

DÔVODOVÁ SPRÁVA

B. Osobitná časť

K § 1

Upravuje sa vecná pôsobnosť zákona. Tento zákon sa vzťahuje na spracúvanie osobných údajov pri plnení úloh Policajného zboru, Vojenskej polície, Zboru väzenskej a justičnej stráže, finančnej správy, Ministerstva spravodlivosti Slovenskej republiky, Kancelárie prezidenta Slovenskej republiky, prokuratúry a súdov (ďalej len „príslušný orgán“) na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií, vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu. Spracúvanie osobných údajov je súčasťou stíhania trestných činov.

Ochrana fyzických osôb musí byť technologicky neutrálna a nesmie závisieť od použitých technologických riešení. Ochrana fyzických osôb sa vzťahuje na spracúvanie osobných údajov automatizovanými prostriedkami, ako aj na manuálne spracúvanie, ak sú osobné údaje uložené v informačnom systéme alebo do neho majú byť uložené. Súbory alebo zbierky súborov, ako aj ich titulné strany, ktoré nie sú štruktúrované podľa špecifických kritérií, by nemali patriť do rozsahu pôsobnosti tohto zákona.

K § 2

Vymedzujú sa základné pojmy a definuje sa ich význam na účel tohto zákona.

Ustanovenie poskytuje definíciu osobného údajá. Zákon neupravuje konkrétny výpočet údajov, ktoré sú považované za osobné údaje. Poskytuje tzv. demonštratívny výpočet charakteristík určujúcich fyzickú osobu. Uvedená definícia osobných údajov nevyžaduje, aby išlo o konkrétnu identitu fyzickej osoby, ale postačuje, aby za splnenia daných podmienok bola osoba identifikovateľná. Z vecnej stránky sa pojem osobných údajov vzťahuje na také údaje, ktoré sa týkajú identifikovanej alebo identifikovateľnej fyzickej osoby, t. j. určenej alebo určiteľnej, či už priamo alebo nepriamo. Z pohľadu ochrany osobných údajov sa „určiteľnosťou fyzickej osoby“ rozumie taký stav, keď na základe jedného alebo viacerých dostupných údajov o danej osobe možno túto osobu identifikovať.

Identifikácia sa realizuje prostredníctvom konkrétnych charakteristických znakov, t. j. „identifikátorov“, ktoré možno priradiť ku konkrétnej fyzickej osobe (napr.: meno, priezvisko, tetovanie, zdravotné postihnutie, dátum narodenia, adresa a iné). Miera, do akej sú určité identifikátory dostačujúce pre dosiahnutie identifikácie konkrétnej fyzickej osoby závisí od komplexného posúdenia dostupných údajov v ich vzájomnej súvislosti a konkrétnej situácie. V závislosti od kvality, kvantity a druhu údajov sa určiteľnosť mení do určenia konkrétnej fyzickej osoby. Fyzickú osobu považujeme za určenú, keď na základe dostupných údajov je jednoznačne identifikovaná a odlišená od ostatných osôb v danom informačnom systéme, v ktorom sa osobné údaje spracúvajú. Na určenie toho, či je fyzická osoba identifikovateľná, sa majú vziať do úvahy všetky prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo akákoľvek iná osoba využije, napríklad osobitným výberom, na priamu alebo nepriamu identifikáciu fyzickej osoby.

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

Pri obmedzení spracúvania sú spracúvané osobné údaje označené na účely obmedzenia ich spracúvania do budúcnosti. Obmedzením nie je vždy potrebné chápať iba ich blokovanie, ale aj obmedzenie ich spracúvania na určitý účel. Obmedzenie spracúvania môže byť vykonané na účely ochrany dotknutej osoby a uplatnenia si jej práv v prípade, že namieta spracúvanie týchto svojich osobných údajov, má pochybnosti o správnosti alebo zákonnosti ich spracúvania, prípadne ak odpadla potreba spracúvania osobných údajov prevádzkovateľom, avšak dotknutá osoba potrebuje naďalej spracúvať tieto osobné údaje u daného prevádzkovateľa, napríklad na účely domáhania sa svojich právnych nárokov v budúcnosti.

Profilovaním sa rozumie spracúvanie osobných údajov, na základe ktorého možno získať v závislosti od kvality a kvantity spracúvaných informácií relatívne ucelený profil dotknutej osoby, ktorý možno využiť s vysokým stupňom pravdepodobnosti najmä na predpovedanie správania konkrétnej dotknutej osoby do budúcnosti. Použitie profilovania je rozsiahle, pričom jednou z možností jeho využitia, ktorá je na vzostupe, je jeho využívanie na vytvorenie cielennej reklamy na mieru konkrétneho jedinca. Na účely profilovania by mali byť používané primerané matematické alebo štatistické postupy, mali by byť prijaté technické a organizačné opatrenia tak, aby sa zabezpečilo, že faktory, ktoré vedú, alebo by mohli viesť k nesprávnosti osobných údajov sa opravujú a riziko chýb sa minimalizuje. Zabezpečí sa tak zohľadnenie súvisiacich potenciálnych rizík pre záujmy a práva dotknutej osoby. Profilovanie založené na spracúvaní osobitných kategórií osobných údajov je možné len za osobitných podmienok viazucich sa na spracúvanie osobitnej kategórie osobných údajov.

Pseudonymizácia je spracúvanie osobných údajov v takej forme, že dané údaje už následne nie je možné priradiť ku konkrétnej dotknutej osobe bez toho, aby sa na to museli použiť dodatočné informácie, ktoré by mali byť uchovávané oddelene a osobitne zabezpečené. Pseudonymizované údaje sú stále osobnými údajmi podliehajúcimi ochrane; ide však o jedno z bezpečnostných opatrení, ktoré môže prevádzkovateľ využiť, aby ním spracúvané osobné údaje chránil.

Rozdiel medzi anonymizovanými a pseudonymizovanými údajmi je v tom, že anonymizované údaje ani s použitím dodatočných informácií nemožno priradiť ku konkrétnej dotknutej osobe, naopak s pseudonymizovanými údajmi by to malo byť možné, a pokiaľ nie je, ide o anonymizované osobné údaje.

Informačným systémom sa na účely tohto zákona rozumie akýkoľvek usporiadaný súbor, sústava alebo databáza určená na zhromažďovanie osobných údajov alebo obsahujúca osobné údaje fyzických osôb, ktoré sú systematicky spracúvané pre potreby dosiahnutia vopred vymedzeného alebo ustanoveného účelu podľa osobitných kritérií a podmienok s použitím automatizovaných, čiastočne automatizovaných alebo iných ako automatizovaných prostriedkov spracúvania bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe. Jedným informačným systémom osobných údajov je aj prípad, keď prevádzkovateľ spracúva osobné údaje viacerými

prostriedkami spracúvania na jeden účel (papierová evidencia dochádzky a čipová karta zamestnanca sú súčasťou dochádzky zamestnancov, teda napriek využitiu viacerých prostriedkov spracúvania ide o jeden informačný systém osobných údajov, nakoľko účelom je sledovanie a zaznamenávanie dochádzky zamestnancov viacerými spôsobmi).

Dotknutou osobou je fyzická osoba, o ktorej sa osobné údaje spracúvajú. Dotknutou osobou je osoba aj vtedy, ak sa jej osobné údaje spracúvané v informačnom systéme osobných údajov týkajú.

Prevádzkovateľom je každý, kto sám alebo spoločne s inými pred začatím spracúvania osobných údajov vymedzí účel spracúvania osobných údajov a prostriedky ich spracúvania. Prevádzkovateľ spracúva osobné údaje vo vlastnom mene. Účel spracúvania môže byť ustanovený v osobitnom predpise (prevádzkovateľ ho musí rešpektovať a dodržiavať) alebo je prevádzkovateľovi daná možnosť, aby si ho vymedzil, napríklad na základe zamerania jeho podnikateľskej činnosti rešpektujúc právny poriadok a legálne možnosti, ktoré mu ponúka.

Sprostredkovateľom je každý, kto spracúva osobné údaje v mene prevádzkovateľa. Právny vzťah, na základe ktorého dochádza k spracúvaniu osobných údajov sprostredkovateľom v mene prevádzkovateľa, je založený na zmluve, alebo na inom právnom akte, napr. poverení sprostredkovateľa prevádzkovateľom. Minimálne náležitosti zmluvy medzi prevádzkovateľom a sprostredkovateľom, alebo iného právneho aktu ustanovuje tento zákon alebo iný osobitný zákon. Sprostredkovateľ spracúva osobné údaje na právnom základe prevádzkovateľa, t.j. sprostredkovateľ nemá osobitný právny základ odlišný od prevádzkovateľa, ale spracúvanie osobných údajov vykonáva na základe podmienok a prostriedkov, ktoré určil prevádzkovateľ, alebo ktoré prevádzkovateľovi ustanovuje napríklad osobitný zákon.

Tak prevádzkovateľ, ako aj sprostredkovateľ, ak je prevádzkovateľom poverený spracúvať v jeho mene osobné údaje, sú viazaní týmto zákonom, prípadne inými osobitnými zákonmi, ak tieto upravujú spracúvanie osobných údajov.

Príjemcom na účely tohto zákona je každý, komu sú osobné údaje poskytnuté, či sa už jedná o tretiu stranu alebo nie. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s osobitným predpisom, sa však nepovažujú za príjemcov; spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s pravidlami ochrany osobných údajov v závislosti od účelov spracúvania im stanovených osobitnými právnymi predpismi. Najmä vo vzťahu k zodpovednej osobe je používaný aj pojem kategória príjemcov, pričom pod ňou si možno predstaviť napríklad kategóriu prevádzkovateľov alebo sprostredkovateľov majúcich rovnaké alebo podobné podnikateľské zameranie, napríklad banky, poisťovne, živnostníkov s rovnakým predmetom podnikania a podobne.

Za porušenie ochrany osobných údajov sa považujú situácie, pri ktorých dochádza k nedovolenému resp. nezákonnému nakladaniu s osobnými údajmi, či už úmyselne alebo v dôsledku zanedbania povinností a opatrení prijatých na ich ochranu. Ak sa porušenie ochrany osobných údajov nerieši primeraným spôsobom a včas, môže fyzickým osobám spôsobiť ujmu napríklad na zdraví, majetkovú alebo nemajetkovú ujmu, alebo môže spôsobiť akékoľvek iné závažné hospodárske či sociálne znevýhodnenie dotknutej fyzickej osoby. Porušenie ochrany môže byť vyvolané zvonka prevádzkovateľa alebo sprostredkovateľa (napr. kybernetický útok) alebo zvnútra prevádzkovateľa alebo sprostredkovateľa (napr. pochybenie zamestnanca, a to

tak úmyselné ako neúmyselné, ktoré povedie k narušeniu integrity, dostupnosti a dôvernosti osobných údajov).

Genetický údaj možno vymedziť ako osobný údaj týkajúci sa zdedených alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré sú najmä výsledkom analýzy biologických vzoriek danej fyzickej osoby, najmä analýzy chromozómov, deoxyribonukleovej kyseliny (DNA) alebo ribonukleovej kyseliny (RNA), alebo analýzy inej látky, ktorá umožňuje získanie rovnocenných informácií o konkrétnej dotknutej osobe. Genetické osobné údaje patria medzi osobitnú kategóriu osobných údajov, ktorá sa tiež označuje, ako citlivé osobné údaje.

Biometrický údaj možno definovať ako biologickú alebo fyziologickú vlastnosť alebo charakteristiku špecifickú pre konkrétneho jednotlivca a zároveň merateľnú veličinu s určitým stupňom zohľadnenej pravdepodobnosti. Príkladom biometrických údajov sú odtlačky prstov, biometrický snímok sietnice oka, tvar tváre a vzdialenosti jej jednotlivých častí, hlas, geometria ruky, geometria štruktúry žíl ruky alebo dlane určitého človeka, alebo určitá hlboko zakorenená schopnosť, alebo vlastnosť týkajúca sa správania konkrétneho jedinca (napr. vlastnoručný podpis spôsob jeho písania, vyvíjanie tlaku na podložku, udieranie na klávesnicu, osobitný spôsob chôdze alebo artikulácie atď.; v tomto prípade ide o tzv. behaviorálnu biometriu).

Osobné údaje týkajúce sa zdravia sú také osobné údaje, ktoré poskytujú informácie o minulom, súčasnom alebo možnom budúcom fyzickom alebo duševnom zdravotnom stave dotknutej osoby. Patria sem aj údaje o zdraví fyzickej osoby získané pri jej registrácii na účely poskytovania služieb zdravotnej starostlivosti, služieb súvisiacich s poskytovaním zdravotnej starostlivosti alebo sociálnych služieb. Medzi osobné údaje týkajúce sa zdravia patrí tiež číslo, symbol alebo osobitný údaj, ktorý bol fyzickej osobe pridelený na jej individuálnu identifikáciu na zdravotné účely, informácie získané na základe vykonania testov alebo prehliadok častí jej organizmu, alebo skúmania jej telesných látok vrátane genetických údajov a biologických vzoriek a akékoľvek informácie o chorobe, zdravotnom postihnutí, riziku ochorenia, anamnéze, klinickej liečbe, alebo o fyziologickom alebo biomedicínskom stave dotknutej osoby bez ohľadu na zdroj týchto informácií, ktorým môže byť lekár alebo iný zdravotnícky pracovník, nemocnica ako inštitúcia, zdravotnícka pomôcka pridelená konkrétnej osobe alebo informácie pochádzajúce z vykonania diagnostického testu in vitro. Medzi údaje o zdraví patria aj informácie o zdraví konkrétnej osoby získané z mobilných aplikácií slúžiacich k monitorovaniu životných funkcií alebo fyziologických parametrov osoby.

Medzinárodná organizácia je inštitucionalizovaná podoba medzinárodných vzťahov vznikajúca najčastejšie dohodou dvoch alebo viacerých krajín, ktoré určia aj jej podobu, stanovia jej orgány, podmienky jej fungovania a podmienky pristúpenia k takejto medzinárodnej organizácii.

Vedenie logov, logovanie je bezpečnostné opatrenie, slúžiace k zaznamenávaniu akýchkoľvek zmien, prehliadania, poskytovania, prenosu, kombinovania alebo vymazávania osobných údajov v rámci informačného systému osobných údajov alebo ich pokusov o zmenu, ktoré je založené na zachytení údaje o tom, kto, kedy a akú zmenu v automatizovanom informačnom systéme osobných údajov vykonal alebo sa pokúšal vykonať. Výsledkom logovania je zaznamenávanie logov, ktoré následne môžu slúžiť na vykonávanie analýzy a na zaznamenávanie činnosti používateľa v automatizovanom informačnom systéme. Logom je tiež akékoľvek používateľské meno alebo heslo alebo iný prihlasovací údaj, ktorý slúži na prihlásenie používateľa do automatizovaného informačného systému osobných údajov.

Online identifikátor alebo jednoznačný identifikátor je využívaný pri vzájomnej komunikácii koncových zariadení užívateľov prostredníctvom komunikačných sietí. Takýmito identifikátormi sú napríklad IP adresa a cookies, či iné identifikátory využívajúce napríklad rádiovú frekvenciu (tzv. RFID identifikátory). Online identifikátor je osobným údajom konkrétnej fyzickej osoby, pokiaľ ho je možné k tejto osobe jednoznačne priradiť, teda pokiaľ sa možno s najvyššou pravdepodobnosťou domnievať alebo je potvrdené, že koncové zariadenie je používané konkrétnou osobu, teda z neho možno aj na základe informácií pochádzajúcich z identifikátorov vyčítať konkrétne aspekty správania a preferencií fyzickej osoby.

Pre účely zákona sa definuje pojem členský štát, keďže tento okrem členských štátov Európskej únie zahŕňa aj zmluvné strany Dohody o Európskom hospodárskom priestore. Z opaku sa potom definuje tretia krajina.

K § 3

Ustanovujú sa dve základné povinnosti príslušných orgánov pri plnení úloh na účely podľa § 1 zákona, a to chrániť základné práva a slobody dotknutých osôb vo všeobecnosti a tiež pri výmene osobných údajov medzi príslušnými orgánmi v rámci Európskej únie. Zákon definuje rozsah ochrany osobných údajov.

K § 4

V súlade s čl. 4 smernice (EÚ) 2016/680 v platnom znení zákon upravuje zásadu obmedzenia účelu. Osobné údaje by mali byť primerané a relevantné vzhľadom na účely, na ktoré sa spracúvajú. Osobné údaje by sa mali spracúvať len vtedy, ak účel spracúvania nebolo možné za primeraných podmienok dosiahnuť inými prostriedkami.

Ak príslušný orgán pôvodne získal osobné údaje na účely tohto zákona, na ich následné spracúvanie na účely odlišné od pôvodných by sa malo uplatňovať nariadenie (EÚ) 2016/679 v platnom znení, pokiaľ je takéto spracúvanie povolené právom EÚ alebo vnútroštátnym právom. Pravidlá nariadenia (EÚ) 2016/679 v platnom znení by sa mali uplatňovať najmä na prenos osobných údajov na účely, ktoré nepatria do rozsahu pôsobnosti tohto zákona. Na spracúvanie osobných údajov príjemcom, ktorý nie je príslušným orgánom alebo ktorý nekoná ako príslušný orgán a ktorému osobné údaje zákonne poskytol príslušný orgán, by sa malo vzťahovať nariadenie (EÚ) 2016/679 v platnom znení.

Ak príslušný orgán spracúva osobné údaje na iné účely ako na plnenie úloh na účely tohto zákona, uplatňuje sa nariadenie (EÚ) 2016/679 v platnom znení. Nariadenie (EÚ) 2016/679 v platnom znení sa uplatňuje v prípadoch, keď príslušný orgán získava osobné údaje na iné účely a ďalej spracúva tieto osobné údaje s cieľom splniť zákonnú povinnosť, ktorá sa naň vzťahuje. Činnosti, ktoré vykonáva príslušný orgán sa sústreďujú predovšetkým na predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie, vrátane policajných činností, pri ktorých nie je vopred známe, či je skutok trestným činom. Medzi takéto činnosti môže patriť aj výkon právomoci prostredníctvom prijatia donucovacích opatrení, ako napríklad činnosť polície pri demonštráciách, významných športových podujatiach a nepokojoch. Zahŕňajú tiež udržiavanie verejného poriadku ako úlohy uloženej polícii alebo iným orgánom, ak je to potrebné na ochranu pred ohrozením verejnej bezpečnosti a základných záujmov spoločnosti chránených zákonom, ktoré môže viesť k spáchaniu trestného činu, a na predchádzanie takémuto ohrozeniu.

Osobné údaje musia byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to nevyhnutné na dosiahnutie účelu spracúvania.

K § 5

Na to, aby bolo spracúvanie osobných údajov zákonné, by malo byť nevyhnutné na plnenie úloh na účely podľa tohto zákona alebo na základe medzinárodnej zmluvy, ktorou je Slovenská republika viazaná alebo na základe vnútroštátneho práva. Zákon súčasne stanovuje minimálne nároky na právny základ spracúvania osobných údajov v rozsahu vymedzenia osobných údajov, ktoré sa majú spracovávať, ako aj cieľa a účelu tohto spracúvania.

K § 6

Osobné údaje, ktoré sú svojou povahou na základe zákona považované za obzvlášť citlivé, si zasluhujú osobitnú ochranu, keďže z kontextu ich spracúvania by mohli pre práva a slobody vyplývať významné riziká. Takéto osobné údaje by sa nemali spracúvať, pokiaľ spracúvanie nepodlieha primeraným zárukám pre práva dotknutých osôb, ktoré sú ustanovené právnymi predpismi, pričom je prípustné v prípadoch povolených právnymi predpismi; ak spracúvanie ešte nie je povolené právnym predpisom, je nevyhnutné na ochranu životne dôležitých záujmov dotknutej alebo inej osoby, alebo ak sa spracúvanie týka osobných údajov, ktoré preukázateľne poskytla dotknutá osoba.

Vyžaduje sa tiež prijatie primeraných záruk na ochranu práv a slobôd dotknutej osoby. Primerané záruky by mohli zahŕňať napríklad možnosť získať uvedené údaje iba v súvislosti s inými údajmi o dotknutej fyzickej osobe, možnosť primerane zabezpečiť získané údaje, prísnejšie pravidlá prístupu personálu príslušného orgánu k údajom a zákaz prenosu týchto údajov.

Spracúvanie osobných údajov na iný účel, než na ktorý boli pôvodne zozbierané, predstavuje dodatočný zásah do práv dotknutej osoby. Aby bol takýto zásah v súlade so zákonom, vyžaduje sa, aby bol nielen nevyhnutný (t. j. cieľ nemožno dosiahnuť iným, menej invazívnym spôsobom), ale aj primeraný uplatňujúc zásadu proporcionality. Takýto zásah vyžaduje vyvážený pomer medzi intenzitou zásahu do práv dotknutej osoby a sledovaným účelom. Spracúvanie osobných údajov na iný účel je primerané vtedy, ak sa obmedzuje len na nevyhnutný rozsah a dobu, pričom sa zohľadňuje povaha spracúvaných údajov a prijaté bezpečnostné záruky. Keďže ide o neurčitý právny pojem, jeho presný obsah sa posudzuje individuálne podľa konkrétnych okolností prípadu, pričom dôkazné bremeno znáša príslušný orgán.

K § 7

Jedným zo základných cieľov právnej úpravy je upraviť individuálne práva a povinnosti orgánov v oblasti ochrany osobných údajov na účely zabezpečenia predchádzania trestnej činnosti, jej vyšetrovania alebo na účely výkonu rozhodnutí v trestnom konaní.

Prevádzkovateľom v prípade spracúvania osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku v registri trestov môže byť iba štátny orgán, ak mu to ustanovuje osobitný zákon. V podmienkach Slovenskej republiky je takýmto

prevádzkovateľom Generálna prokuratúra Slovenskej republiky. Iný prevádzkovateľ môže spracúvať tieto osobné údaje, len ak ho na to oprávňuje osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, za splnenia podmienky, že daný osobitný predpis alebo medzinárodná zmluva poskytuje primerané záruky ochrany pre práva dotknutej osoby v súvislosti so spracúvaním osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky.

Týmito zárukami sa rozumejú najmä osobitné technické, organizačné a procesné opatrenia, ktoré kompenzujú zvýšené riziko spojené so spracúvaním citlivých údajov. Môže ísť napríklad o striktné obmedzenie prístupových oprávnení, uplatňovanie šifrovania či pseudonymizácie, vedenie logov, stanovenie prísnejších lehôt preskúmania potreby spracúvania, predchádzajúce posúdenie vplyvu na ochranu osobných údajov (DPIA) atď. Konkrétne forma a rozsah primeraných záruk sa odvíjajú od povahy spracúvaných údajov, rozsahu spracúvania a z toho vyplývajúcich rizík pre práva a slobody dotknutých osôb.

K § 8

K spracúvaniu osobných údajov v oblasti justičnej spolupráce v trestných veciach a v oblasti policajnej spolupráce nevyhnutne patrí spracúvanie osobných údajov, ktoré sa týkajú rôznych kategórií dotknutých osôb. Preto by sa tam, kde je to uplatniteľné, malo v čo najväčšom možnom rozsahu jasne rozlišovať medzi osobnými údajmi rôznych kategórií dotknutých osôb ako sú podozrivé osoby, osoby odsúdené za spáchanie trestného činu, obeť a iné osoby ako sú svedkovia, osoby disponujúce relevantnými informáciami alebo kontaktné osoby a spoločníci podozrivých osôb a odsúdených páchateľov trestných činov.

K § 9

Príslušné orgány by mali zabezpečiť, aby sa osobné údaje, ktoré sú nesprávne, neúplné alebo už nie sú aktuálne, neprenášali ani neposkytovali. S cieľom zabezpečiť ochranu fyzických osôb, správnosť, úplnosť alebo mieru aktuálnosti a spoľahlivosť prenášaných alebo poskytovaných osobných údajov by mali príslušné orgány pri každom prenose osobných údajov doplniť potrebné informácie.

K § 10

Odsek 1

Ochrana fyzických osôb by sa mala vzťahovať na spracúvanie osobných údajov automatizovanými prostriedkami, ako aj na manuálne spracúvanie, ak sú osobné údaje uložené v informačnom systéme alebo do neho majú byť uložené. Všetky informácie určené dotknutej osobe zo strany prevádzkovateľa jej majú byť poskytnuté v stručnej, ľahko prístupnej, ľahko pochopiteľnej forme, formulované jasne a jednoducho, a ak je to vhodné a technicky možné aj ľahko zrakovo vnímateľné. Týka sa to najmä situácií, v ktorých veľký počet účastníkov a technologická zložitosť činnosti sťažujú dotknutej osobe možnosť zistiť a pochopiť, kým a na aké účely boli jej osobné údaje získané. Prevádzkovateľ tieto povinnosti môže splniť zverejnením adekvátnych informácií na svojom webovom sídle, ich fyzickou dostupnosťou v papierovej podobe v priestoroch svojich pobočiek, ich distribúciou formou e-mailov alebo dorúčením poštou, prípadne priamym informovaním prostredníctvom svojich zamestnancov.

Prevádzkovateľ môže skombinovať niekoľko foriem informovania dotknutých osôb tak, aby sa ich informovanosť zaručila aj viacerými spôsobmi súbežne. Transparentnosť informácií najmä pri uplatňovaní si práv dotknutej osoby je osobitne dôležitá. Ustanovenie taxatívne nestanovuje v akej forme má prevádzkovateľ informovanie dotknutej osoby vykonávať, o tom vzhľadom na spracovateľské operácie a svoje možnosti rozhoduje prevádzkovateľ sám, zákon mu iba stanovuje podmienky, ktoré je potrebné, aby pri plnení informačnej povinnosti dodržal.

Odseky 2 a 3

Prevádzkovateľ uľahčuje dotknutej osobe výkon jej práv, ak si ich voči nemu uplatňuje. V prípade, ak prevádzkovateľ nevie identifikovať dotknutú osobu, ktorá si uplatní právo dotknutej osoby a ona mu poskytne osobné údaje na účely jej identifikácie a ľahšieho uplatnenia si svojich práv, nesmie prevádzkovateľ takúto jej iniciatívu odmietnuť, a to práve z dôvodu, že ide o uplatnenie si práv dotknutej osoby. Prevádzkovateľ nemusí vyhovieť žiadosti dotknutej osoby iba vtedy, ak preukáže, že dotknutú osobu napriek svojej maximálne vynaloženej snahe nie je schopný identifikovať.

Odseky 4 a 5

Na základe žiadosti dotknutej osoby je prevádzkovateľ povinný konať a prijať adekvátne opatrenia, o ktorých je povinný dotknutú osobu informovať najneskôr do mesiaca od doručenia žiadosti dotknutej osoby. V odôvodnených prípadoch môže prevádzkovateľ lehotu predĺžiť, a to o dva mesiace, pričom každé predĺženie lehoty je povinný dotknutej osobe bezodkladne oznámiť. S ohľadom na zásady spracúvania, ako aj transparentnosť postupov pri plnení si informačnej povinnosti by takéto predĺženie lehoty na plnenie si tejto informačnej povinnosti malo byť len zo závažných dôvodov na strane prevádzkovateľa, napríklad s ohľadom na časovú náročnosť prijatia primeraných a účinných bezpečnostných opatrení potrebných v súvislosti s uplatnením práva dotknutej osoby. Pokiaľ ide o spôsob konania a informovania zo strany prevádzkovateľa, ten by mal rešpektovať prostriedky, aké použila dotknutá osoba na podanie žiadosti, teda ak sa táto na prevádzkovateľa obrátila elektronicky, mal by jej odpovedať elektronicky, ak si dotknutá osoba nestanovila iný spôsob, ktorý jej vyhovuje viac. V prípade, že na základe žiadosti dotknutej osoby prevádzkovateľ nekonal, neprijal žiadne opatrenia, je povinný o tom dotknutú osobu informovať a taktiež jej uviesť dôvody, pre ktoré nekonal a tiež ju informovať o tom, že môže podať návrh na začatie konania na úrad.

Odseky 6 a 7

Žiadosť dotknutej osoby je prevádzkovateľ povinný vybaviť bezplatne. V prípade, ak sú žiadosti dotknutej osoby opakujúceho sa charakteru a rovnakého obsahu alebo sú neprimerané a neopodstatnené, a dotknutá osoba prípadne ani na základe výzvy prevádzkovateľa ich obsah nedoplní, prevádzkovateľ môže ich vybavenie spoplatniť, a to vo výške administratívnych nákladov potrebných na ich vybavenie, prípadne môže prevádzkovateľ odmietnuť na základe takejto žiadosti dotknutej osoby konať. Bremeno preukázania toho, že žiadosť dotknutej osoby bola neprimeraná alebo neopodstatnená, znáša prevádzkovateľ.

K § 11

Dotknutej osobe by sa mali zo strany príslušných orgánov poskytnúť aspoň tieto informácie: identifikačné údaje a kontaktné údaje príslušného orgánu, kontaktné údaje zodpovednej osoby, účely spracúvania, právo podať sťažnosť a právo žiadať prístup k osobným údajom a ich opravu

alebo vymazanie či obmedzenie spracúvania. Formulácia „identifikačné údaje a kontaktné údaje“ predstavuje ustálenú legislatívnu kategóriu, ktorá je plne kompatibilná s európskym rámcom ochrany osobných údajov (čl. 13 ods. 1 písm. a) smernica (EÚ) 2016/680 a čl. 13 ods. 1 písm. a) nariadenia (EÚ) 2016/679). Právna úprava zámerne nedefinuje podrobný taxatívny výpočet jednotlivých údajov (ako napr. adresa sídla, e-mailový kontakt či telefónne číslo), nakoľko konkrétny rozsah a forma ich poskytnutia závisia od povahy príslušného orgánu a zvoleného spôsobu komunikácie. Tieto informácie by sa mohli poskytnúť najmä, nie však výlučne, prostredníctvom webového sídla príslušného orgánu. S cieľom zaručiť spravodlivé spracúvanie vo vzťahu k dotknutej osobe a na to, aby mohla uplatňovať svoje práva, by mala byť okrem toho dotknutá osoba v osobitných prípadoch informovaná o právnom základe pre spracúvanie, o dobe uchovávaní údajov, účeloch spracúvania, kategóriách príjemcov a prípadne ďalšie informácie. Tieto informácie sa neposkytujú dotknutej osobe automaticky, ale predstavujú užšiu skupinu informácií, ktoré sa dotknutej osobe poskytnú popri základných informáciách uvedených v odseku 1 v tých prípadoch, ktoré budú upravené osobitne alebo špeciálne vo vzťahu k všeobecnej úprave v tomto zákone. Pôjde o také osobitné situácie alebo osobitné prípady, ktoré predstavujú obsahovo odchýlku od základného poskytovania údajov a formálne budú upravené, resp. budú vyplývať z osobitného predpisu.

K § 12

Fyzická osoba by mala mať právo na prístup k údajom, ktoré boli o nej získané, a toto právo aj jednoducho uplatňovať, aby si bola vedomá zákonnosti spracúvania a mohla si ju overiť. Každá dotknutá osoba by preto mala mať právo vedieť a byť informovaná najmä o účeloch spracúvania údajov, kategóriách dotknutých osobných údajov a o dobe, počas ktorej sa budú údaje spracúvať, ako aj o príjemcoch osobných údajov atď. Na dodržanie tohto práva je dostatočné, aby mala dotknutá osoba k dispozícii úplné zhrnutie uvedených údajov v zrozumiteľnej forme, to znamená vo forme, ktorá umožňuje, aby bola dotknutá osoba informovaná o uvedených údajoch, aby si mohla uplatniť práva, ktoré jej tento zákon priznáva.

K § 13

Fyzická osoba by tiež mala mať právo na opravu nesprávnych osobných údajov, ktoré sa jej týkajú, ako aj právo na ich vymazanie, ak je spracúvanie takýchto údajov v rozpore so zákonom. Právom na opravu by však nemal byť napríklad dotknutý obsah svedeckej výpovede. Fyzická osoba by mala mať právo na obmedzenie spracúvania, ak napadne správnosť osobných údajov a nemožno určiť ich správnosť či nesprávnosť, alebo keď je potrebné osobné údaje uchovať na účely dokazovania. Namiesto vymazania osobných údajov by sa spracúvanie malo obmedziť najmä vtedy, keď sa v osobitnom prípade možno odôvodnene domnievať, že vymazanie by mohlo ovplyvniť oprávnené záujmy dotknutej osoby. V takomto prípade by sa obmedzené údaje mali spracúvať len na účely, ktoré zabránili ich vymazaniu. To sú prípady, ak dotknutá osoba napadla správnosť osobných údajov a ich správnosť alebo nesprávnosť nemožno určiť, alebo sa osobné údaje zachováajú na účely dokazovania.

Metódy na obmedzenie spracúvania osobných údajov by okrem iného mohli zahŕňať presunutie vybraných údajov do iného systému spracúvania, napríklad na účely archivácie, alebo zamedzenie prístupu k nim. V automatizovaných informačných systémoch by sa obmedzenie spracúvania malo v zásade zabezpečiť technickými prostriedkami. Skutočnosť, že spracúvanie osobných údajov je obmedzené, by sa v systéme mala vyznačiť tak, aby bolo jednoznačné, že spracúvanie osobných údajov je obmedzené. Takáto oprava alebo vymazanie osobných údajov alebo obmedzenie spracúvania by sa mali oznámiť príjemcom, ktorým sa údaje poskytnú,

a príslušným orgánom, od ktorých nesprávne údaje pochádzajú. Príslušné orgány by takisto mali upustiť od ďalšieho šírenia takýchto údajov.

K § 14

Podľa tohto ustanovenia sa poskytovanie informácií dotknutým osobám odloží, obmedzí alebo sa od neho upustí, alebo sa úplne či čiastočne obmedzí prístup k ich osobným údajom, a to v takom rozsahu a na tak dlho, ako je toto opatrenie s náležitým zreteľom na práva a oprávnené záujmy dotknutej fyzickej osoby v demokratickej spoločnosti nevyhnutné a primerané tak, aby sa zabránilo mareniu úradného alebo súdneho zisťovania, vyšetrovania alebo konania, aby sa zabránilo ohrozeniu plnenia úloh na účely trestného konania, aby sa ochránila verejná bezpečnosť alebo národná bezpečnosť, alebo aby sa ochránili práva a slobody iných. Príslušný orgán by mal prostredníctvom konkrétneho a individuálneho preskúmania každého prípadu posúdiť, či by sa právo na prístup malo čiastočne alebo úplne obmedziť.

Akékoľvek zamietnutie alebo obmedzenie prístupu by malo byť dotknutej osobe oznámené písomne a malo by zahŕňať skutkové alebo právne dôvody, na ktorých je toto rozhodnutie založené.

K § 15

Oprava alebo vymazanie osobných údajov alebo obmedzenie spracúvania by sa mali oznámiť príslušným orgánom, od ktorých nesprávne údaje pochádzajú. Prijemcovia týchto údajov by takisto mali nimi spracúvané osobné údaje opraviť, vymazať alebo obmedziť ich spracúvanie.

K § 16

Keďže smernica (EÚ) 2016/680 v platnom znení nebráni členským štátom Európskej únie (ďalej len „členský štát“) v tom, aby implementovali výkon práv dotknutých osôb na informácie, prístup a opravu alebo vymazanie osobných údajov a obmedzenie spracúvania počas trestného konania, ako aj prípadné obmedzenia týchto práv do vnútroštátnych predpisov upravujúcich trestné právo procesné, platí, že ak sa osobné údaje spracúvajú počas vyšetrovania trestného činu a súdneho konania v trestných veciach, uplatňovanie práva na informácie, prístup a opravu alebo vymazanie osobných údajov a obmedzenie spracúvania sa vykonáva v súlade napríklad so zákonom č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov, ktorého súčasťou je aj vykonávacie konanie, respektíve zákonom č. 757/2004 Z. z. o súdoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákonom č. 475/2005 Z. z. o výkone trestu odňatia slobody a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákonom č. 221/2006 Z. z. o výkone väzby v znení neskorších predpisov.

K § 17

Dotknutá osoba by mala mať právo na to, aby sa na ňu nevzťahovalo rozhodnutie hodnotiace osobné aspekty s ňou súvisiace, ktoré je založené výlučne na automatizovanom spracúvaní a ktoré má pre túto osobu nepriaznivé právne účinky alebo významné dôsledky. V každom prípade by takéto spracúvanie malo podliehať primeraným zárukám vrátane poskytnutia určitých informácií dotknutej osobe a právu na iný ako automatizovaný zásah, ľudský zásah (t. j. situáciu, keď kontrolu automatizovaného spracúvania vykoná na žiadosť dotknutej osoby zamestnanec prevádzkovateľa; pôjde o fyzickú kontrolu a prípadné odstránenie chýb**, ak** vznikli, napríklad nesprávnym nastavením algoritmu), ďalej právu vyjadriť svoj názor, dostať

vysvetlenie k rozhodnutiu dosiahnutému po takomto posúdení alebo napadnutí toto rozhodnutie.

Profilovanie, ktoré vedie k diskriminácii fyzických osôb na základe osobných údajov, ktoré sú svojou povahou obzvlášť citlivé v súvislosti so základnými právami a slobodami, sa zakazuje.

K § 18

Základná požiadavka na spracúvanie osobných údajov iba v súlade so zákonom sa premieta aj do povinnosti príslušného orgánu ako prevádzkovateľa prijať opatrenia na zabezpečenie zákonnosti spracúvania osobných údajov, pričom zákon ich bližšie nešpecifikuje a ponecháva na príslušnom orgáne, aby vzhľadom na spracovateľské operácie prijal vhodné technické a organizačné opatrenia a primerané postupy ochrany osobných údajov.

K § 19

Vyžaduje sa, aby príslušný orgán ako prevádzkovateľ zaviedol pri spracúvaní osobných údajov účinné opatrenia na ochranu práv a slobôd fyzických osôb, pričom zákon ako vhodné opatrenia uvádza pseudonymizáciu. Ďalej sa v súlade s minimalizáciou spracúvania osobných údajov vyžaduje len spracúvanie nevyhnutného množstva osobných údajov vo vzťahu ku každej spracovateľskej operácii.

K § 20

Smernica (EÚ) 2016/680 v platnom znení umožňuje aj tzv. spoločných prevádzkovateľov, preto túto možnosť dáva aj predložený zákon. Vymedzuje sa, čo sú spoloční prevádzkovatelia, právny základ ich spoločného pôsobenia ako prevádzkovateľov, určenie zodpovedností za plnenie povinností podľa tohto zákona a osobitne tých povinností, ktoré sa týkajú uplatnenia práv dotknutej osoby.

K § 21

Upravuje sa postavenie sprostredkovateľa, teda osoby, ktorá uskutočňuje spracúvanie osobných údajov v mene príslušného orgánu ako prevádzkovateľa. Stanovuje sa, kto môže byť sprostredkovateľom a stanovuje sa právny základ zakladajúci vzťah medzi príslušným orgánom ako prevádzkovateľom a sprostredkovateľom vrátane minimálneho povinného obsahu tohto právneho vzťahu.

Zákon umožňuje sprostredkovateľovi využitie aj ďalšieho sprostredkovateľa, ale viaže ho na predchádzajúce písomné povolenie príslušného orgánu, pričom toto povolenie môže byť jednak osobitné, teda iba na konkrétny prípad alebo konkrétnu situáciu spracúvania osobných údajov, a jednak všeobecné, čo umožňuje vyššiu flexibilitu pri využívaní sprostredkovateľov.

K § 22

Sprostredkovateľ je viazaný tým, že bez súhlasu prevádzkovateľa nesmie spracúvať osobné údaje, ku ktorým má ako sprostredkovateľ prístup, teda, že ako sprostredkovateľ koná až na základe pokynu príslušného orgánu ako prevádzkovateľa a nie z vlastnej iniciatívy. Ak by, ale iniciatívne konanie sprostredkovateľa vyžadoval ďalší osobitný predpis, teda by malo

právny základ a oporu v osobitnom, vo vzťahu k tomuto zákonu špeciálnom, právnom predpise, tak by mohol sprostredkovateľ konať aj bez pokynu.

K § 23

Zákon ukladá príslušnému orgánu ako prevádzkovateľovi určiť zodpovednú osobu. Voľba zodpovednej osoby je na príslušnom orgáne, pričom vodítkom pre jeho rozhodnutie o tom, kto bude pre neho vykonávať funkciu zodpovednej osoby, je jej schopnosť zabezpečiť plnenie úloh podľa tohto zákona.

K § 24

Aby mohla určená zodpovedná osoba riadne plniť úlohy, ktoré jej zveruje tento zákon, je nevyhnutné, aby mala zo strany príslušného orgánu ako prevádzkovateľa vytvorené na to zodpovedajúce podmienky, najmä aby mala na to potrebné prostriedky a musí tiež zabezpečovať udržiavanie svojich odborných znalostí, a to najmä v oblasti práva a ochrany osobných údajov. Zodpovedná osoba ďalej musí mať prístup k spracúvaným osobným údajom a spracovateľským operáciám, inak nemôže riadne plniť svoje úlohy.

K § 25

Zákon v súlade s čl. 34 smernice (EÚ) 2016/680 v platnom znení upravuje úlohy zodpovednej osoby. Zákon nejde nad rámec smernice (EÚ) 2016/680 v platnom znení a stanovuje úlohy zodpovednej osoby iba v minimálnom rozsahu.

K § 26

Zákon stanovuje povinnosť viesť v písomnej podobe záznamy o všetkých kategóriách spracovateľských činností s osobnými údajmi, a to tak zo strany príslušného orgánu ako prevádzkovateľa v rozsahu jeho zodpovednosti za príslušnú spracovateľskú činnosť, ako aj zo strany sprostredkovateľa za spracovateľské činnosti, ktoré vykonal v mene prevádzkovateľa.

K § 27

Logy by sa mali viesť pre operácie v systémoch automatizovaného spracúvania, ako sú získavanie, zmena, prehliadanie, poskytovanie vrátane prenosov, kombinovanie alebo vymazanie. Mali by sa zaznamenávať dôvody spracovateľských operácií, dátum a čas operácie a, pokiaľ možno, aj identifikačné údaje osoby, ktorá osobné údaje prehliadala alebo ich poskytla a totožnosť príjemcov. Logy by sa mali využívať výlučne na overovanie zákonnosti spracúvania, vlastné monitorovanie, zabezpečenie integrity a bezpečnosti údajov a na účely trestného konania. Vlastné monitorovanie by malo zahŕňať aj interné disciplinárne konanie príslušných orgánov. Uchovávanie logov po celú dobu spracúvania osobných údajov a okrem toho ešte najmenej päť rokov po jeho skončení je nevyhnutné na zabezpečenie spätnej preveriteľnosti spracovateľských operácií, identifikáciu incidentov, výkon auditu a preukázanie súladu so zákonom. Minimálna lehota päť rokov po skončení spracúvania osobných údajov zabezpečuje, že príslušný orgán bude schopný plniť svoje povinnosti aj spätne, najmä v prípadoch oneskorených zistení alebo konaní pred dozorným orgánom. V aplikačnej praxi môžu nastať situácie, kedy bude potrebné napríklad spätne preveriť záznamy o spracovateľských operáciách (prehliadanie, zmena, šírenie osobných údajov).

K § 28

Potreba posúdenia vplyvu spracúvania osobných údajov na ochranu týchto údajov je spojená s využívaním nových technológií, ktoré sa pri spracúvaní osobných údajov používajú. Ak by ich použitie malo predstavovať vysoké riziko pre práva a slobody fyzických osôb, má príslušný orgán ako prevádzkovateľ povinnosť vykonať ex ante posúdenie, pričom zákon v súlade so smernicou (EÚ) 2016/680 v platnom znení stanovuje iba minimálny rozsah posúdenia vplyvu.

K § 29

V určitých prípadoch by príslušný orgán alebo sprostredkovateľ mali uskutočniť s dozorným orgánom konzultácie pred spracúvaním s cieľom zabezpečiť účinnú ochranu práv dotknutých osôb. Dochádza k tomu, ak z posúdenia vplyvu na ochranu osobných údajov vyplýva vysoké riziko pre práva a slobody fyzických osôb.

K § 30

S cieľom zachovať bezpečnosť a predchádzať spracúvaniu, ktoré je v rozpore s týmto zákonom, by príslušný orgán alebo sprostredkovateľ mali posúdiť riziká súvisiace so spracúvaním a mali by prijať opatrenia na zmiernenie týchto rizík, ako napríklad šifrovanie. Takýmito opatreniami by sa mala zabezpečiť primeraná úroveň bezpečnosti vrátane dôvernosti a mali by sa zohľadniť najnovšie poznatky, náklady na vykonanie opatrení v súvislosti s rizikami a povahou osobných údajov, ktoré sa majú chrániť. Pri posudzovaní rizík v oblasti bezpečnosti údajov by sa mali zohľadniť riziká spojené so spracúvaním údajov, ako sú napríklad náhodná alebo nezákonná likvidácia, strata, zmena alebo neoprávnené poskytovanie prenášaných, uchovávaných alebo inak spracúvaných osobných údajov alebo neoprávnený prístup k nim, ktoré by mohli viesť k ujme na zdraví, majetkovej alebo nemajetkovej ujme. Príslušný orgán a sprostredkovateľ by mali zabezpečiť, aby spracúvanie osobných údajov nevykonávali neoprávnené osoby.

K § 31

Ak sa porušenie ochrany osobných údajov nerieši primeraným spôsobom a včas, môže fyzickým osobám spôsobiť ujmu na zdraví, majetkovú alebo nemajetkovú ujmu, ako je napríklad strata kontroly nad svojimi osobnými údajmi alebo obmedzenie práv týchto osôb, diskriminácia, krádež totožnosti alebo podvod, finančná strata, neoprávnená reverzná pseudonymizácia, poškodenie dobrého mena, strata dôvernosti osobných údajov chránených profesijným tajomstvom alebo akékoľvek iné závažné hospodárske či sociálne znevýhodnenie dotknutej fyzickej osoby. Príslušný orgán ako prevádzkovateľ by mal preto ihneď, ako sa dozvie, že došlo k porušeniu ochrany osobných údajov, najneskôr do 72 hodín od okamihu, ako sa dozvedel, že došlo k porušeniu ochrany osobných údajov, toto porušenie oznámiť úradu s výnimkou prípadov, keď vie v súlade so zásadou zodpovednosti preukázať, že nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb. Ak nie je možné oznámenie podať do 72 hodín, mal by (príslušný orgán) k oznámeniu pripojiť odôvodnenie omeškania, pričom informácie možno poskytnúť vo viacerých fázach bez ďalšieho zbytočného odkladu.

K § 32

Ak porušenie ochrany osobných údajov pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, mala by sa táto skutočnosť oznámiť fyzickým osobám, aby sa im umožnilo prijať potrebné preventívne opatrenia. V oznámení by sa mala uviesť povaha porušenia ochrany osobných údajov, ako aj odporúčania pre dotknutú fyzickú osobu o tom, ako zmierniť potenciálne nepriaznivé dôsledky. Dotknuté osoby by mali byť informované čo možno najskôr, v úzkej spolupráci s úradom a v súlade s usmerneniami tohto alebo iného príslušného orgánu. Napríklad potreba zmierniť bezprostredné riziko škody by si vyžadovala promptné informovanie dotknutých osôb, zatiaľ čo potreba vykonať primerané opatrenia na zabránenie pretrvávaniu alebo výskytu podobných porušení ochrany údajov môže vyžadovať viac času na informovanie. Ak by mohlo dôjsť k mareniu úradného alebo súdneho zisťovania, vyšetrovania alebo konania, zabrániť ohrozeniu plnenia úloh na účely trestného konania, či dosiahnuť ochranu verejnej bezpečnosti alebo národnej bezpečnosti alebo ochranu práv iných osôb prostredníctvom odkladu alebo obmedzenia informovania dotknutej osoby o porušení ochrany osobných údajov, možno od takéhoto oznámenia upustiť.

K § 33

Upravuje sa cezhraničný prenos osobných údajov príjemcovi v inom členskom štáte, agentúre alebo orgánu Európskej únie, pričom platí požiadavka, že sa pri takomto prenose nemôžu uplatňovať iné podmienky, ako pri prenose v rámci Slovenskej republiky. Tieto podmienky by mali byť vo všetkých členských štátoch rovnaké.

K § 34

Prenos do tretej krajiny alebo medzinárodnej organizácie sa môže uskutočniť len vtedy, ak je to potrebné na plnenie úloh na účely trestného konania, pričom prevádzkovateľ v tretej krajine alebo medzinárodná organizácia je príslušným orgánom v zmysle tohto zákona. Prenos by mali uskutočniť len príslušné orgány konajúce ako prevádzkovatelia s výnimkou prípadov, keď sa sprostredkovateľovi výslovne udelil pokyn uskutočniť prenos v mene príslušných orgánov. Takýto prenos sa môže uskutočniť v prípade, ak Európska komisia rozhodla, že daná tretia krajina alebo medzinárodná organizácia zaručuje primeranú úroveň ochrany, ak sa poskytnú primerané záruky, alebo ak platia výnimky pre osobitné situácie. Úroveň ochrany fyzických osôb by nemala byť ohrozená, keď sa osobné údaje prenášajú z Európskej únie prevádzkovateľom, sprostredkovateľom alebo iným príjemcom v tretích krajinách alebo medzinárodným organizáciám, a to ani v prípadoch následného prenosu osobných údajov z tretej krajiny alebo medzinárodnej organizácie prevádzkovateľom, či sprostredkovateľom v rovnakej alebo inej tretej krajine alebo medzinárodnej organizácii.

V prípade prenosu osobných údajov do tretích krajín alebo medzinárodným organizáciám by sa takýto prenos mal uskutočniť iba po tom, čo ho povolil členský štát, od ktorého sa údaje získali. Záujmy efektívnej spolupráce v oblasti presadzovania práva si vyžadujú, aby v prípade, keď je ohrozenie verejnej bezpečnosti členského štátu alebo tretej krajiny alebo záujmov členského štátu také bezprostredné, že nie je možné včas získať predchádzajúce povolenie, príslušný orgán by mal mať možnosť uskutočniť prenos daných osobných údajov do dotknutej tretej krajiny alebo medzinárodnej organizácie bez takéhoto predchádzajúceho povolenia. Akékoľvek osobitné podmienky týkajúce sa prenosu by sa mali oznámiť tretím krajinám alebo medzinárodným organizáciám. Následné prenosi osobných údajov by mali podliehať predchádzajúcemu povoleniu príslušného orgánu, ktorý uskutočnil pôvodný prenos. Pri rozhodovaní o žiadosti o povolenie následného prenosu by mal príslušný orgán, ktorý uskutočnil pôvodný prenos, náležite zohľadniť všetky relevantné okolnosti vrátane závažnosti

trestného činu, osobitných podmienok a účelu pôvodného prenosu údajov, povahy a podmienok výkonu trestných sankcií a úrovne ochrany osobných údajov v tretej krajine alebo medzinárodnej organizácii, do ktorej sa uskutočňuje následný prenos osobných údajov. Príslušný orgán, ktorý uskutočnil pôvodný prenos, by mal mať aj možnosť stanoviť osobitné podmienky pre následný prenos, ktoré možno popísať napríklad v manipulačných pravidlách.

K § 35

Prenosy, ktoré nie sú založené na rozhodnutí o primeranosti, by sa mali umožniť len vtedy, ak sa poskytnú primerané záruky v právne záväznom akte, ktorý zaručuje ochranu osobných údajov, alebo ak príslušný orgán posúdil všetky okolnosti sprevádzajúce prenos údajov a na základe tohto posúdenia dospel k záveru, že existujú primerané záruky ochrany osobných údajov. Právne záväznými aktmi môžu byť napríklad právne záväzné dvojstranné dohody, ktorých výkonu by sa mohli domáhať dotknuté osoby, zabezpečujúce súlad s požiadavkami na ochranu údajov a práva dotknutých osôb vrátane práva na účinný správny alebo súdny prostriedok nápravy. Príslušný orgán môže zohľadniť aj skutočnosť, že prenos osobných údajov bude podliehať povinnostiam zachovávanía dôvernosti a zásade špecifickosti, čím sa zabezpečí, že údaje sa nebudú spracúvať na iné účely, než sú účely prenosu. Okrem toho by mal príslušný orgán zohľadniť, že sa osobné údaje nepoužijú na požadovanie, uloženie alebo vykonanie trestu smrti alebo akejkoľvek inej formy krutého alebo neľudského zaobchádzania. Hoci by sa uvedené podmienky mohli považovať za primerané záruky umožňujúce prenos údajov, príslušný orgán by mal mať možnosť vyžadovať dodatočné záruky.

K § 36

V prípadoch, keď neexistuje žiadne rozhodnutie o primeranosti ani primerané záruky, malo by byť možné uskutočniť prenos alebo kategóriu prenosov len v osobitných situáciách, ak je to nevyhnutné na ochranu životne dôležitých záujmov dotknutej osoby či inej osoby alebo na zabezpečenie oprávnených záujmov dotknutej osoby za podmienok v tomto ustanovení, na predchádzanie bezprostrednému a vážnemu ohrozeniu verejnej bezpečnosti členského štátu alebo tretej krajiny, v jednotlivom prípade na plnenie úloh na účely trestného konania, alebo v jednotlivom prípade na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov. Uvedené výnimky by sa mali vykladať reštriktívne a nemali by umožňovať časté, hromadné a štruktúrované prenosy osobných údajov alebo rozsiahle prenosy údajov, ale mali by byť obmedzené na nevyhnutne potrebné údaje. Takéto prenosy musia byť zdokumentované a musia sa na požiadanie poskytnúť dozornému orgánu na účely monitorovania zákonnosti prenosu.

K § 37

Príslušné orgány uplatňujú platné dvojstranné alebo mnohostranné medzinárodné dohody uzavreté s tretími krajinami v oblasti justičnej spolupráce v trestných veciach a policajnej spolupráce na výmenu relevantných informácií, ktoré im umožňujú výkon ich úloh uložených zákonom. V zásade sa to uskutočňuje na základe spolupráce orgánov dotknutých tretích krajín príslušných na plnenie úloh na účely trestného konania alebo aspoň v spolupráci s nimi, niekedy dokonca aj vtedy, ak dvojstranná či mnohostranná medzinárodná dohoda neexistuje. V osobitných jednotlivých prípadoch však riadne postupy požadujúce nadviazanie kontaktu s takýmto orgánom v tretej krajine môžu byť neefektívne alebo nevhodné, najmä preto, že by sa presun nemohol uskutočniť včas, alebo preto, že tento orgán v tretej krajine nedodržiava zásady právneho štátu alebo medzinárodné normy a štandardy v oblasti ľudských práv, a preto by sa príslušné orgány mohli rozhodnúť, že uskutočnia prenos osobných údajov priamo

príjemcom usadeným v týchto tretích krajinách. Možno tak postupovať vtedy, keď je naliehavo potrebné vykonať prenos osobných údajov na záchranu života osoby, ktorej hrozí, že sa stane obeťou trestného činu, alebo v záujme zabránenia bezprostrednému spáchaniu trestného činu vrátane terorizmu. Aj keby k takémuto presunu medzi príslušnými orgánmi a príjemcami usadenými v tretích krajinách malo dochádzať len v určitých jednotlivých prípadoch, v tomto zákone sa ustanovujú podmienky s cieľom úpravy takýchto prípadov. Uvedené ustanovenia by sa nemali považovať za výnimky zo žiadnych existujúcich dvojstranných alebo mnohostranných medzinárodných dohôd v oblasti justičnej spolupráce v trestných veciach a policajnej spolupráce.

K § 38

Dozor nad ochranou osobných údajov podľa tohto zákona je zverený úradu, postavenie ktorého upravuje osobitný zákon o zabezpečení ochrany fyzických osôb pri spracúvaní osobných údajov a o zmene a doplnení niektorých zákonov (zákon o ochrane osobných údajov). Ak tento všeobecný zákon o ochrane osobných údajov zveruje dozor nad ochranou osobných údajov Ministerstvu spravodlivosti Slovenskej republiky, zostáva to zachované aj na účely tohto zákona.

Na výkon kontroly, na mlčanlivosť, na konanie o ochrane osobných údajov a na ukladanie pokút sa vzťahuje zákon o zabezpečení ochrany fyzických osôb pri spracúvaní osobných údajov a o zmene a doplnení niektorých zákonov (zákon o ochrane osobných údajov).

K § 39

Upravuje sa postup pri spolupráci úradu a dozorných orgánov iných členských štátov hlavne pri výmene relevantných informácií, poskytovaní vzájomnej pomoci a prijímaní opatrení v oblasti dozoru s cieľom zabezpečiť spoločný postup pri ochrane osobných údajov.

K §40

Za porušenie povinností ustanovených týmto zákonom možno diferencovane, podľa závažnosti, rozsahu a času trvania, následkov protiprávneho konania, prípadného opakovania takéhoto protiprávneho konania a miery ohrozenia súkromného a rodinného života, počtu dotknutých osôb a iných faktorov, ktoré musí brať úrad do úvahy, uložiť pokutu.

K § 41

V prílohe sa uvádza právne záväzný akt Európskej únie, ktorý sa týmto zákonom preberá.

K § 42

Navrhuje sa účinnosť zákona od 1. januára 2027.