúvanie nezahŕňa vo veľkom rozsahu spracúvanie osobitných kategórií osobných údajov alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky a zároveň nie je pravdepodobné, že povedie k riziku pre práva a slobody fyzických osôb, avšak spracúvanie nie je občasné (ale pravidelné alebo sústavné).

Splnenie podmienok na aplikáciu výnimky zo strany prevádzkovateľa nezbavuje sprostredkovateľa povinnosti určiť svojho zástupcu, ak sa na neho táto povinnosť vzťahuje, a naopak. V prípade, ak je prevádzkovateľ alebo sprostredkovateľ orgánom verejnej moci alebo verejnoprávnym subjektom, na ktorý sa vzťahuje čl. 3 ods. 2 Nariadenia, aplikuje sa na neho výnimka z povinnosti určiť zástupcu na území EÚ z pozície jeho postavenia. V danom prípade sa teda neskúma, či je spracúvanie vykonávané prevádzkovateľom alebo sprostredkovateľom občasné alebo nie, či je pravdepodobné, že povedie k riziku pre práva a slobody fyzických osôb, alebo či zahŕňa vo veľkom rozsahu spracúvanie osobitných kategórií osobných údajov alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky. Podľa názoru autorov tohto komentára by postavenie prevádzkovateľa alebo sprostredkovateľa ako orgánu verejnej moci alebo verejnoprávneho subjektu malo vyplývať z národného práva upravujúceho zriadenie či založenie prevádzkovateľa alebo sprostredkovateľa.

Nariadenie bližšie nedefinuje, kedy, resp. aké spracúvanie osobných údajov považuje za spracúvanie vo veľkom rozsahu. Určitou pomôckou k určeniu veľkého rozsahu môže byť recitál 91, ktorý sa však primárne vzťahuje na povinnosť vykonať posúdenie vplyvu na ochranu údajov. V zmysle tohto recitálu o *spracovateľské operácie veľkého rozsahu ide vtedy, ak ich cieľom je spracúvať značný objem osobných údajov na regionálnej, vnútroštátnej alebo nadnárodnej úrovni, mohli by ovplyvniť veľký počet dotknutých osôb a pravdepodobne povedú k vysokému riziku.* Recitál 91 zároveň uvádza, že *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 tomto smere nie je možné určiť konkrétne, presné číslo, ktoré by vytváralo deliacu čiaru pre určenie, či prevádzkovateľ alebo sprostredkovateľ spracúva danú kategóriu osobných údajov vo veľkom rozsahu, alebo nie. Určenie veľkého rozsahu bude vždy závisieť od okolností daného prípadu. Prevádzkovateľ alebo sprostredkovateľ by mal pri posudzovaní zobrať do úvahy najmä geografický rozsah spracúvania (napr. či spracúva danú kategóriu osobných údajov dotknutých osôb nachádzajúcich sa iba v určitom regióne, alebo v celej republike, prípade vo viacerých členských štátoch), aký je objem spracúvaných osobných údajov danej kategórie vo vzťahu ku geografickému rozsahu spracúvania. Ďalej je potrebné zohľadniť rozsah spracúvaných kategórií osobných údajov osobitnej kategórie, počet dotknutých osôb, trvanie spracovateľskej operácie ako aj riziká, ktoré môžu zo spracúvania vyplývať pre práva a slobody fyzických osôb. Uvedené údaje je potrebné

vyhodnotiť vo vzájomnej súvislosti. V tomto smere dávame do pozornosti zoznam spracovateľských operácií, ktoré podliehajú požiadavke na vykonanie DPIA, vydaný českým dozorným orgánom, ktorý v zozname poskytuje prevádzkovateľom prvé konkrétnejšie návody na určenie, či ide o spracúvanie osobných údajov vo veľkom rozsahu alebo nie; v tejto súvislosti však netreba opomenúť skutočnosť, že zoznam je vypracovaný po zohľadnení skutočností (napr. veľkosti populácie, administratívneho členenia republiky a pod.) daného členského štátu.

O spracúvanie vo veľkom rozsahu ide napr., ak internetový prehliadač spracúva osobitné kategórie osobných údajov dotknutých osôb na účely cielenej (behaviorálnej) reklamy.

Pojem riziko pre práva a slobody fyzických osôb je bližšie upravený v recitáli 75, v zmysle ktorého môže riziko pre práva a slobody fyzických osôb s rôznym stupňom pravdepodobnosti a závažnosti 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 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. Prevádzkovateľ aj sprostredkovateľ je povinný posúdiť riziko pre práva a slobody fyzických osôb a následne prijať vhodné technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku. Technickým a organizačným opatreniam sa venujeme v komentári k článku 24 a analýze rizika v komentári k článku 32.

Od povinnosti určiť zástupcu nie je oslobodený prevádzkovateľ ani sprostredkovateľ z dôvodu, že nebol schopný nájsť komerčného partnera, ktorý by bol ochotný vykonávať funkciu zástupcu a akceptovať všetky riziká s tým súvisiace. Tento argument použil WhatsApp pred Správnym súdom v Haagu, ktorý ho však neakceptoval ako výnimku, na základe ktorej sa na prevádzkovateľa alebo sprostredkovateľa povinnosť ustanoviť zástupcu nevzťahuje.

K ods. 3

Prevádzkovateľ alebo sprostredkovateľ, v závislosti od toho, na ktorý z uvedených subjektov sa povinnosť určiť zástupcu vzťahuje, je povinný určiť takého zástupcu, ktorý je usadený v jednom z tých členských štátov, v ktorých sa nachádzajú dotknuté osoby, ktorých osobné údaje sa spracúvajú v súvislosti s ponukou tovaru alebo služieb alebo so sledovaním ich správania. Cieľom tejto úpravy je zabezpečiť kontaktné miesto pre dozorné orgány aj dotknuté osoby aspoň v jednom z členských štátoch, v ktorých sa dotknuté osoby nachádzajú. Zákonodarca ponecháva výber členského štátu v plnej miere na dotknutého prevádzkovateľa alebo sprostredkovateľa. Tak, ako bolo uvedené v komentári k čl. 3 ods. 2 týkajúcom sa územnej pôsobnosti Nariadenia, mechanizmus one stop shop (t. j. mechanizmus jednotného kontaktného miesta) a určovanie vedúceho dozorného orgánu sa aplikuje iba na prípady cezhraničného spracúvania, pri ktorom sa vyžaduje, aby mal prevádzkovateľ alebo sprostredkovateľ v EÚ aspoň jednu prevádzkareň. Nevzťahuje sa teda na prípady, ak prevádzkovateľ alebo sprostredkovateľ nie je v EÚ usadený, a teda tu nemá ani jednu prevádzkareň. K výkladu pojmu prevádzkareň pozri bližšie komentár k čl. 3 ods. 1. Tento mechanizmus nie je aktivovaný ani určením zástupcu prevádzkovateľa alebo sprostredkovateľa v niektorom z členských štátov. Zvolením členského štátu A nie je vylúčená pôsobnosť členského štátu B, ak v súvislosti s ponukou tovaru alebo služieb dotknutým osobám v EÚ alebo so sledovaním správania dotknutých osôb, pokiaľ ide o ich správanie na území EÚ, dochádza k spracúvaniu osobných údajov týchto osôb

nachádzajúcich sa v členskom štáte B. Zástupca je teda povinný spolupracovať s príslušnými dozornými orgánmi.

K ods. 4

Prevádzkovateľ alebo sprostredkovateľ je povinný zástupcu písomne poveriť, aby konal v mene prevádzkovateľa alebo sprostredkovateľa, a to v súvislosti s plnením jeho povinností podľa Nariadenia. Zástupca je povinný vykonávať svoje úlohy podľa poverenia, ktoré dostal od prevádzkovateľa alebo sprostredkovateľa. Prevádzkovateľ alebo sprostredkovateľ sa môže rozhodnúť, či zástupcu poverí voči dozorným orgánom a dotknutým osobám popri prevádzkovateľovi alebo sprostredkovateľovi, alebo namiesto neho. Na zástupcu sa môžu obracať dozorné orgány ako aj dotknuté osoby, a to vo všetkých otázkach týkajúcich sa spracúvania na účely zabezpečenia súladu s Nariadením. Dozorný orgán aj dotknuté osoby sa však môžu kedykoľvek obrátiť priamo na prevádzkovateľa alebo sprostredkovateľa. Recitál 80 v tomto smere uvádza, že v prípade, ak prevádzkovateľ alebo sprostredkovateľ nezabezpečia súlad s Nariadením, určený zástupca by mal podliehať konaniam na presadenie práva. Napriek tomu, že tento recitál predpokladá zodpovednosť zástupcu v prípade porušenie Nariadenia zo strany prevádzkovateľa alebo sprostredkovateľa, samotný text Nariadenia túto situáciu v jednotlivých článkoch bližšie neupravuje. Je otázne, či jednotlivé členské štáty prijmú do svojich národných predpisov aj sankcie voči zástupcovi prevádzkovateľa alebo sprostredkovateľa. Slovenská republika upravila v novom zákone o ochrane osobných údajov voči zástupcovi iba oprávnenie úradu uložiť zástupcovi poriadkovú pokutu, a to do výšky 2 000 eur, ak nezabezpečí primerané podmienky na výkon kontroly alebo do výšky 10 000 eur, ak marí výkon kontroly.

V prípade, ak je prevádzkovateľ alebo sprostredkovateľ povinný určiť v EÚ svojho zástupcu, je povinný poskytnúť dotknutej osobe informáciu o jeho totožnosti a kontaktných údajoch v súlade s článkom 13 alebo 14 Nariadenia.

Nariadenie zástupcu prevádzkovateľa alebo sprostredkovateľa výslovne spomína v článku 30 v súvislosti so záznamami o spracovateľských činnostiach, ako aj v článku 31 upravujúcom spoluprácu s dozorným orgánom. V zmysle uvedených článkov je zástupca prevádzkovateľa povinný viesť záznamy o spracovateľských činnostiach, za ktoré je zodpovedný, ak nie je od tejto povinnosti podľa článku 31 ods. 5 oslobodený. V zmysle článku 30 ods. 2 je zástupca sprostredkovateľa povinný viesť záznamy o všetkých kategóriách spracovateľských činností, ktoré vykonal v mene prevádzkovateľa, ak sa na neho nevzťahuje výnimka podľa článku 30 ods. 5. Zástupca prevádzkovateľa aj sprostredkovateľa je povinný na požiadanie spolupracovať s dozorným orgánom pri výkone jeho úloh. Táto povinnosť je prepojená s oprávnením dozorného orgánu uvedeným v článku 58 ods. 1 písm. a) Nariadenia nariadiť zástupcovi prevádzkovateľa alebo sprostredkovateľa, aby mu poskytol všetky informácie, ktoré vyžaduje na plnenie svojich úloh. Inštitút zástupcu prevádzkovateľa alebo sprostredkovateľa výrazne uľahčuje výkon vyšetrovacích právomocí dozorného orgánu a tým priaznivo prispieva k zabezpečeniu ochrany práv dotknutých osôb.

Vzhľadom na zásadu zodpovednosti a povinnosť preukazovania súladu s Nariadením je nevyhnutné, aby zástupca pre prípad možnej kontroly od dozorného orgánu uchoval počas svojho poverenia písomný dôkaz o poverení.

Za porušenie povinnosti prevádzkovateľa a sprostredkovateľa určiť zástupcu v EÚ hrozí prevádzkovateľovi a sprostredkovateľovi správna pokuta až do výšky 10 000 000 eur alebo v prípade podniku až do výšky 2 % celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia. K pokutám pozri komentár k článku 83.

K ods. 5

Určením zástupcu nie je dotknutá samotná zodpovednosť prevádzkovateľa alebo sprostredkovateľa za dodržiavanie ich povinností v zmysle Nariadenia. K zodpovednosti pozri bližšie komentár k článku 82. Rovnako nie sú dotknuté ani právne prostriedky nápravy, ktoré by sa mohli iniciovať proti samotnému prevádzkovateľovi alebo sprostredkovateľovi.

Článok 28
Sprostredkovateľ

1. Ak sa má spracúvanie uskutočniť v mene prevádzkovateľa, prevádzkovateľ využíva len sprostredkovateľov poskytujúcich dostatočné záruky na to, že sa prijmú primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo požiadavky tohto nariadenia a aby sa zabezpečila ochrana práv dotknutej osoby.

2. Sprostredkovateľ nezapojí ďalšieho sprostredkovateľa bez predchádzajúceho osobitného alebo všeobecného písomného povolenia prevádzkovateľa. V prípade všeobecného písomného povolenia sprostredkovateľ informuje prevádzkovateľa o akýchkoľvek zamýšľaných zmenách v súvislosti s pridaním alebo nahradením ďalších sprostredkovateľov, čím sa prevádzkovateľovi dá možnosť namietať voči takýmto zmenám.

3. Spracúvanie sprostredkovateľom sa riadi zmluvou alebo iným právnym aktom podľa práva Únie alebo práva členského štátu, ktoré zaväzuje sprostredkovateľa voči prevádzkovateľovi a ktorým sa stanovuje predmet a doba spracúvania, povaha a účel spracúvania, typ osobných údajov a kategórie dotknutých osôb a povinnosti a práva prevádzkovateľa. Uvedená zmluva alebo iný právny akt najmä stanovia, že sprostredkovateľ:

a) spracúva osobné údaje len na základe zdokumentovaných pokynov prevádzkovateľa, a to aj pokiaľ ide o prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii, s výnimkou prípadov, keď si to vyžaduje právo Únie alebo právo členského štátu, ktorému sprostredkovateľ podlieha; v takom prípade sprostredkovateľ oznámi prevádzkovateľovi túto právnu požiadavku pred spracúvaním, pokiaľ dané právo takéto oznámenie nezakazuje zo závažných dôvodov verejného záujmu;

b) zabezpečí, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovajú dôvernosť informácií, alebo aby boli viazané vhodnou povinnosťou zachovávať dôvernosť informácií vyplývajúcou zo štatútu;

c) vykoná všetky požadované opatrenia podľa článku 32;

d) dodržiava podmienky zapojenia ďalšieho sprostredkovateľa uvedené v odsekoch 2 a 4;

e) po zohľadnení povahy spracúvania v čo najväčšej miere pomáha prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti reagovať na žiadosti o výkon práv dotknutej osoby ustanovených v kapitole III;

f) pomáha prevádzkovateľovi zabezpečiť plnenie povinností podľa článkov 32 až 36 s prihliadnutím na povahu spracúvania a informácie dostupné sprostredkovateľovi;

g) po ukončení poskytovania služieb týkajúcich sa spracúvania na základe rozhodnutia prevádzkovateľa všetky osobné údaje vymaže alebo vráti prevádzkovateľovi a vymaže existujúce kópie, ak právo Únie alebo právo členského štátu nepožaduje uchovávanie týchto osobných údajov;

h) poskytne prevádzkovateľovi všetky informácie potrebné na preukázanie splnenia povinností stanovených v tomto článku a umožní audity, ako aj kontroly vykonávané prevádzkovateľom alebo iným audítorom, ktorého poveril prevádzkovateľ, a prispieva k nim.

So zreteľom na písmeno h) prvého pododseku sprostredkovateľ bezodkladne informuje prevádzkovateľa, ak sa podľa jeho názoru pokynom porušuje toto nariadenie alebo iné právne predpisy Únie alebo členského štátu týkajúce sa ochrany údajov.

4. Ak sprostredkovateľ zapojí do vykonávania osobitných spracovateľských činností v mene prevádzkovateľa ďalšieho sprostredkovateľa, tomuto ďalšiemu sprostredkovateľovi sa prostredníctvom zmluvy alebo iného právneho aktu podľa práva Únie alebo práva členského štátu uložia rovnaké povinnosti ochrany údajov, ako sa stanovujú v zmluve alebo inom právnom akte uzatvorenom medzi prevádzkovateľom a sprostredkovateľom podľa odseku 3, a to predovšetkým poskytnutie dostatočných záruk na vykonanie primeraných technických a organizačných opatrení takým spôsobom, aby spracúvanie spĺňalo požiadavky tohto nariadenia. Ak tento ďalší sprostredkovateľ nesplní svoje povinnosti ochrany údajov, pôvodný sprostredkovateľ

zostáva voči prevádzkovateľovi plne zodpovedný za plnenie povinností tohto ďalšieho sprostredkovateľa.

5. Dodržiavanie schváleného kódexu správania uvedeného v článku 40 alebo schváleného certifikačného mechanizmu uvedeného v článku 42 sprostredkovateľom sa môže použiť ako prvok na preukázanie dostatočných záruk uvedených v odsekoch 1 a 4 tohto článku.

6. Bez toho, aby tým bola dotknutá individuálna zmluva medzi prevádzkovateľom a sprostredkovateľom, zmluva alebo iný právny akt uvedené v odsekoch 3 a 4 tohto článku sa môžu vcelku alebo sčasti zakladať na štandardných zmluvných doložkách uvedených v odsekoch 7 a 8 tohto článku, a to aj v prípadoch, keď sú súčasťou certifikácie udelenej prevádzkovateľovi alebo sprostredkovateľovi podľa článkov 42 a 43.

7. Komisia môže stanoviť štandardné zmluvné doložky pre záležitosti uvedené v odsekoch 3 a 4 tohto článku a v súlade s postupom preskúmania uvedeným v článku 93 ods. 2.

8. Dozorný orgán môže prijať štandardné zmluvné doložky pre záležitosti uvedené v odsekoch 3 a 4 tohto článku a v súlade s mechanizmom konzistentnosti uvedeným v článku 63.

9. Zmluva alebo iný právny akt uvedené v odsekoch 3 a 4 sa vypracujú v písomnej podobe vrátane elektronickej podoby.

10. Bez toho, aby dotknuté články 82, 83 a 84, ak sprostredkovateľ poruší toto nariadenie tým, že určí účely a prostriedky spracúvania, považuje sa v súvislosti s daným spracúvaním za prevádzkovateľa.

Súvisiace ustanovenia: recitál 79, 81, 95 a 146, článok 4 ods. 8, článok 30, 31, 32, 33 ods. 2, článok 37, článok 82 a 83

Súvisiace predpisy: Občiansky zákonník, nový zákon o ochrane osobných údajov

---

Komentár k článku 28

Recitál 79: Ochrana práv a slobôd dotknutých osôb, ako aj povinnosti a zodpovednosť prevádzkovateľov a sprostredkovateľov, a to aj v súvislosti s monitorovaním zo strany dozorných orgánov a ich opatreniami, si vyžaduje jasné rozdelenie povinností podľa tohto nariadenia vrátane prípadov, v ktorých prevádzkovateľ určuje účely a prostriedky spracúvania spoločne s inými prevádzkovateľmi, alebo v prípadoch, v ktorých sa spracovateľská operácia vykonáva v mene prevádzkovateľa.

Recitál 81: S cieľom zabezpečiť súlad s požiadavkami tohto nariadenia v súvislosti so spracúvaním, ktoré má v mene prevádzkovateľa vykonať sprostredkovateľ, by mal prevádzkovateľ pri poverovaní sprostredkovateľa spracovateľskými činnosťami využívať len takých sprostredkovateľov, ktorí poskytujú dostatočné záruky, najmä pokiaľ ide o odborné znalosti, spoľahlivosť a zdroje, na to, že prijmú technické a organizačné opatrenia, ktoré budú spĺňať požiadavky tohto nariadenia, vrátane požiadavky na bezpečnosť spracúvania. Dodržiavanie schváleného kódexu správania alebo schváleného certifikačného mechanizmu sprostredkovateľom sa môže použiť ako prvok na preukázanie súladu s povinnosťami prevádzkovateľa. Vykonávanie spracúvania sprostredkovateľom by sa malo riadiť zmluvou alebo iným právnym aktom podľa práva Únie alebo práva členského štátu, ktorými by bol sprostredkovateľ viazaný voči prevádzkovateľovi a v ktorých by sa stanovil predmet a doba spracúvania, povaha a účely spracúvania, typ osobných údajov a kategórie dotknutých osôb, a ktoré by mali zohľadniť osobitné úlohy a povinnosti sprostredkovateľa v kontexte spracúvania, ktoré sa má vykonať, a riziko pre práva a slobody dotknutých osôb. Prevádzkovateľ a sprostredkovateľ si môžu vybrať použitie individuálnej zmluvy alebo štandardných zmluvných doložiek, ktoré prijme buď priamo Komisia, alebo ktoré prijme dozorný orgán v súlade s mechanizmom konzistentnosti a následne ich prijme Komisia. Po ukončení spracúvania v mene prevádzkovateľa by mal sprostredkovateľ podľa rozhodnutia prevádzkovateľa vrátiť alebo vymazať osobné údaje, pokiaľ podľa práva Únie alebo práva členského štátu, ktorému sprostredkovateľ podlieha, neexistuje požiadavka na uchovanie osobných údajov.

Recitál 95: Sprostredkovateľ by mal pomáhať prevádzkovateľovi pri zabezpečovaní súladu s povinnosťami, ktoré vyplývajú z vykonávania posúdení vplyvu na ochranu údajov a z predchádzajúcej konzultácie dozorného orgánu, keď je to potrebné alebo keď ho o to prevádzkovateľ požiada.

Recitál 146: Prevádzkovateľ alebo sprostredkovateľ by mali nahradiť akúkoľvek škodu, ktorú môže osoba utrpieť v dôsledku spracúvania, ktoré je v rozpore s týmto nariadením. Prevádzkovateľ alebo sprostredkovateľ by však mali byť tejto zodpovednosti zbavení, ak preukážu, že za škodu nenesú žiadnu zodpovednosť. Podľa judikatúry Súdneho dvora EÚ by sa mal pojem škody vykladať v širokom zmysle spôsobom, ktorý v plnej miere zohľadňuje ciele tohto nariadenia. Týmto nie sú dotknuté prípadné nároky na náhradu škody vyplývajúce z porušenia iných pravidiel stanovených v práve Únie alebo v práve členského štátu. Spracúvanie, ktoré je v rozpore s týmto nariadením, zahŕňa aj spracúvanie, ktoré je v rozpore s delegovanými a vykonávacími aktmi prijatými v súlade s týmto nariadením a právom členského štátu, ktorým sa podrobnejšie upravujú pravidlá z tohto nariadenia. Dotknuté osoby by za utrpenú škodu mali dostať úplnú a účinnú náhradu. Ak sú prevádzkovatelia alebo sprostredkovatelia zapojení do rovnakého spracúvania, každý prevádzkovateľ alebo sprostredkovateľ by mal byť zodpovedný za celú škodu. Ak sú však v súlade s právom členského štátu účastníkmi toho istého súdneho konania, náhrada škody sa môže rozdeliť podľa miery zodpovednosti každého prevádzkovateľa alebo sprostredkovateľa za škodu spôsobenú spracúvaním, pokiaľ je zaistená úplná a účinná náhrada pre dotknutú osobu, ktorá utrpela škodu. Každý prevádzkovateľ alebo sprostredkovateľ, ktorý nahradil celú škodu, môže následne začať regresné konanie voči iným prevádzkovateľom alebo sprostredkovateľom zapojeným do toho istého spracúvania.

K ods. 1

Základné definície pojmov prevádzkovateľ a sprostredkovateľ sú obsiahnuté v článku 4 body 7 a 8. Vo všeobecnosti platí, že za súlad spracúvania osobných údajov s Nariadením zodpovedá prevádzkovateľ, ktorý je povinný tento súlad v prípade kontroly dozornému orgánu preukázať. Prevádzkovateľ je povinný prijať vhodné technické a organizačné opatrenia, a to s ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb. V prípade, ak sa spracúvaním osobných údajov rozhodne poveriť sprostredkovateľa, musí zabezpečiť, aby boli požiadavky Nariadenia, a teda aj primeraná úroveň bezpečnosti dodržané. Nariadenie v tomto smere vyžaduje, aby prevádzkovateľ využíval iba takých sprostredkovateľov, ktorí poskytujú dostatočné záruky, že prijmú primerané technické a organizačné opatrenia a zabezpečia tým nielen súlad spracúvania s požiadavkami Nariadenia ale aj ochranu práv dotknutej osoby. Okrem hlavných cieľov, akými sú zachovanie dôvernosti, integrity a celistvosti, by mal prevádzkovateľ upriamiť pozornosť aj na zabezpečenie transparentnosti, izolovanosti (neprepojiteľnosti osobných údajov, ktoré sprostredkovateľ spracúva v mene prevádzkovateľa s inými osobnými údajmi dotknutých osôb, napr. získanými a spracúvanými sprostredkovateľom pre iného prevádzkovateľa alebo získanými činnosťou sprostredkovateľa, ktorá nesúvisí so spracúvaním realizovaným v mene prevádzkovateľa), schopnosti intervencie (poskytovať prevádzkovateľovi podporu pri uľahčovaní výkonu práv dotknutých osôb a reagovaní na ich žiadosti) a prenosnosti (článok 20). Existenciu dostatočných záruk je prevádzkovateľ povinný preveriť pred samotným poverením sprostredkovateľa. To platí aj v prípade prolongácie zmluvy uzatvorenej so sprostredkovateľom. Prevádzkovateľ by mal preveriť poskytnutie dostatočných záruk, najmä z hľadiska spoľahlivosti sprostredkovateľa, jeho odborných znalostí a zdrojov potrebných na prijatie primeraných technických a organizačných opatrení tak, aby spracúvanie spĺňalo požiadavky Nariadenia a až v prípade kladného preverenia sprostredkovateľa spracúvaním poveriť.

Cieľom tejto úpravy je nezniżovať úroveň ochrany dotknutých osôb v prípade, ak sa bude spracúvanie vykonávať prostredníctvom sprostredkovateľa. Jedným zo spôsobov preukázania dostatočných záruk môže byť dodržiavanie schváleného kódexu správania, dodržiavanie vydaného certifikátu, určenie zodpovednej osoby sprostredkovateľa v prípade, ak nejde o prípady obligatórne určenej zodpovednej osoby, checklist s požiadavkami týkajúcimi sa ochrany osobných údajov a bezpečnosti, vykonanie due dilligence preukazujúceho, že sprostredkovateľ poskytuje dostatočné záruky, platné certifikáty zamerané na riadenie informačnej bezpečnosti v organizáciách udelené sprostredkovateľovi (certifikácia systému manažérstva informačnej bezpečnosti podľa ISO/IEC 27001), pričom sa v závislosti od konkrétneho spracúvania môže vyžadovať aj ich kombinácia.

K výkladu pojmu „primerané technické a organizačné opatrenia“ pozri komentár k článku 24.

V súlade so zásadou zodpovednosti a povinnosti prevádzkovateľa preukázať súlad s požiadavkami Nariadenia odporúčame prevádzkovateľovi zdokumentovať skutočnosti, ktoré ho viedli k záveru, že sprostredkovateľ poskytuje dostatočné záruky a takúto dokumentáciu uchovať ako dôkaz pre prípad možnej kontroly.

K ods. 2

Nariadenie rovnako ako Smernica o ochrane osobných údajov a zákon č. 122/2013 Z. z. pripúšťa možnosť reťazenia sprostredkovateľov, teda situáciu, keď sprostredkovateľ, ktorý spracúva osobné údaje v mene prevádzkovateľa, zapojí do spracúvania osobných údajov ďalší subjekt, t. j. ďalšieho sprostredkovateľa. Aj v takom prípade spracúva ďalší sprostredkovateľ osobné údaje v mene prevádzkovateľa. V zmysle Nariadenia nie je sprostredkovateľ oprávnený zapojiť do spracúvania ďalšieho sprostredkovateľa bez **predchádzajúceho písomného povolenia** prevádzkovateľa. S poukazom na § 40 ods. 1 Občianskeho zákonníka, v zmysle ktorého je právny úkon neplatný, ak nebol urobený vo forme, ktorú vyžaduje zákon alebo dohoda účastníkov, platí, že nedostatok písomnej formy povolenia spôsobuje jeho absolútnu neplatnosť, ktorá sa nedá konvalidovať. Takéto povolenie je neplatné od počiatku, a to bez ohľadu na to, či sa prevádzkovateľ, sprostredkovateľ alebo ďalší sprostredkovateľ neplatnosti dovolá. Len pre úplnosť uvádzame, že v zmysle slovenského právneho poriadku[363)] písomná forma je zachovaná aj v prípade, ak je právny úkon urobený telegraficky, ďalekopisom alebo elektronickými prostriedkami, ktoré umožňujú zachytenie obsahu právneho úkonu a určenie osoby, ktorá právny úkon urobila. Písomná forma je zachovaná vždy, ak právny úkon urobený elektronickými prostriedkami je podpísaný zaručeným elektronickým podpisom alebo zaručenou elektronickou pečaťou.

Prevádzkovateľ má podľa Nariadenia možnosť udeliť sprostredkovateľovi osobitné povolenie využívať konkrétneho, v povolení vopred určeného ďalšieho sprostredkovateľa. Prevádzkovateľ tiež môže vydať všeobecné povolenie oprávňujúce sprostredkovateľa (alebo viacerých sprostredkovateľov prevádzkovateľa) využívať ďalšieho, prípadne ďalších vopred neurčených sprostredkovateľov. V prípade všeobecného povolenia prevádzkovateľa je sprostredkovateľ povinný pred zapojením konkrétneho ďalšieho sprostredkovateľa o tejto skutočnosti informovať prevádzkovateľa, aby mu poskytol možnosť namietať. To platí aj v prípade, ak chce sprostredkovateľ v rámci všeobecného povolenia nahradiť jedného sprostredkovateľa za iného. Informácia o konkrétnom ďalšom sprostredkovateľovi musí byť doručená prevádzkovateľovi tak, aby prevádzkovateľ mohol zasiahnuť voči výberu ďalšieho sprostredkovateľa efektívne ešte pred začatím výkonu spracovateľských činností takýmto ďalším sprostredkovateľom.

Uvedené povolenie (osobitné alebo všeobecné) môže byť súčasťou sprostredkovateľskej zmluvy alebo iného právneho aktu podľa práva Únie alebo práva členského štátu, ktoré zaväzuje sprostredkovateľa voči prevádzkovateľovi. Písomné povolenie prevádzkovateľa je potrebné archivovať ako dôkaz pre prípad možnej kontroly.

Banka sa rozhodne, že na doručovanie platobných kariet do vlastných rúk klientov banky využije služby kuriérskej spoločnosti ABC, s. r. o. Za tým účelom uzatvorí so spoločnosťou ABC, s. r. o., sprostredkovateľskú zmluvu. V uvedenom vzťahu vystupuje banka v postavení prevádzkovateľa a spoločnosť ABC, s. r. o., v postavení sprostredkovateľa. Banka v sprostredkovateľskej zmluve spoločnosti ABC, s. r. o., povolí, aby do spracúvania zapojila aj spoločnosť Data, s. r. o. (v tomto prípade ide o osobitné povolenie, pričom spoločnosť Data, s. r. o., vystupuje v postavení ďalšieho sprostredkovateľa).

Banka v sprostredkovateľskej zmluve môže spoločnosti ABC, s. r. o., povoliť, aby do spracúvania zapojila ľubovoľnú kuriérsku spoločnosť, ktorá je spôsobilá poskytnúť dodatočné záruky určené v sprostredkovateľskej zmluve (v tomto prípade ide o všeobecné povolenie). Spoločnosť ABC, s. r. o., je povinná banku informovať o výbere ďalšieho sprostredkovateľa pred začatím výkonu spracovateľských činností takýmto ďalším sprostredkovateľom.

Sprostredkovateľ (a rovnako aj ďalší sprostredkovateľ) spracúva osobné údaje dotknutých osôb v mene prevádzkovateľa na právnom základe prevádzkovateľa. Uvedené samozrejme platí len v prípade, ak sprostredkovateľ spracúva osobné údaje dotknutých osôb len na účely určené prevádzkovateľom a podľa jeho pokynov.

363) Ust. § 40 ods. 4 Občianskeho zákonníka.

K ods. 3

Odsek 3 upravuje priamy vzťah prevádzkovateľa a sprostredkovateľa. Vzťah medzi sprostredkovateľom a ďalším sprostredkovateľom zapojeným do spracovateľských činností vykonávaných v mene prevádzkovateľa je upravený v ods. 4.

Sprostredkovateľ je oprávnený spracúvať osobné údaje v mene prevádzkovateľa **iba na základe zmluvy uzatvorenej s prevádzkovateľom, prípadne so spoločnými prevádzkovateľmi, alebo na základe iného právneho aktu** podľa práva Únie alebo práva členského štátu zaväzujúceho sprostredkovateľa voči prevádzkovateľovi.

Pojem „právny akt" Nariadenie spája najmä s normatívnou činnosťou orgánov verejnej správy (pozri recitál 17, 19, 115 a iné), ale nie je ani vylúčené, že tento pojem zahŕňa aj právny úkon, teda prejav vôle smerujúci k vzniku, zmene alebo zániku práv a povinností, ktoré právne predpisy spájajú s týmto prejavom (§ 34 Občianskeho zákonníka).

Podľa názoru autorov tohto komentára sa za iný právny akt podľa práva Únie alebo práva členského štátu môže považovať akýkoľvek právny úkon, ktorým je možné platne založiť záväzok sprostredkovateľa voči prevádzkovateľovi a ktorý bude obsahovať povinné náležitosti uvedené v ods. 3. Nariadenie výslovne neurčuje, že daný právny akt má byť dvojstranný (ako zmluva), domnievame sa však, že dvojstrannosť tohto aktu implicitne vyplýva zo vzájomného vzťahu medzi prevádzkovateľom a sprostredkovateľom. Pritom môže ísť aj o dva jednostranné právne úkony. V slovenskom právnom prostredí pôjde napr. o jednostranné vyhlásenie sprostredkovateľa s obsahovými náležitosťami podľa ods. 3, ktorým sprostredkovateľ prevezme tam uvedené záväzky voči prevádzkovateľovi, na ktoré môže nadväzovať súhlas prevádzkovateľa udelený napr. v písomnej forme, zakliknutím políčka súhlasu na webe a pod. Do úvahy prichádza aj dohoda o plnomocenstve alebo poverenie na spracúvanie osobných údajov vystavené zo strany prevádzkovateľa s výslovným akceptovaním určených povinností zo strany sprostredkovateľa. Prirodzene bez ohľadu na možnosť založenia spolupráce medzi prevádzkovateľom a sprostredkovateľom na základe takýchto právnych aktov podľa práva Únie alebo práva členského štátu zmluva upravujúca spracúvanie sprostredkovateľom obsahujúca minimálne náležitosti uvedené v ods. 3 je ako dvojstranný právny úkon najistejším základom spracúvania sprostredkovateľom.

Formou zmluvy alebo právneho aktu podľa práva Únie alebo práva členského štátu sa zaoberá ods. 9.

Prevádzkovateľ a sprostredkovateľ môžu uzatvoriť individuálnu zmluvu alebo môžu využiť štandardné zmluvné doložky, ktoré stanoví buď Komisia alebo prijme dozorný orgán v súlade s mechanizmom konzistentnosti. V čase písania tohto komentára majú autori vedomosť o jedných štandardných zmluvných doložkách upravujúcich vzťah medzi sprostredkovateľom a prevádzkovateľom, ktoré predložil v súlade s mechanizmom konzistentnosti dánsky dozorný orgán. Jednotlivé dokumenty nájdete na stránke Výboru https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-142019-draft-standard-contractual-clauses_en.

Náležitosti zmluvy alebo iného právneho aktu podľa práva Únie alebo práva členského štátu

Medzi základné náležitosti zmluvy alebo iného právneho aktu podľa práva Únie alebo práva členského štátu patrí určenie predmetu a doby spracúvania, povahy a účelu spracúvania, typu osobných údajov, kategórie dotknutých osôb a určenie práv a povinností prevádzkovateľa a sprostredkovateľa v kontexte spracúvania, ktoré sa má vykonať. Prevádzkovateľ a sprostredkovateľ sú povinní v zmluve alebo v inom právnom akte podľa práva Únie alebo práva členského štátu stanoviť, aké spracúvanie má sprostredkovateľ v mene prevádzkovateľa vykonávať (napr. poskytovať cloudové služby, zabezpečovať likvidáciu osobných údajov). Zmluva alebo iný právny akt podľa práva Únie alebo práva členského štátu musí obsahovať aj určenie typu osobných údajov, t. j. napr. určenie, že prevádzkovateľ poveril sprostredkovateľa spracúvaním mena, priezviska, dátumu narodenia, adresy a telefónneho čísla dotknutej osoby. Ďalej musia obsahovať účel spracúvania, ktorý musí byť určený v súlade s účelom spracúvania prevádzkovateľa. Nariadenie neobsahuje obmedzenie platnosti zmluvy, preto môže byť uzatvorená aj na dobu neurčitú. Pokiaľ ide o kategórie dotknutých osôb, sprostredkovateľská zmluva či iný právny akt podľa práva Únie alebo práva členského štátu musia obsahovať určenie, či je sprostredkovateľ poverený spracúvaním osobných údajov klientov banky,

zamestnancov spoločnosti, uchádzačov o zamestnanie a pod. Hoci Nariadenie používa pojem „povaha spracúvania“ v súvislosti s viacerými povinnosťami prevádzkovateľa aj sprostredkovateľa, nikde tento pojem bližšie nevysvetľuje ani nedefinuje. Podľa názorov autorov tohto komentára môžeme pod povahou spracúvania rozumieť to, či sa budú spracúvať bežné osobné údaje alebo osobné údaje odhaľujúce rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie, členstvo v odborových organizáciách, alebo genetické údaje, biometrické údaje na individuálnu identifikáciu fyzickej osoby, údaje týkajúce sa zdravia, alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby, alebo osobné údaje týkajúce sa uznania viny za trestné činy a priestupky. Povaha spracúvania môže zahŕňať aj určenie, či sa osobné údaje budú spracúvať s využitím nových technológií, či pôjde o výlučne automatizované individuálne rozhodovanie s právnymi účinkami vrátane profilovania alebo spracúvanie vykonávané neautomatizovanými prostriedkami a pod.

Nariadenie stanovuje povinné minimálne požiadavky na obsah zmluvy alebo iného právneho aktu podľa práva Únie alebo práva členského štátu, ktoré zaväzuje sprostredkovateľa voči prevádzkovateľovi. V porovnaní s doterajšou úpravou obsiahnutou v Smernici o ochrane osobných údajov, ako aj v zákone č. 122/2013 Z. z. došlo k ich zmene. Zmluva alebo iný právny akt musia najmä stanoviť, že sprostredkovateľ spracúva osobné údaje len na základe zdokumentovaných pokynov prevádzkovateľa. K výkladu pojmu „pokyn“ odporúčame pozrieť rozsudok Súdneho dvora EÚ z 22. novembra 2012 vo veci C-119/12 Josef Probst spracovaný v časti judikatúra. Rozsudok sa týkal výkladu ustanovení Smernica 2002/58/ES, avšak Súdny dvor EÚ v uvedenom rozsudku v časti právny rámec odkazuje aj na ustanovenia Smernice o ochrane osobných údajov týkajúce sa sprostredkovateľa. Súdny dvor EÚ v predmetnej veci konštatoval, že ani Smernica 2002/58, ani dokumenty relevantné pre jej výklad, akými sú *travaux préparatoires*, neposkytujú vysvetlenia presného dosahu pojmu „na pokyn“. Za týchto okolností v súlade s judikatúrou Súdneho dvora EÚ sa význam tohto pojmu musí určiť podľa jeho obvyklého významu v bežnom jazyku, pričom sa zároveň zohľadnia súvislosti, v ktorých sa používa, ako aj účel sledovaný právnou úpravou, v ktorej sa nachádza. Pokiaľ ide o obvyklý význam tohto pojmu v bežnom jazyku, treba sa domnievať, že osoba koná na pokyn inej osoby vtedy, keď prvá osoba koná na základe pokynov a pod dohľadom druhej osoby. Článok 6 ods. 2 a 5 Smernice 2002/58 obsahuje výnimku z povinnosti zabezpečiť dôvernosť správ stanovenej v článku 5 ods. 1 tejto smernice tým, že povoľuje spracovávať údaje o prenose dát v súvislosti s požiadavkami spojenými s činnosťami fakturácie služieb. Keďže ide o výnimku, toto ustanovenie smernice, a teda aj pojem „na pokyn“, treba vykladať doslovne. V posudzovanej veci Súdny dvor EÚ uviedol, že takýto výklad znamená, že poskytovateľ služieb musí mať možnosť vykonávať účinný dohľad, ktorý mu umožňuje overiť, či postupník pohľadávok dodržiava povinnosti, ktoré má pri spracovaní údajov o prenose dát.

Zmluva alebo iný právny akt musia ďalej stanoviť, že sprostredkovateľ zabezpečí, že osoby oprávnené spracúvať osobné údaje sú zaviazané zachovať dôvernosť informácií, vykoná všetky požadované primerané technické a organizačné opatrenia, zapojí ďalšieho sprostredkovateľa iba s predchádzajúcim písomným povolením prevádzkovateľa a na základe uzatvorenej písomnej zmluvy so sprostredkovateľom, po zohľadnení povahy spracúvania pomáha v čo najväčšej miere prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti reagovať na žiadosti o výkon práv dotknutej osoby podľa Nariadenia, pomáha prevádzkovateľovi zabezpečiť plnenie povinností vo vzťahu k bezpečnosti spracúvania, oznámeniu porušenia ochrany osobných údajov dozornému orgánu, oznámeniu porušenia ochrany osobných údajov dotknutej osobe a vykonaniu posúdenia vplyvu na ochranu údajov, po ukončení poskytovania služieb týkajúcich sa spracúvania na základe rozhodnutia prevádzkovateľa všetky osobné údaje vymaže alebo vráti prevádzkovateľovi a vymaže existujúce kópie, ak právo Únie alebo právo členského štátu nepožaduje uchovávanie týchto osobných údajov. Zmluva alebo iný právny akt musia ďalej stanoviť, že sprostredkovateľ poskytne prevádzkovateľovi všetky informácie potrebné na preukázanie splnenia svojich povinností stanovených v článku 28 ods. 3 a umožní audity a kontroly vykonávané prevádzkovateľom alebo iným audítorom, ktorého poveril prevádzkovateľ a prispieva k nim. V tomto smere je sprostredkovateľ povinný bezodkladne informovať prevádzkovateľa, ak sa podľa jeho názoru

pokynom porušuje Nariadenie alebo iné právne predpisy Únie alebo členského štátu týkajúce sa ochrany údajov. Sprostredkovateľ sa môže s prevádzkovateľom v zmluve alebo v inom právnom akte podľa práva Únie alebo práva členského štátu dohodnúť aj na plnení iných prevádzkovateľových povinností (napr. informačnej povinnosti voči dotknutým osobám).

Základné povinnosti sprostredkovateľa

Jednou z kľúčových povinností sprostredkovateľa vo vzájomnom vzťahu s prevádzkovateľom je povinnosť sprostredkovateľa spracúvať osobné údaje len na základe a v rozsahu zdokumentovaných pokynov prevádzkovateľa. Táto povinnosť sprostredkovateľa je úzko spätá so zodpovednosťou oboch subjektov (prevádzkovateľa, ako aj sprostredkovateľa) za škodu spôsobenú spracúvaním, ktoré je v rozpore s Nariadením. V súlade so zásadou zodpovednosti platí, že za súlad spracúvania s požiadavkami Nariadenia zodpovedá prevádzkovateľ. Prevádzkovateľ zodpovedá za súlad spracúvania s Nariadením aj v prípade, ak spracúvanie v jeho mene vykonáva sprostredkovateľ alebo ďalší sprostredkovateľ (sprostredkovateľ sprostredkovateľa). Sprostredkovateľ zodpovedá prevádzkovateľovi za plnenie povinností ďalšieho sprostredkovateľa (sprostredkovateľa sprostredkovateľa, tzv. subsprostredkovateľa). Sprostredkovateľ zodpovedá za škodu spôsobenú spracúvaním vykonávaným v rozpore s Nariadením iba v dvoch prípadoch. Prvým prípadom je situácia, ak sprostredkovateľ nesplnil povinnosť, ktorú mu Nariadenie výslovne ukladá. Druhým prípadom zodpovednosti sprostredkovateľa za škodu spôsobenú spracúvaním, ktoré je v rozpore s Nariadením je situácia, ak sprostredkovateľ konal nad rámec alebo v rozpore s pokynmi prevádzkovateľa za predpokladu, že tieto pokyny boli v súlade s Nariadením. V prípade, ak sprostredkovateľ poruší Nariadenie tým, že určí účely a prostriedky spracúvania, považuje sa v súvislosti s daným spracúvaním za prevádzkovateľa. Na vymedzenie deliacej čiary medzi zodpovednosťou prevádzkovateľa a zodpovednosťou sprostredkovateľa je preto potrebné, aby boli všetky pokyny prevádzkovateľa udelené sprostredkovateľovi jasné, presné, určité a zdokumentované. Odporúčame prevádzkovateľovi ubezpečiť sa, že sprostredkovateľ si je vedomý dôsledkov a sankcií, ktoré mu môžu byť uložené v prípade porušenia Nariadenia.

Ak sú pokyny prevádzkovateľa nejednoznačné, z pozície prevádzkovateľa bude ťažké preukázať a dokázať zodpovednosť sprostredkovateľa. K zodpovednosti prevádzkovateľa a sprostredkovateľa za škodu pozri bližšie článok 82. Povinnosť sprostredkovateľa spracúvať osobné údaje iba na základe zdokumentovaných pokynov prevádzkovateľa sa vzťahuje aj na prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii. Výnimku z povinnosti spracúvať osobné údaje len na základe zdokumentovaných pokynov prevádzkovateľa tvoria prípady, keď si to vyžaduje právo Únie alebo právo členského štátu, ktorému sprostredkovateľ podlieha (napr. poskytnúť osobné údaje orgánom činným v trestnom konaní). V takom prípade je sprostredkovateľ povinný oznámiť prevádzkovateľovi túto právnu požiadavku ešte pred spracúvaním, pokiaľ dané právo takéto oznámenie nezakazuje zo závažných dôvodov verejného záujmu (napr. v prípade, ak by oznámenie mohlo ohroziť alebo zmariť vyšetrovanie trestného činu).

Ďalšou povinnosťou sprostredkovateľa je povinnosť zaviesť všetky bezpečnostné opatrenia, ktorých vykonanie prevádzkovateľ v zmluve alebo v inom právnom akte vyžaduje. Prevádzkovateľ je oprávnený za účelom zabezpečenia primeranej úrovne bezpečnosti nariadiť sprostredkovateľovi, aby prijal konkrétne technické a organizačné opatrenia. Uvedené oprávnenie prevádzkovateľa nezbavuje samotného sprostredkovateľa povinnosti prijať so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb primerané technické a organizačné opatrenia, aby tak zaistil úroveň bezpečnosti primeranú tomuto riziku. K technickým a organizačným opatreniam pozri komentár k článku 24.

V praxi sa niekedy stáva, že sprostredkovateľ má silnejšiu pozíciu na trhu ako prevádzkovateľ, a teda prevádzkovateľ nemá takú silnú vyjednávaciu pozíciu v otázke nastavenia bezpečnostných opatrení. Ide o prípady „take it or leave it“, kedy je vzťah medzi prevádzkovateľom a sprostredkovateľom v značnej nerovnováhe, najmä v prípade rôznych cloudových, webových služieb alebo služieb poskytovaných prostredníctvom sociálnych sietí. Ani takáto situácia však neoprávňuje prevádzkovateľa prijať ustanovenia a podmienky spracúvania osobných údajov, ktoré nie sú v súlade s Nariadením. Prevádzkovateľ nie je oprávnený poveriť spracúvaním osobných údajov subjekt, ktorý nie

je schopný zabezpečiť úroveň bezpečnosti primeranú rizikám pre práva a slobody fyzických osôb, a ak tak urobí, nesie zodpovednosť za takéto svoje rozhodnutie. Nerovnováha postavenia „malého" prevádzkovateľa voči silnému sprostredkovateľovi nezbavuje prevádzkovateľa zodpovednosti za dodržiavanie Nariadenia.

Malá spoločnosť predávajúca detské oblečenie hľadá dopravcu na doručenie zásielok objednaných cez e-shop. Zo vzájomných obchodných rokovaní s medzinárodným dopravcom zistí, že tento dopravca spracúva osobné údaje prostredníctvom ďalšieho subjektu bez písomne uzatvorenej zmluvy (prípadne zistí, že dopravca uchováva osobné údaje príliš dlhú dobu). Napriek tomu, že dopravca poskytne spoločnosti najlepšiu cenovú ponuku na doručovanie zásielok, spoločnosť by si mala vybrať takého dopravcu, ktorý dodržiava pravidlá ochrany osobných údajov vyplývajúce z Nariadenia.

Veľmi významným a zároveň novým právom prevádzkovateľa voči sprostredkovateľovi je právo požadovať od sprostredkovateľa poskytnutie všetkých informácií, ktoré preukazujú splnenie sprostredkovateľových povinností, a za tým účelom vykonávať u sprostredkovateľa audity a kontroly. Cieľom tohto oprávnenia je zabezpečiť, aby si prevádzkovateľ mohol v realite overiť, či požiadavky, vrátane bezpečnostných opatrení, ktoré sú stanovené v zmluve alebo v inom právnom akte, sprostredkovateľ dodržiava. Toto právo má rovnako posilniť postavenie prevádzkovateľa v prípade, ak je v porovnaní so sprostredkovateľom slabšou zmluvnou stranou. Nariadenie pritom pripúšťa, aby audity a kontroly vykonával prevádzkovateľ alebo iný, prevádzkovateľom poverený audítor. Sprostredkovateľ je povinný zabezpečiť súčinnosť pri výkone auditov a kontrol a uvedeným spôsobom k nim prispievať.

Ďalšími povinnosťami sprostredkovateľa je povinnosť zabezpečiť, aby osoby, ktoré sú oprávnené spracúvať osobné údaje, boli povinné zachovávať dôvernosť informácií (či už na základe zmluvy, štatútu alebo iného právneho aktu). Niektorým profesiám vyplýva táto povinnosť priamo zo zákona, pri iných profesiách je sprostredkovateľ povinný zabezpečiť jej splnenie. Táto povinnosť sprostredkovateľa je úzko prepojená s bezpečnosťou spracúvania. Sprostredkovateľ je rovnako povinný dodržiavať podmienky pre zapojenie ďalšieho sprostredkovateľa stanovené v Nariadení (je oprávnený zapojiť ďalšieho sprostredkovateľa iba s predchádzajúcim písomným povolením prevádzkovateľa a na základe uzatvorenej zmluvy so sprostredkovateľom alebo iného právneho aktu podľa práva Únie alebo práva členského štátu) a na základe rozhodnutia prevádzkovateľa po ukončení spolupráce osobné údaje buď vymazať, alebo vrátiť prevádzkovateľovi a vymazať existujúce kópie, ak právo Únie alebo právo členského štátu nepožaduje uchovávanie týchto osobných údajov. Bezpečné vymazanie osobných údajov si vyžaduje buď zničenie, alebo demagnetizáciu pamäťového média, na ktorom sú osobné údaje uchovávané, alebo efektívne vymazanie osobných údajov ich prepísaním. Pri prepisovaní osobných údajov by sa mali používať osobitné softvérové nástroje, ktoré v súlade s uznávanými postupmi údaje viacnásobne prepíšu.[364)]

Sprostredkovateľ je povinný s prihliadnutím na povahu spracúvania a informácie dostupné sprostredkovateľovi pomáhať prevádzkovateľovi zabezpečiť plnenie povinnosti prijať vhodné technické a organizačné opatrenia, oznámiť porušenie ochrany osobných údajov dozornému orgánu, oznámiť porušenie ochrany osobných údajov dotknutej osobe a vykonať posúdenia vplyvu na ochranu údajov. Sprostredkovateľ je povinný bez zbytočného odkladu oznámiť prevádzkovateľovi porušenie ochrany osobných údajov. Podľa názoru WP29 nemusí sprostredkovateľ vyhodnocovať, či je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku, prípadne vysokému riziku pre práva a slobody fyzických osôb. To je povinnosťou prevádzkovateľa. Sprostredkovateľ musí mať zavedené procesy aby zistil, že došlo k porušeniu ochrany osobných údajov.[365)] V tejto súvislosti platí, že lehota na oznámenie porušenia dozornému orgánu, ako aj dotknutej osobe začína plynúť od momentu, odkedy sa o porušení dozvedel prevádzkovateľ. Do tejto lehoty sa nepočíta čas, po ktorý mal sprostredkovateľ vedomosť o porušení ochrany osobných údajov, avšak o tejto skutočnosti prevádzkovateľa ešte neinformoval. V prípade, 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, je sprostredkovateľ povinný pomáhať prevádzkovateľovi

364) Stanovisko WP29 č. 05/2012 ku cloud computingu (WP 196) prijaté 1. júla 2012, str. 13.

365) Usmernenie WP29 o oznámení porušenia ochrany osobných údajov podľa Nariadenia 679/2016 (WP250 rev.01) prijaté 3. októbra 2017, naposledy revidované a prijaté 6. februára 2018.

aj pri vykonaní posúdenia vplyvu na ochranu údajov, pretože ako subjekt vykonávajúci spracúvanie môže mať relevantné informácie potrebné na jeho vykonanie. Ak z posúdenia vplyvu vyplýva, že toto spracúvanie by viedlo k vysokému riziku, v prípade, ak by prevádzkovateľ neprijal opatrenia na jeho zmiernenie, je sprostredkovateľ povinný pomáhať prevádzkovateľovi aj v procese predchádzajúcej konzultácie. V uvedených prípadoch (pri vykonaní posúdenia vplyvu a prípadnej predchádzajúcej konzultácii) pomáha sprostredkovateľ prevádzkovateľovi s prihliadnutím na povahu spracúvania a informácie dostupné sprostredkovateľovi. Zmluva alebo iný právny akt musí tiež obsahovať povinnosť sprostredkovateľa po zohľadnení povahy spracúvania v čo najväčšej miere pomáhať prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti reagovať na žiadosti dotknutých osôb o výkon ich práv napr. pri uplatnení práva na prenosnosť údajov alebo práva na opravu.

V prípade, keď sa spracúvanie vykonáva prostredníctvom sprostredkovateľa, je potrebné, aby zmluva alebo iný právny akt obsahoval jasné rozdelenie povinností a presné nastavenie procesov pre ich výkon (napr. proces pre oznamovanie porušenia ochrany osobných údajov prevádzkovateľovi, proces súvisiaci s vybavovaním žiadostí dotknutých osôb o výkon ich práv).

Sprostredkovateľ v oblasti cloudových služieb

Prevádzkovateľ môže v zmluve delegovať určenie prostriedkov spracúvania na sprostredkovateľa, napr. v prípade cloudovej služby môže prevádzkovateľ (zákazník cloudovej služby) poveriť poskytovateľa tejto služby (sprostredkovateľa) výberom metód, ktoré sa použijú na dosiahnutie sledovaného cieľa prevádzkovateľa.

WP29 vo svojom stanovisku ku cloud computingu prijatom pred nadobudnutím účinnosti Nariadenia uviedla, že „v zmluve uzatvorenej medzi zákazníkom cloudovej služby (prevádzkovateľom) a poskytovateľom tejto služby (sprostredkovateľom) sa musí minimálne stanovovať, že sprostredkovateľ musí plniť pokyny prevádzkovateľa a zaviesť technické a organizačné opatrenia na účely primeranej ochrany osobných údajov. Na zaistenie právnej istoty by mali byť v zmluve stanovené:

1. Podrobnosti (rozsah a modality) o pokynoch, ktoré zákazník (t. j. prevádzkovateľ) udelí poskytovateľovi cloudovej služby (t. j. sprostredkovateľovi), najmä pokiaľ ide o uplatniteľné dohody o úrovni služieb (ktoré by mali byť objektívne a merateľné) a príslušné sankcie (finančné alebo iné vrátane možnosti žalovať poskytovateľa v prípade nedodržania zmluvy).
2. Špecifikácia bezpečnostných opatrení, ktoré musí poskytovateľ cloudovej služby dodržiavať v závislosti od rizík, ktoré prináša spracúvanie údajov, a povahy údajov, ktoré je potrebné chrániť. Je veľmi dôležité, aby boli špecifikované konkrétne technické a organizačné opatrenia. To platí bez toho, aby bola dotknutá možnosť uplatnenia prípadných prísnejších opatrení, ktoré môžu byť požadované vo vnútroštátnych právnych predpisoch vzťahujúcich sa na zákazníka.
3. Predmet a časový rámec cloudovej služby poskytovanej poskytovateľom cloudu, rozsah, spôsob a účel spracovania osobných údajov týmto poskytovateľom, ako aj typy spracovávaných osobných údajov.
4. Špecifikácia podmienok pre navrátenie (osobných) údajov alebo zničenie údajov po ukončení poskytovania služby. Okrem toho musí byť zaistené bezpečné vymazanie osobných údajov na požiadanie zákazníka cloudovej služby.
5. Zahrnutie ustanovenia o zachovávaní dôvernosti, ktoré bude záväzné pre poskytovateľa cloudovej služby a všetkých jeho zamestnancov, ktorí budú mať prístup k údajom. Prístup k údajom môžu mať iba oprávnené osoby.
6. Povinnosť poskytovateľa poskytovať zákazníkovi podporu pri uľahčovaní výkonu práv dotknutých osôb na prístup, opravu alebo vymazanie ich údajov.
7. V zmluve by malo byť výslovne stanovené, že poskytovateľ cloudovej služby nesmie poskytovať údaje tretím stranám, a to ani na účely uchovávania, pokiaľ nie je v zmluve stanovené, že sa budú využívať služby subdodávateľov. V zmluve by malo byť uvedené, že subsprostredkovatelia môžu byť zapojení iba na základe súhlasu, ktorý môže vo všeobecnosti udeliť prevádzkovateľ. Sprostredkovateľ je povinný informovať prevádzkovateľa o akýchkoľvek plánovaných zmenách v tejto súvislosti a prevádzkovateľ má neustále možnosť namietať voči týmto zmenám alebo ukončiť zmluvu. Poskytovateľ cloudovej služby by mal mať jasnú povinnosť uviesť všetkých

zapojených subdodávateľov (napr. vo verejnom digitálnom registri). Je nutné zabezpečiť, aby zmluvy uzatvorené medzi poskytovateľom cloudovej služby a subdodávateľom odrážali požiadavky uvedené v zmluve uzatvorenej medzi zákazníkom a poskytovateľom cloudovej služby (t. j. že na subsprostredkovateľov sa uplatňujú tie isté zmluvné povinnosti ako na poskytovateľa cloudovej služby). Predovšetkým je potrebné zaručiť, aby poskytovateľ cloudovej služby a všetci subdodávatelia konali len na základe pokynov zákazníka cloudovej služby. V zmluve by mal byť jasne stanovený reťazec zodpovednosti. Mala by tu byť stanovená povinnosť pre sprostredkovateľa vytvoriť rámec pre medzinárodné prenosy údajov, napríklad podpísaním zmlúv so subsprostredkovateľmi, ktoré by vychádzali zo štandardných zmluvných doložiek podľa rozhodnutia 2010/87/EÚ. Len pre úplnosť si dovoľujeme doplniť, že rozhodnutie 2010/87/EÚ je predmetom sporu vedeného pred Súdnym dvorom EÚ vo veci C-311/18 – Komisár pre ochranu údajov/Facebook Ireland a Maximillian Schrems, v ktorom pán M. Schrems navrhuje rozhodnúť, že predmetné rozhodnutie Komisie je neplatné. K meritu veci sa vyjadroval Generálny advokát Saugmandsgaard Øe, podľa ktorého pri preskúmaní otázok nevyšli najavo žiadne skutočnosti, ktoré by mohli mať vplyv na platnosť napádaného rozhodnutia; vec zatiaľ nie je ukončená.

8. Spresnenie zodpovednosti poskytovateľa cloudovej služby oznámiť zákazníkovi tejto služby akékoľvek porušenie ochrany údajov, ktoré by sa dotýkalo údajov zákazníka cloudovej služby.
9. Povinnosť poskytovateľa cloudovej služby poskytnúť zoznam miest, na ktorých môžu byť údaje spracúvané.
10. Právo prevádzkovateľa monitorovať a zodpovedajúca povinnosť poskytovateľa cloudovej služby spolupracovať.
11. V zmluve by malo byť zakotvené, že poskytovateľ cloudovej služby musí informovať zákazníka o relevantných zmenách týkajúcich sa predmetnej cloudovej služby, ako je zavedenie dodatočných funkcií.
12. V zmluve by malo by ustanovenie o protokolovaní a auditovaní príslušných operácií spracovania osobných údajov, ktoré vykonáva poskytovateľ cloudovej služby alebo subdodávatelia.
13. Oznámenie zo strany zákazníka cloudovej služby akejkoľvek právne záväznej žiadosti o sprístupnenie osobných údajov podanej zo strany orgánu presadzovania práva, pokiaľ to nie je inak zakázané, napríklad trestným právom, v záujme zachovania dôvernosti vyšetrovania v rámci presadzovania práva.
14. Všeobecná povinnosť prevádzkovateľa poskytnúť uistenie, že interná organizácia a opatrenia na spracovanie údajov (ako aj opatrenia jeho subsprostredkovateľov, ak sú zapojení) sú v súlade s platnými vnútroštátnymi a medzinárodnými právnymi požiadavkami a normami.“[366)]

Zo znenia článkov 28 ods. 2 a 3 Nariadenia upravujúceho vzťah medzi sprostredkovateľom a prevádzkovateľom vyplýva, že väčšinu týchto odporúčaní WP29 predstavujú povinné minimálne požiadavky zmluvy uzatvorenej medzi prevádzkovateľom a sprostredkovateľom alebo iného právneho aktu podľa práva Únie alebo práva členského štátu zaväzujúceho sprostredkovateľa voči prevádzkovateľovi.

Okrem horeuvedených povinností, ktoré je potrebné v zmluve alebo v inom právnom akte stanoviť, je potrebné si uvedomiť, že Nariadenie výslovne ukladá sprostredkovateľovi aj ďalšie povinnosti, a to napr. povinnosť viesť záznamy o všetkých kategóriách spracovateľských činností, ak sa na sprostredkovateľa nevzťahuje výnimka podľa článku 30 ods. 5, povinnosť spolupracovať s dozorným úradom (článok 31), povinnosť prijať primerané technické a organizačné opatrenia (článok 32), povinnosť oznámiť prevádzkovateľovi porušenie ochrany osobných údajov (článok 33), povinnosť určiť zodpovednú osobu v prípade splnenia podmienok pre jej povinné určenie (článok 37), povinnosť dodržiavať schválený kódex správania, ak sa sprostredkovateľ rozhodol uplatňovať ho, povinnosť dodržiavať sprostredkovateľovi vydaný certifikát, pečať alebo značku ochrany údajov, povinnosť písomne určiť zástupcu v Únii, ak sa uplatňuje článok 3 ods. 2 Nariadenia (článok 27).

Pre prípad možnej kontroly odporúčame sprostredkovateľovi aj prevádzkovateľovi uchovávať najmä zdokumentované pokyny prevádzkovateľa, zmluvu alebo iný právny akt zaväzujúci sprostredkovateľa voči prevádzkovateľovi, písomné povolenie na zapojenie ďalšieho sprostredkovateľa,

366) Stanovisko WP29 č. 05/2012 ku cloud computingu (WP 196) prijaté 1. júla 2012.

zmluvu uzatvorenú medzi sprostredkovateľom a ďalším sprostredkovateľom, ako aj všetky dokumenty, resp. dôkazy preukazujúce splnenie sprostredkovateľových povinností.

K ods. 4

Nariadenie umožňuje reťazenie sprostredkovateľov. Pôvodný sprostredkovateľ (t. j. sprostredkovateľ, ktorý uzatvoril zmluvu s prevádzkovateľom alebo vykonáva spracúvanie osobných údajov v mene prevádzkovateľa na základe iného právneho aktu podľa práva Únie alebo práva členského štátu) je oprávnený zapojiť do spracúvania ďalšieho sprostredkovateľa iba na základe predchádzajúceho písomného povolenia prevádzkovateľa. K povoleniu pozri bližšie komentár k odseku 2. Ďalší sprostredkovateľ vykonáva spracúvanie osobných údajov v mene prevádzkovateľa, a to buď na základe zmluvy uzatvorenej so sprostredkovateľom alebo iného právneho aktu podľa práva Únie alebo práva členského štátu (k týmto pojmom pozri komentár k ods. 3). Nariadenie vyžaduje, aby zmluva alebo iný právny akt ukladal ďalšiemu sprostredkovateľovi v súvislosti s ochranou osobných údajov rovnaké povinnosti, aké boli uložené sprostredkovateľovi zo strany prevádzkovateľa (ak je napríklad sprostredkovateľ povinný šifrovať osobné údaje, táto povinnosť musí byť preklopená aj na ďalšieho sprostredkovateľa). To isté platí aj vo vzťahu k preukázaniu dostatočných záruk. Ako sme už uviedli, cieľom tejto úpravy je nezničovať úroveň ochrany dotknutých osôb v prípade, ak sa spracúvanie vykonáva prostredníctvom sprostredkovateľa, prípadne ďalšieho sprostredkovateľa.

Na vzájomný vzťah medzi sprostredkovateľom a ďalším sprostredkovateľom sa obdobne použijú ustanovenia upravujúce vzťah medzi prevádzkovateľom a sprostredkovateľom, teda spracúvanie osobných údajov sa má vykonávať v súlade s požiadavkami Nariadenia bez ohľadu na to, či osobné údaje spracúva prevádzkovateľ, sprostredkovateľ alebo ďalší sprostredkovateľ. Pokyny sprostredkovateľa udelené ďalšiemu sprostredkovateľovi musia byť v súlade s pokynmi, ktoré udelil sprostredkovateľovi prevádzkovateľ.

V prípade, keď sprostredkovateľ zapojí do spracúvania ďalšieho sprostredkovateľa, je potrebné, aby zmluva alebo iný právny akt obsahoval jasné rozdelenie povinností medzi sprostredkovateľom a ďalším sprostredkovateľom a presné nastavenie procesov pre ich výkon (napr. proces pre oznamovanie porušenia ochrany osobných údajov, proces súvisiaci s vybavovaním žiadostí dotknutých osôb o výkon ich práv). Ak ďalší sprostredkovateľ nesplní svoje povinnosti, voči prevádzkovateľovi zostáva za plnenie povinností ďalšieho sprostredkovateľa plne zodpovedný pôvodný sprostredkovateľ.

Pre prípad možnej kontroly odporúčame v súvislosti so spracúvaním osobných údajov ďalším sprostredkovateľom uchovávať popri dokumentácii uvedenej v závere k ods. 3 vyššie aj písomné povolenie na zapojenie ďalšieho sprostredkovateľa, zmluvu uzatvorenú medzi sprostredkovateľom a ďalším sprostredkovateľom alebo iný právny akt podľa práva Únie alebo práva členského štátu, ako aj všetky dokumenty, resp. dôkazy preukazujúce splnenie sprostredkovateľových povinností (pôvodného aj ďalšieho sprostredkovateľa). Na ďalšieho sprostredkovateľa sa v plnom rozsahu vzťahujú správne pokuty uvedené v Nariadení pre sprostredkovateľa, ako aj príslušné ustanovenia o zodpovednosti za škodu (článok 82).

K ods. 5

Nariadenie stanovuje, že jedným zo spôsobov preukázania dostatočných záruk v procese výberu sprostredkovateľa, ako aj ďalšieho sprostredkovateľa je dodržiavanie schváleného kódexu správania alebo vydaného certifikátu. Ku kódexom správania pozri bližšie komentár k článku 40 a 41, k certifikátom článok 42 a 43.

Ďalším spôsobom preukázania dostatočných záruk môže byť určenie zodpovednej osoby v prípade, ak nejde o prípady obligatórne určenej zodpovednej osoby, checklist s požiadavkami týkajúcimi sa ochrany osobných údajov a bezpečnosti, vykonanie due dilligence preukazujúceho, že sprostredkovateľ a/alebo ďalší sprostredkovateľ poskytuje dostatočné záruky, platné certifikáty zamerané na riadenie informačnej bezpečnosti v organizáciách udelené sprostredkovateľovi a/alebo ďalšiemu sprostredkovateľovi (certifikácia systému manažérstva informačnej bezpečnosti podľa ISO/IEC 27001). V závislosti od konkrétneho spracúvania sa môže vyžadovať aj ich kombinácia.

K ods. 6, 7, 8 a 9

Zmluva alebo iný právny akt podľa práva Únie alebo práva členského štátu upravujúci vzťah medzi prevádzkovateľom a sprostredkovateľom, ako aj vzťah medzi sprostredkovateľom a ďalším sprostredkovateľom musia byť vypracované v písomnej alebo elektronickej podobe.

Prevádzkovateľ a sprostredkovateľ alebo sprostredkovateľ a ďalší sprostredkovateľ si môžu zvoliť jednu z týchto foriem dotknutých právnych úkonov, avšak vždy tak, aby existovali dôkazné prostriedky o ich minimálnych obsahových náležitostiach podľa ods. 3 a podľa základných požiadaviek kladených na právne úkony v zmysle ust. § 34 a nasl. Občianskeho zákonníka. Zdôrazňujeme však, že poverenie sprostredkovateľa na zapojenie ďalšieho sprostredkovateľa do spracúvania v mene prevádzkovateľa musí byť realizované v písomnej forme.

Ako sme už uviedli v zmysle § 40 ods. 4 Občianskeho zákonníka, písomná forma je zachovaná, ak je právny úkon urobený telegraficky, ďalekopisom alebo elektronickými prostriedkami, ktoré umožňujú zachytenie obsahu právneho úkonu a určenie osoby, ktorá právny úkon urobila. Písomná forma je zachovaná vždy, ak právny úkon urobený elektronickými prostriedkami je podpísaný zaručeným elektronickým podpisom alebo zaručenou elektronickou pečaťou.

Na riadenie vzťahu medzi prevádzkovateľom a sprostredkovateľom alebo sprostredkovateľom a ďalším sprostredkovateľom sa môžu úplne alebo sčasti použiť štandardné zmluvné doložky, ktoré stanoví priamo Komisia alebo prijme dozorný orgán v súlade s mechanizmom konzistentnosti.

Komisia zatiaľ vydala štandardné zmluvné doložky týkajúce sa prenosov osobných údajov do tretích krajín a medzinárodným organizáciám [bližšie v komentári k čl. 46 ods. 2 písm. c) Nariadenia].[367)]

Vo vzťahu k dozornému orgánu dávame do pozornosti štandardné zmluvné doložky upravujúce vzťah medzi sprostredkovateľom a prevádzkovateľom, ktoré predložil v súlade s mechanizmom konzistentnosti dánsky dozorný orgán. Jednotlivé dokumenty nájdete na stránke Výboru https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-142019-draft-standard-contractual-clauses_en.

K ods. 10

Sprostredkovateľ je oprávnený spracúvať osobné údaje v mene prevádzkovateľa iba na základe zmluvy alebo iného právneho aktu podľa práva Únie alebo práva členského štátu zaväzujúceho sprostredkovateľa voči prevádzkovateľovi, a to iba v súlade so stanoveným účelom spracúvania. Sprostredkovateľ musí spracúvať osobné údaje len na základe pokynov prevádzkovateľa, ktoré musia byť zdokumentované. V prípade, ak sprostredkovateľ poruší Nariadenie tým, že určí účely a prostriedky spracúvania, napr. rozšíri alebo zmení účel spracúvania, považuje sa v súvislosti s daným spracúvaním sám za prevádzkovateľa. V takom prípade sa na neho v plnom rozsahu aplikujú všetky ustanovenia, resp. povinnosti Nariadenia vzťahujúce sa na prevádzkovateľa.

Z judikatúry:

Rozsudok Súdneho dvora EÚ z 22. novembra 2012 vo veci C-119/12 Josef Probst

2 Tento návrh bol podaný v rámci sporu medzi spoločnosťou mr.nexnet GmbH (ďalej len „nexnet), ktorá je postupníčkou pohľadávok vyplývajúcich z poskytovania služieb prístupu k internetu spoločnosťou Verizon Deutschland GmbH (ďalej len „Verizon“), a pánom Probstom, príjemcom uvedených služieb.

8 článok 6 smernice 2002/58 stanovuje:

„1. Prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*] týkajúce sa účastníkov a užívateľov, spracovávané a uložené poskytovateľom verejnej komunikačnej siete alebo verejne dostupnej elektronickej komunikačnej služby, sa musia vymazať alebo zanonymniť, ak už naďalej nie sú potrebné na účely prenosu správy, bez vplyvu na odseky 2, 3 a 5 tohto článku…

367) Rozhodnutie Komisie z 15. júna 2001 o štandardných zmluvných doložkách na prenos osobných údajov do tretích krajín podľa smernice 95/46/ES, 2001/497/ES.
Rozhodnutie Komisie z 27. decembra 2004, ktorým sa mení a dopĺňa rozhodnutie 2001/497/ES o zavedení alternatívneho súboru o štandardných zmluvných doložkách na prenos osobných údajov do tretích krajín, 2004/915/ES.
Rozhodnutie Komisie z 5. februára 2010 o štandardných zmluvných doložkách pre prenos osobných údajov spracovateľom usadeným v tretích krajinách podľa smernice Európskeho parlamentu a Rady 95/46/ES, 2010/87/EÚ.

2. Prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*] potrebné na účely fakturácie účastníka a platby za spojenie sa môžu spracovávať. Také spracovanie je povolené len do konca obdobia, počas ktorého môže byť faktúra právne napadnutá alebo sa môže uplatniť nárok na platbu.

...

5. Spracovávanie prevádzkových dát [údajov o prenose dát – *neoficiálny preklad*], v súlade s odsekmi 1, 2, 3 a 4, sa musí obmedziť na osoby konajúce na pokyn poskytovateľa verejných komunikačných sietí a verejne dostupných elektronických komunikačných služieb, ktoré sú zodpovedné za fakturovanie alebo riadenie prevádzky, vybavovanie dotazov zákazníkov, odhaľovanie podvodov, marketing elektronických komunikačných služieb alebo poskytovanie služby s pridanou hodnotou, a musí sa obmedziť na to, čo je nevyhnutné na účely takých činností.

..."

11 Pán Probst má telefónnu prípojku od Deutsche Telekom AG, cez ktorú je jeho počítač pripojený na internet. V období od 28. júna do 6. septembra 2009 používal telefónne číslo, ktoré mu poskytla spoločnosť Verizon, na získanie jednorazového prístupu na internet. Najprv Deutsche Telekom AG za tieto pripojenia vyúčtovala pánovi Probstovi poplatky pod názvom „poplatky iných poskytovateľov". V dôsledku nezaplatenia pánom Probstom týchto poplatkov spoločnosť nexnet, postupníčka tejto pohľadávky na základe faktoringovej zmluvy, ktorú uzavreli právni predchodcovia spoločností Verizon a nexnet, od neho požadovala zaplatenie vyúčtovaných súm zvýšených o rôzne výdavky. V súlade s faktoringovou zmluvou spoločnosť nexnet znáša riziko, že sa jej ich nepodarí vymôcť.

15 Za týchto okolností Bundesgerichtshof rozhodol prerušiť konanie a položiť Súdnemu dvoru túto prejudiciálnu otázku:

„Umožňuje článok 6 ods. 2 a 5 smernice 2002/58/ES poskytovateľovi služieb preniesť údaje o prenose dát na postupníka nadobúdajúceho pohľadávku vyplývajúcu z odmeny za telekomunikačné služby, ak je postúpenie uskutočnené na účel vymáhania spätne postúpených pohľadávok, okrem všeobecnej povinnosti zachovávať telekomunikačné tajomstvo a ochranu údajov v zmysle platnej zákonnej úpravy, založené na nasledujúcich zmluvných podmienkach:

– poskytovateľ služieb a postupník sa zaviažu spracovávať a používať chránené údaje iba v rámci ich spolupráce a výlučne na cieľ sledovaný touto zmluvou a spôsobom, ktorý sa v nej uvádza,
– len čo už chránené údaje nebudú potrebné na spĺňanie tohto cieľa, všetky údaje získané v tejto súvislosti musia byť nenávratne vymazané alebo vrátené,
– zmluvné strany sú oprávnené kontrolovať dodržiavanie ochrany a bezpečnosti údajov druhou zmluvnou stranou v zmysle tejto dohody,
– odovzdané dôverné dokumenty a informácie môžu byť sprístupnené iba tým zamestnancom, ktorí ich potrebujú na plnenie zmluvy,
– zmluvné strany zaviažu svojich zamestnancov na zachovávanie dôvernosti, tak ako je to uvedené v tejto dohode,
– na žiadosť niektorej zo zmluvných strán alebo najneskôr pri ukončení ich spolupráce musia byť všetky dôverné informácie, ktoré boli v tejto súvislosti získané, nenávratne vymazané alebo vrátené druhej zmluvnej strane?"

16 Svojou otázkou sa vnútroštátny súd v podstate pýta, či a za akých podmienok umožňuje článok 6 ods. 2 a 5 smernice 2002/58 poskytovateľovi služieb preniesť údaje o prenose dát na postupníka, na ktorého postúpil svoje pohľadávky, a tomuto postupníkovi spracovávať uvedené údaje.

19 Z celkového znenia ustanovení smernice 2002/58 vyplýva, že poskytovateľ služieb môže preniesť údaje o prenose dát na postupníka, na ktorého postúpil svoje pohľadávky na ich vymáhanie, a ten ich môže spracovávať pod podmienkou, že jednak uvedené údaje spracováva „na pokyn" poskytovateľa služieb a jednak spracováva len údaje o prenose dát, ktoré sú nevyhnutné na vymáhanie uvedených pohľadávok.

20 Treba konštatovať, že ani smernica 2002/58, ani dokumenty relevantné pre jej výklad, akými sú *travaux préparatoires*, neposkytujú vysvetlenia presného dosahu pojmu „na pokyn". Za týchto okolností v súlade s judikatúrou Súdneho dvora sa význam tohto pojmu musí určiť podľa jeho obvyklého významu v bežnom jazyku, pričom sa zároveň zohľadnia súvislosti, v ktorých sa používa, ako aj účel sledovaný právnou úpravou, v ktorej sa nachádza (pozri v tomto zmysle rozsudky z 10. marca 2005, easyCar, C-336/03, Zb. s. I-1947, body 20 a 21, ako aj z 5. júla 2012, Content Services, C-49/11, bod 32).

21 Pokiaľ ide o obvyklý význam tohto pojmu v bežnom jazyku, treba sa domnievať, že osoba koná na pokyn inej osoby vtedy, keď prvá osoba koná na základe pokynov a pod dohľadom druhej osoby.

23 Článok 6 ods. 2 a 5 smernice 2002/58 obsahuje výnimku z povinnosti zabezpečiť dôvernosť správ stanovenej v článku 5 ods. 1 tejto smernice tým, že povoľuje spracovávať údaje o prenose dát v súvislosti

s požiadavkami spojenými s činnosťami fakturácie služieb (pozri v tomto zmysle rozsudok z 29. januára 2008, Promusicae, C-275/06, Zb. s. I-271, bod 48). Keďže ide o výnimku, toto ustanovenie smernice, a teda aj pojem „na pokyn", treba vykladať doslovne [pozri rozsudok zo 17. februára 2011, The Number (UK) a Conduit Enterprises, C-16/10, Zb. s. I-691, bod 31]. Takýto výklad znamená, že poskytovateľ služieb musí mať možnosť vykonávať účinný dohľad, ktorý mu umožňuje overiť, či postupník pohľadávok dodržiava povinnosti, ktoré má pri spracovaní údajov o prenose dát.

27 Z vyššie uvedeného vyplýva, že bez ohľadu na kvalifikáciu zmluvy o postúpení pohľadávok na účely ich vymáhania koná postupník pohľadávky vyplývajúcej z poskytovania telekomunikačných služieb „na pokyn" poskytovateľa uvedených služieb v zmysle článku 6 ods. 5 smernice 2002/58, ak pri spracovaní údajov o prenose dát, ktoré taká činnosť zahŕňa, koná tento postupník len na základe pokynov a pod dohľadom daného poskytovateľa. Zmluva uzavretá medzi poskytovateľom služieb, ktorý postupuje svoje pohľadávky, a postupníkom týchto pohľadávok musí najmä obsahovať ustanovenia, ktoré zabezpečujú, že postupník bude spracovávať údaje o prenose dát v súlade so zákonom, a umožňujú poskytovateľovi služieb kedykoľvek sa ubezpečiť, či postupník dodržiava tieto ustanovenia.

29 So zreteľom na predchádzajúce úvahy treba na položenú otázku odpovedať tak, že článok 6 ods. 2 a 5 smernice 2002/58 sa má vykladať v tom zmysle, že poskytovateľovi služieb umožňuje preniesť údaje o prenose dát na postupníka, na ktorého postúpil svoje pohľadávky vyplývajúce z poskytovania telekomunikačných služieb na ich vymáhanie, pričom tento postupník môže dané údaje spracovávať pod podmienkou, že ich jednak spracováva na pokyn poskytovateľa služieb a jednak spracováva len údaje o prenose dát, ktoré sú nevyhnutné na vymáhanie postúpených pohľadávok.

30 Bez ohľadu na kvalifikáciu zmluvy o postúpení pohľadávok sa má postupník považovať za osobu konajúcu na pokyn poskytovateľa služieb v zmysle článku 6 ods. 5 smernice 2002/58, ak pri spracovaní údajov o prenose dát koná len na základe pokynov a pod dohľadom daného poskytovateľa. Zmluva uzavretá medzi nimi musí najmä obsahovať ustanovenia, ktoré zabezpečujú, že údaje o prenose dát budú spracovávané v súlade so zákonom, a umožňujú poskytovateľovi služieb kedykoľvek sa ubezpečiť, že postupník dodržiava tieto ustanovenia.

Článok 29

Spracúvanie na základe poverenia prevádzkovateľa alebo sprostredkovateľa

Sprostredkovateľ a každá osoba konajúca na základe poverenia prevádzkovateľa alebo sprostredkovateľa, ktorá má prístup k osobným údajom, môže spracúvať tieto údaje len na základe pokynov prevádzkovateľa s výnimkou prípadov, keď sa to vyžaduje podľa práva Únie alebo práva členského štátu.

Súvisiace ustanovenia: recitál 29, články 83 a 84

Súvisiace predpisy: článok 16 Smernice o ochrane osobných údajov, nový zákon o ochrane osobných údajov

---

Komentár k článku 29

Recitál 29: Prevádzkovateľ, ktorý spracúva osobné údaje, by mal určiť oprávnené osoby v rámci toho istého prevádzkovateľa.

Doterajšia úprava obsiahnutá v Smernici o ochrane osobných údajov obsahovala, čo sa týka významu, obdobné ustanovenie v článku 16, v zmysle ktorého nesmela akákoľvek osoba konajúca v právomoci prevádzkovateľa alebo sprostredkovateľa, vrátane samotného sprostredkovateľa, ktorá mala prístup k osobným údajom, tieto údaje spracovať, s výnimkou toho, ak konala na základe pokynu prevádzkovateľa alebo v prípadoch, keď sa to vyžadovalo v zmysle zákona. Smernica o ochrane osobných údajov ďalej v článku 17 obsahovala povinnosť sprostredkovateľa konať na základe pokynov prevádzkovateľa.

Zákon č. 122/2013 Z. z. v časti týkajúcej sa bezpečnosti osobných údajov zakotvil povinnosť prevádzkovateľa aj sprostredkovateľa[368)] poučiť oprávnenú osobu o jej právach a povinnostiach pri spracúvaní osobných údajov. Pod oprávnenou osobou pritom rozumel iba fyzickú osobu, ktorá prichádzala

368) § 21 a § 8 ods. 8 zákona č. 122/2013 Z. z.

do styku s osobnými údajmi dotknutých osôb, a to v rámci svojho pracovnoprávneho vzťahu, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie, a ktorá zároveň spracúvala osobné údaje v rozsahu a spôsobom určeným v poučení. Za oprávnenú osobu sa tak podľa zákona č. 122/2013 Z. z. považovala napr. zamestnankyňa oddelenia HR, interná mzdová účtovníčka alebo personalistka, administratívny pracovník vybavujúci objednávky prijaté prostredníctvom e-shopu, administratívny pracovník vybavujúci sťažnosti a reklamácie fyzických osôb, zamestnanec majúci na základe svojej pracovnej pozície prístup do klientskeho informačného systému, a to ak spracúval osobné údaje v rozsahu a spôsobom určeným v poučení.

Nariadenie pracuje s pojmom oprávnená osoba iba v recitáli, a to konkrétne v recitáli 29, v ktorom stanovuje, že každý prevádzkovateľ, ktorý spracúva osobné údaje, by mal určiť oprávnené osoby v rámci toho istého prevádzkovateľa. Ustanovenie spomínaného recitálu pokrýva iba časť prípadov, ktoré spadajú pod úpravu uvedenú v článku 29.

Predmetné ustanovenie Nariadenia ukladá sprostredkovateľovi a každej osobe, ktorá koná na základe poverenia prevádzkovateľa alebo sprostredkovateľa a má súčasne k osobným údajom dotknutých osôb prístup, povinnosť spracúvať tieto údaje iba na základe pokynov prevádzkovateľa. Výnimku tvoria prípady, ak sa to vyžaduje podľa práva Únie alebo práva členského štátu. Pokyny prevádzkovateľa na spracúvanie osobných údajov by mali obsahovať najmä vymedzenie osobných údajov, ku ktorým má mať konkrétna osoba prístup na účel plnenia jej povinností alebo úloh, určenie postupov, ktoré je poverená osoba povinná uplatňovať pri spracúvaní osobných údajov, vymedzenie základných postupov alebo operácií s osobnými údajmi, ako aj vymedzenie zodpovednosti za porušenie Nariadenia alebo iných právnych predpisov. Uvedená povinnosť sprostredkovateľa a každej osoby konajúcej na základe poverenia od prevádzkovateľa alebo sprostredkovateľa a majúcej prístup k osobným údajom spracúvať osobné údaje výlučne na základe pokynov prevádzkovateľa veľmi úzko súvisí s povinnosťou prevádzkovateľa a sprostredkovateľa prijať primerané bezpečnostné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú riziku spracúvania. Pokyny musia byť poverenej osobe dané pred tým, ako uskutočnení prvú spracovateľskú operáciu s osobnými údajmi. V tomto smere je irelevantné, či sa samotný dokument bude nazývať poučenie alebo pokyny, posudzovaný bude z hľadiska jeho obsahu. Ide o organizačné opatrenie, bez ktorého by ani akékoľvek technické bezpečnostné opatrenie neviedlo k efektívnej a účinnej ochrane osobných údajov fyzických osôb. Cieľom tejto úpravy je predovšetkým minimalizovať riziko nezákonného alebo neoprávneného spracúvania osobných údajov.

Povinnosť spracúvať osobné údaje výlučne na základe pokynov prevádzkovateľa sa vzťahuje na sprostredkovateľa, zamestnancov prevádzkovateľa a sprostredkovateľa, ako aj na ďalšie osoby, ktoré pristupujú k osobným údajov na základe poverenia prevádzkovateľa alebo sprostredkovateľa. Poverenie prevádzkovateľa alebo sprostredkovateľa môže vyplývať z pracovnoprávneho vzťahu, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, ako aj zo zvolenia, vymenovania do funkcie, zo zmluvy uzatvorenej s prevádzkovateľom alebo sprostredkovateľom a pod. Je rovnako bezpredmetné, či je osoba v pracovnom pomere na základe pracovnej zmluvy alebo dohody o práci vykonávanej mimo pracovného pomeru. Nariadenie pritom nevyžaduje, aby malo poverenie prevádzkovateľa alebo sprostredkovateľa písomnú formu. Rovnako pre platnosť pokynu nevyžaduje jeho písomnú formu. V súlade so zásadou zodpovednosti, ako aj vzhľadom na dôkazné bremeno prevádzkovateľa (či už voči dozornému orgánu alebo voči súdu) je však žiaduce, aby boli pokyny zdokumentované či už v písomnej, alebo inej forme.

Autori tohto komentára odporúčajú, aby pokyny obsahovali poučenie osoby (sprostredkovateľa a každej osoby, ktorá koná na základe poverenia prevádzkovateľa alebo sprostredkovateľa a má súčasne k osobným údajom dotknutých osôb prístup) o jej právach a povinnostiach v súvislosti so spracúvaním osobných údajov, o jej zodpovednosti za porušenie uvedených povinností, aby určovali postupy, ktoré je osoba povinná uplatňovať pri spracúvaní osobných údajov, vymedzovali zakázané postupy a operácie s osobnými údajmi a vymedzovali osobné údaje, ku ktorým má mať konkrétna osoba prístup za účelom plnenia svojich povinností vyplývajúcich z poverenia prevádzkovateľa alebo sprostredkovateľa.