

Prehľad zmien v oblasti ochrany osobných údajov vo vzťahu k Nariadeniu Európskeho parlamentu a Rady č. 2002/58/ES týkajúceho sa spracovávaní osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

I.

Pramene práva

Právny stav do 24.05.2018

Na území Slovenskej republiky je vo vzťahu k ochrane osobných údajov do 24.05.2018 účinný zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „**Pôvodný zákon**“), a to v znení všetkých neskorších noviel. Súčasne je za ďalší prameň práva potrebné považovať rôzne vykonávacie vyhlášky, prostredníctvom ktorých dochádza k vykonávaniu vyššie uvedeného zákona o ochrane osobných údajov ako aj Smernicu Európskeho parlamentu a Rady č. 95/46/ES o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov.

Právny stav od 25.05.2018

Za hlavný prameň práva je potrebné považovať predovšetkým Nariadenie Európskeho parlamentu a Rady č. 2016/679 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „**Nariadenie**“). Predmetné Nariadenie je v súlade s právom EÚ priamo aplikovateľné v jednotlivých členských štátoch EÚ. Slovenská republika však aj napriek automatickej aplikovateľnosti Nariadenia na území Slovenskej republiky prijala zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „**Zákon**“), ktorého účelom bolo dosiahnuť súlad vnútroštátneho právneho poriadku pre oblasť ochrany osobných údajov s Nariadením a zároveň týmto transponovať Smernicu Európskeho parlamentu a rady (EÚ) č. 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracovaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV do právneho poriadku Slovenskej republiky.

Predmetné Nariadenie bolo zo strany Európskej únie (ďalej len „**Únia**“ alebo „**EÚ**“) prijaté s cieľom zabezpečiť konzistentnú a vysokú úroveň ochrany fyzických osôb a odstrániť prekážky tokov osobných údajov v rámci Únie. Súčasne Únia chcela týmto Nariadením zabezpečiť, aby úroveň ochrany práv a slobôd fyzických osôb pri spracovaní týchto údajov bola rovnaká vo všetkých jej členských štátoch. Ďalším z cieľov Nariadenia je zaručiť konzistentnú úroveň ochrany fyzických osôb v celej Únii a zabrániť rozdielom, ktoré sú prekážkou voľného pohybu osobných údajov v rámci vnútorného trhu Únie.

II.

Zhrnutie podstatných bodov novej právnej úpravy

Pôsobnosť Nariadenia

Nariadenie sa vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie inými než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.

Nariadenie sa nevzťahuje na spracúvanie osobných údajov:

- a) v rámci činnosti, ktorá nepatrí do pôsobnosti práva Únie;
- b) členskými štátmi pri vykonávaní činností patriacich do rozsahu pôsobnosti kapitoly 2 hlavy V ZEÚ;
- c) fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti;
- d) príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetovania, odhaľovania alebo stíhania, alebo výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzania.

Nariadenie sa vzťahuje na spracúvanie osobných údajov v rámci činnosti prevádzky prevádzkovateľa alebo sprostredkovateľa v Únii, a to bez ohľadu na to, či sa spracúvanie vykonáva v Únii alebo nie.

Identifikácia osobných údajov ako aj iných druhov údajov, ktoré majú vplyv vo vzťahu k ochrane osobných údajov

Podľa Nariadenia sa za osobné údaje považujú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby; identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby. Podľa Nariadenia je možné za osobné údaje dokonca považovať (podľa bodu 30 recitálu Nariadenia) aj teoreticky IP adresu, cookies, alebo iné identifikátory, ako napríklad štítky na rádiový frekvenčnú identifikáciu.

Podľa Nariadenia (čl. 9) ako aj Zákona (§ 16 ods. 1) sa vo všeobecnosti zakazuje spracúvanie osobných údajov, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby, pričom však Nariadenie ako aj Zákon pripúšťajú výnimky z tohto pravidla (čl. 9 ods. 2 Nariadenia a § 16 ods. 2 Zákona).

Krátky prehľad jednotlivých inštitútov týkajúcich sa ochrany osobných údajov podľa Nariadenia a Zákona

Nariadenie prináša oproti Pôvodnému zákonu viaceré nové pojmy ako napríklad: profilovanie, pseudonymizácia, porušovanie ochrany osobných údajov, genetické údaje, údaje týkajúce sa zdravia, hlavná prevádzkareň, zástupca, podnik, skupina podnikov, dozorný orgán, dotknutý dozorný orgán, relevantná a odôvodnená námietka, služba informačnej spoločnosti, medzinárodná organizácia, atď.. Tieto sú definované predovšetkým v čl. 4 Nariadenia.

Nakoľko dochádza k zavedeniu viacerých nových pojmov je potrebné si definovať aspoň niektoré z nich.

Pod pojmom „*spracúvanie*“ sa rozumie operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovaním iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.

Pod pojmom „*profilovanie*“ sa rozumie akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spolahľivosťou, správaním, polohou alebo pohybom.

Pod pojmom „*pseudonymizácia*“ sa rozumie spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe.

Pod pojmom „*šifrovanie*“ sa rozumie transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo.

Súčasne je potrebné definovať osoby, ktoré nejakým spôsobom spracúvajú osobné údaje:

Pod pojmom „*dotknutá osoba*“ sa rozumie každá fyzická osoba, ktorej osobné údaje sa spracúvajú.

Pod pojmom „*prevádzkovateľ*“ sa rozumie fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu.

Pod pojmom „*sprostredkovateľ*“ sa rozumie fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.

Pod pojmom „*príjemca*“ sa rozumie fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom Únie alebo právom členského štátu, sa však nepovažujú za príjemcov; spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s uplatniteľnými pravidlami ochrany údajov v závislosti od účelov spracúvania.

Pod pojmom „*tretia strana*“ sa rozumie fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov.

Je potrebné uviesť, že Nariadenie ako aj Zákon je postavený na tom, že osobné údaje musia byť:

- a) spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe („zákonnosť, spravodlivosť a transparentnosť“);
- b) získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi; ďalšie spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či štatistické účely sa v súlade s článkom 89 ods. 1 nepovažuje za nezlučiteľné s pôvodnými účelmi („obmedzenie účelu“);
- c) primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú („minimalizácia údajov“);
- d) správne a podľa potreby aktualizované; musia sa prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia („správnosť“);
- e) uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú; osobné údaje sa môžu uchovávať dlhšie, pokiaľ sa budú spracúvať výlučne na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely v súlade s článkom 89 ods. 1 Zákona za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných týmto nariadením na ochranu práv a slobôd dotknutých osôb („minimalizácia uchovávaní“);
- f) spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení („integrita a dôvernosť“).

Právny základ spracúvania osobných údajov:

Spracúvanie osobných údajov je v súlade s Nariadením a Zákonom zákonné, ak sa vykonáva na základe aspoň jedného z týchto právnych základov:

- a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel,
- b) spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby,
- c) spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
- d) spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby,
- e) spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, alebo
- f) spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh.

Novou právnou úpravou ochrany osobných údajov dochádza k zrušeniu právneho základu spracúvania osobných údajov podľa § 10 ods. 3 písm. d) Pôvodného zákona „priamy marketing v poštovom styku“, taktiež dochádza k zrušeniu právneho základu spracúvania osobných údajov podľa § 10 ods. 3 písm. e) Pôvodného zákona „ďalšie spracúvanie už zverejnených osobných údajov“, taktiež dochádza k zrušeniu právneho základu podľa § 15 ods. 4 Pôvodného zákona „jednorazový vstup“, taktiež dochádza k zrušeniu právneho základu podľa § 15 ods. 7 Pôvodného zákona „monitorovanie priestorov prístupných verejnosti“. Ak teda prevádzkovateľ zistí, že spracúva osobné údaje dotknutých osôb na niektorom právnom základe, ktorý bude zrušený s účinnosťou novej právnej úpravy, bude musieť nájsť a disponovať iným primeraným právnym základom.

Súhlas so spracúvaním osobných údajov:

Novou právnou úpravou sa bližšie určujú obsahové a formálne podmienky súhlasu, ako právneho základu na spracúvanie osobných údajov, pričom:

- a) súhlas by sa mal poskytnúť jasným prejavom vôle, ktorý je slobodným, konkrétnym, informovaným a jednoznačným vyjadrením súhlasu dotknutej osoby so spracúvaním osobných údajov, ktoré sa jej týkajú,
- b) súhlas sa má vzťahovať na všetky spracovateľské činnosti vykonávané na ten istý účel alebo účely,
- c) ak sa spracúvanie vykonáva na viaceré účely, súhlas sa má udeliť/má byť oddelený/uvedený oddelene na všetky tieto účely,
- d) udelenie súhlasu musí byť jasne odlíšiteľné od iných skutočností, so súhlasom na spracúvanie osobných údajov nesúvisiacich,
- e) súhlas má byť formulovaný v zrozumiteľnej a ľahko dostupnej forme, jasne a jednoducho,
- f) informovanie o možnosti súhlas odvolať musí byť také jednoduché, ako poskytnutie súhlasu,
- g) zákaz podmieňovať súhlas so spracúvaním osobných údajov, ktorý nie je na plnenie zmluvy, vrátane poskytnutia služby, nevyhnutný.

Povinnosti prevádzkovateľa z pohľadu jeho informačnej povinnosti

Nová právna úprava ustanovuje prevádzkovateľovi povinnosť, ak sa od dotknutej osoby získavajú osobné údaje, ktoré sa jej týkajú, aby dotknutej osobe pri ich získavaní poskytol nasledovné informácie:

- a) identifikačné údaje a kontaktné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený,
- b) kontaktné údaje zodpovednej osoby, ak je určená,
- c) účel spracúvania osobných údajov, na ktorý sú osobné údaje určené, ako aj právny základ spracúvania osobných údajov,
- d) oprávnené záujmy prevádzkovateľa alebo tretej strany, ak sa osobné údaje spracúvajú podľa § 13 ods. 1 písm. f) Zákona,
- e) identifikáciu príjemcu alebo kategóriu príjemcu, ak existuje,
- f) informáciu o tom, že prevádzkovateľ zamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii, identifikáciu tretej krajiny alebo medzinárodnej organizácie, informáciu o existencii alebo neexistencii rozhodnutia Európskej komisie (ďalej len „Komisia“) o primeranosti alebo odkaz na primerané záruky alebo vhodné záruky a prostriedky na získanie ich kópie alebo informáciu o tom, kde boli sprístupnené, ak prevádzkovateľ zamýšľa prenos podľa § 48 ods. 2, § 49 alebo § 51 ods. 1 a 2 Zákona.

Okrem vyššie uvedených informácií je prevádzkovateľ povinný pri získavaní osobných údajov poskytnúť dotknutej osobe informácie o

- a) dobe uchovávaní osobných údajov; ak to nie je možné, informácie o kritériách jej určenia,
- b) práve požadovať od prevádzkovateľa prístup k osobným údajom týkajúcich sa dotknutej osoby, o práve na opravu osobných údajov, o práve na vymazanie osobných údajov alebo o práve na obmedzenie spracúvania osobných údajov, o práve namietať spracúvanie osobných údajov, ako aj o práve na prenosnosť osobných údajov,
- c) práve kedykoľvek svoj súhlas odvolať,
- d) práve podať návrh na začatie konania podľa § 100 Zákona,
- e) tom, či je poskytovanie osobných údajov zákonnou požiadavkou alebo zmluvnou požiadavkou alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, a o tom, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj o možných následkoch neposkytnutia osobných údajov,
- f) existencii automatizovaného individuálneho rozhodovania vrátane profilovania podľa § 28 ods. 1 a 4 Zákona; v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie o použítom postupe, ako aj o význame a predpokladaných dôsledkoch takého spracúvania osobných údajov pre dotknutú osobu.

Ak osobné údaje neboli získané od dotknutej osoby, prevádzkovateľ je povinný dotknutej osobe poskytnúť

- a) identifikačné údaje a kontaktné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený,
- b) kontaktné údaje zodpovednej osoby, ak je určená,
- c) účel spracúvania osobných údajov, na ktorý sú osobné údaje určené, ako aj právny základ spracúvania osobných údajov,
- d) kategórie spracúvaných osobných údajov,
- e) identifikáciu príjemcu alebo kategóriu príjemcu, ak existuje,
- f) informáciu o tom, že prevádzkovateľ zamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii, identifikáciu tretej krajiny alebo medzinárodnej organizácie, informáciu o existencii alebo neexistencii rozhodnutia Komisie o primeranosti alebo odkaz na primerané záruky alebo vhodné záruky a

prostriedky na získanie ich kópie alebo informáciu o tom, kde boli sprístupnené, ak prevádzkovateľ zamýšľa prenos podľa § 48 ods. 2, § 49 alebo § 51 ods. 1 a 2 Zákona.

Okrem vyššie uvedených informácií je prevádzkovateľ povinný poskytnúť dotknutej osobe informácie o

- a) dobe uchovávaní osobných údajov; ak to nie je možné, informáciu o kritériách jej určenia,
- b) oprávnených záujmoch prevádzkovateľa alebo tretej strany, ak sa spracúvajú osobné údaje podľa § 13 ods. 1 písm. f) Zákona,
- c) práve požadovať od prevádzkovateľa prístup k osobným údajom týkajúcich sa dotknutej osoby o práve na opravu osobných údajov, o práve na vymazanie osobných údajov alebo o práve na obmedzenie spracúvania osobných údajov, o práve namietat' spracúvanie osobných údajov, ako aj o práve na prenosnosť osobných údajov,
- d) práve kedykoľvek svoj súhlas odvolať,
- e) práve podať návrh na začatie konania podľa § 100 Zákona,
- f) zdroji, z ktorého pochádzajú osobné údaje, prípadne informácie o tom, či pochádzajú z verejne prístupných zdrojov,
- g) existencii automatizovaného individuálneho rozhodovania vrátane profilovania podľa § 28 ods. 1 a 4 Zákona; v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie o použítom postupe, ako aj o význame automatizovaného individuálneho rozhodovania a predpokladaných dôsledkoch takého spracúvania osobných údajov pre dotknutú osobu.

Zákon ustanovuje aj taxatívne prípady a podmienky, kedy prevádzkovateľ nemá povinnosť poskytnúť dotknutej osobe informácie uvedené vyššie v písm. a) až g), ak osobné údaje prevádzkovateľ nezískal priamo od dotknutej osoby, ide o nasledovné prípady:

- a) v rozsahu, v akom dotknutá osoba už dané informácie má,
- b) v rozsahu, v akom sa poskytovanie týchto informácií ukáže ako nemožné alebo by si vyžadovalo neprimerané úsilie, najmä ak sa spracúvajú osobné údaje na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, na ktorý sa vzťahujú podmienky a záruky podľa § 78 ods. 8 Zákona, alebo ak je pravdepodobné, že povinnosť uvedená v odseku 1 znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takého spracúvania osobných údajov; prevádzkovateľ je v takom prípade povinný prijať vhodné opatrenia na ochranu práv a oprávnených záujmov dotknutej osoby vrátane sprístupnenia daných informácií verejnosti,
- c) v rozsahu, v akom sa získanie týchto informácií alebo poskytnutie týchto informácií ustanovuje v osobitnom predpise, ktorý sa na prevádzkovateľa vzťahuje a v ktorom sú ustanovené primerané opatrenia na ochranu práv a oprávnených záujmov dotknutej osoby, alebo
- d) ak osobné údaje musia zostať dôverné na základe povinnosti mlčanlivosti podľa osobitného predpisu.

Práva dotknutej osoby

Podľa Nariadenia a Zákona má dotknutá osoba bližšie špecifikované aj svoje práva, ktoré môže využiť vo vzťahu k spracovaným osobným údajom. Tieto sú nasledovné:

- a) právo na prístup k osobným údajom,
- b) právo na opravu osobných údajov,
- c) právo na výmaz osobných údajov (resp. právo na zabudnutie),
- d) právo na obmedzenie spracúvania osobných údajov,
- e) právo na prenosnosť osobných údajov,
- f) právo namietat' spracúvanie osobných údajov,
- g) právo namietat' automatizované individuálne rozhodovanie a profilovanie.

Povinnosti prevádzkovateľa

Poverenie spracovania osobných údajov sprostredkovateľom

Ak sa má spracúvanie osobných údajov uskutočniť v mene prevádzkovateľa, prevádzkovateľ môže poveriť len sprostredkovateľa, ktorý poskytuje dostatočné záruky na prijatie primeraných technických a organizačných opatrení tak, aby spracúvanie osobných údajov spĺňalo požiadavky tohto zákona a aby sa zabezpečila ochrana práv dotknutej osoby. Na poverenie sprostredkovateľa spracúvaním osobných údajov podľa prvej vety sa súhlas dotknutej osoby nevyžaduje.

Spracúvanie osobných údajov sprostredkovateľom sa riadi zmluvou alebo iným právnym úkonom, ktorý zaväzuje sprostredkovateľa voči prevádzkovateľovi a v ktorom je ustanovený predmet a doba spracúvania, povaha a účel spracúvania, zoznam alebo rozsah osobných údajov, kategórie dotknutých osôb a povinnosti a práva prevádzkovateľa.

V zmluve alebo inom právnom úkone sa musí najmä ustanoviť, že sprostredkovateľ je povinný:

- a) spracúvať osobné údaje len na základe písomných pokynov prevádzkovateľa, a to aj vtedy, ak ide o prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii okrem prenosu na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná; sprostredkovateľ je pri takom prenose povinný oznámiť prevádzkovateľovi túto požiadavku pred spracúvaním osobných údajov, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, takéto oznámenie nezakazuje z dôvodov verejného záujmu,
- b) zabezpečiť, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovávajú mlčanlivosť o informáciách, o ktorých sa dozvedeli, ak nie sú viazané povinnosťou mlčanlivosti podľa osobitného zákona,
- c) vykonať opatrenia podľa § 39 Zákona,
- d) dodržiavať podmienky zapojenia ďalšieho sprostredkovateľa podľa odsekov 2 a 5 § 34 Zákona,
- e) po zohľadnení povahy spracúvania osobných údajov v čo najväčšej miere poskytnúť súčinnosť prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti prijímať opatrenia na základe žiadosti dotknutej osoby podľa druhej časti druhej hlavy,
- f) poskytnúť súčinnosť prevádzkovateľovi pri zabezpečovaní plnenia povinností podľa § 39 až 43 Zákona s prihliadnutím na povahu spracúvania osobných údajov a informácie dostupné sprostredkovateľovi,
- g) vymazať osobné údaje alebo vrátiť prevádzkovateľovi osobné údaje po ukončení poskytovania služieb týkajúcich sa spracúvania osobných údajov na základe rozhodnutia prevádzkovateľa a vymazať existujúce kópie, ktoré obsahujú osobné údaje, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto osobných údajov,
- h) po ukončení poskytovania služieb týkajúcich sa spracúvania osobných údajov na základe rozhodnutia prevádzkovateľa osobné údaje vymazať alebo vrátiť prevádzkovateľovi a vymazať existujúce kópie, ktoré obsahujú osobné údaje, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto osobných údajov,
- i) poskytnúť prevádzkovateľovi informácie potrebné na preukázanie splnenia povinností a poskytnúť súčinnosť v rámci auditu ochrany osobných údajov a kontroly zo strany prevádzkovateľa alebo audítora, ktorého poveril prevádzkovateľ.

Záznam o spracovateľských činnostiach

V čase účinnosti Pôvodného zákona bol prevádzkovateľ povinný v prípade spracúvania osobných údajov v informačnom systéme, oznamovať takúto skutočnosť Úradu na ochranu osobných údajov Slovenskej republiky (ďalej len „Úrad“) ako aj v niektorých prípadoch vykonať osobitnú registráciu takéhoto programu. Podľa Nariadenia a Zákona takáto povinnosť je už zrušená, pričom ju nahrádza nový inštitút a to „Záznam o spracovateľských činnostiach.“

Každý prevádzkovateľ a zástupca prevádzkovateľa, ak bol poverený, je povinný viesť záznam o spracovateľských činnostiach, za ktoré je zodpovedný. Tento záznam musí obsahovať

- a) identifikačné údaje a kontaktné údaje prevádzkovateľa, spoločného prevádzkovateľa, zástupcu prevádzkovateľa, ak bol poverený, a zodpovednej osoby,
- b) účel spracúvania osobných údajov,
- c) opis kategórií dotknutých osôb a kategórií osobných údajov,
- d) kategórie príjemcov vrátane príjemcu v tretej krajine alebo medzinárodnej organizácii,
- e) označenie tretej krajiny alebo medzinárodnej organizácie, ak prevádzkovateľ zamýšľa prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii a dokumentáciu o primeraných zárukách, ak prevádzkovateľ zamýšľa prenos podľa § 51 ods. 1 a 2 Zákona,
- f) predpokladané lehoty na vymazanie rôznych kategórií osobných údajov,
- g) všeobecný opis technických a organizačných bezpečnostných opatrení podľa § 39 ods. 1 Zákona.

Vyššie uvedená povinnosť sa nevzťahuje na zamestnávateľa s menej ako 250 zamestnancami, ak nie je pravdepodobné, že spracúvanie osobných údajov, ktoré vykonáva, povedie k riziku ochrany práv dotknutej osoby, ak je spracúvanie osobných údajov príležitostné alebo ak nezáhŕňa osobitné kategórie osobných údajov podľa § 16 ods. 1 Zákona alebo osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 Zákona.

Prevádzkovateľ alebo sprostredkovateľ a zástupca prevádzkovateľa alebo zástupca sprostredkovateľa, ak bol poverený, sú povinní na požiadanie sprístupniť záznam o spracovateľských činnostiach Úradu.

Vzor záznamu o spracovateľských činnostiach zverejní Úrad na svojom webovom sídle.

Bezpečnosť spracúvania osobných údajov

Prevádzkovateľ a sprostredkovateľ sú súčasne povinní prijať so zreteľom na najnovšie poznatky, na náklady na vykonanie opatrení, na povahu, rozsah, kontext a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzických osôb primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti primeranej tomuto riziku, pričom uvedené opatrenia môžu zahŕňať najmä

- a) pseudonymizáciu a šifrovanie osobných údajov,
- b) zabezpečenie trvalej dôverylosti, integrity, dostupnosti a odolnosti systémov spracúvania osobných údajov,
- c) proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického incidentu alebo technického incidentu,
- d) proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov.

Prevádzkovateľ je povinný oznámiť Úradu porušenie ochrany osobných údajov do 72 hodín po tom, ako sa o ňom dozvedel; to neplatí, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby. V prípade ak dôjde k porušeniu ochrany osobných údajov dotknutej osoby, prevádzkovateľ je povinný bez zbytočného odkladu oznámiť dotknutej osobe porušenie ochrany osobných údajov, ak takéto porušenie ochrany osobných údajov môže viesť k vysokému riziku pre práva fyzickej osoby.

Posúdenie vplyvu na ochranu osobných údajov

Prevádzkovateľ bol podľa Pôvodného zákona povinný vypracovať bezpečnostný projekt ako aj prijať bezpečnostné opatrenia.

Nová právna úprava zakotvila povinnosť prevádzkovateľa posúdiť vplyv na ochranu osobných údajov podľa čl. 35 Nariadenia a § 42 Zákona, ktoré musí obsahovať aspoň:

Posúdenie vplyvu na ochranu osobných údajov obsahuje najmä:

- a) systematický opis plánovaných spracovateľských operácií a účel spracúvania osobných údajov vrátane uvedenia prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ,
- b) posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu,
- c) posúdenie rizika pre práva dotknutej osoby a
- d) opatrenia na elimináciu rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto zákonom s prihliadnutím na práva a oprávnené záujmy dotknutej osoby a ďalších fyzických osôb, ktorých sa to týka.

Zoznam spracovateľských operácií, ktoré podliehajú posúdeniu vplyvov zverejní Úrad.

Výsledok posúdenia by sa mal zohľadniť pri stanovení primeraných opatrení, ktoré sa majú prijať s cieľom preukázať, že spracúvanie osobných údajov je v súlade s Nariadením a Zákonom. Ak sa na základe posúdenia vplyvu na ochranu údajov ukáže, že spracovateľské operácie zahŕňajú vysoké riziko, ktoré prevádzkovateľ nemôže zmierniť primeranými opatreniami, pokiaľ ide o najnovšie technológie a náklady na vykonanie opatrení, mala by sa pred spracúvaním uskutočniť konzultácia s Úradom. Prevádzkovateľ prípadne sprostredkovateľ je povinný požiadať Úrad o predchádzajúcu konzultáciu.

Zodpovedná osoba

Prevádzkovateľ a sprostredkovateľ sú povinní určiť zodpovednú osobu, ak

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

Zodpovedná osoba sa určí na základe jej odborných kvalít, a to najmä na základe jej odborných znalostí práva a postupov v oblasti ochrany osobných údajov a na základe spôsobilosti plniť úlohy podľa § 46 Zákona. Zodpovedná osoba môže byť zamestnancom prevádzkovateľa alebo sprostredkovateľa alebo môže plniť úlohy na

základe zmluvy. Ďalšou základnou požiadavkou na zodpovednú osobu je, aby konala nezávisle (absencia konfliktu záujmov), tzn. že zodpovedná osoba nemôže v organizácii zastávať pozíciu, v ktorej by určovala účely a prostriedky spracúvania osobných údajov (napr. generálny riaditeľ, výkonný riaditeľ). Prevádzkovateľ a sprostredkovateľ sú povinní zverejniť, napríklad na ich webovom sídle, kontaktné údaje zodpovednej osoby, ak je určená, a oznámiť ich úradu. Zákon výslovne nevyžaduje, aby prevádzkovateľ/sprostredkovateľ zverejnil meno a priezvisko zodpovednej osoby ale zverejnil kontaktné údaje napr. na svojom webovom sídle vo forme adresy a e-mailu, na ktorom je zodpovedná osoba zastihnuteľná (z dôvodu, že sa môže zmeniť kontaktná osoba je vhodnejšie zvoliť všeobecnú e-mailovú adresu, napr. zodpovednaosoba@nazovspolocnosti.sk). Úradu je však potrebné oznámiť skutočné údaje zodpovednej osoby.

Zodpovedná osoba najmä

- a) poskytuje informácie a poradenstvo prevádzkovateľovi alebo sprostredkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa tohto zákona, osobitných predpisov alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná, týkajúcich sa ochrany osobných údajov,
- b) monitoruje súlad s týmto zákonom, osobitnými predpismi alebo medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, týkajúcimi sa ochrany osobných údajov a s pravidlami prevádzkovateľa alebo sprostredkovateľa súvisiacimi s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy osôb, ktoré sú zapojené do spracovateľských operácií a súvisiacich auditov ochrany osobných údajov,
- c) poskytuje na požiadanie poradenstvo, ak ide o posúdenie vplyvu na ochranu osobných údajov a monitorovanie jeho vykonávania podľa § 42 Zákona,
- d) spolupracuje s úradom pri plnení svojich úloh,
- e) plní úlohy kontaktného miesta pre úrad v súvislosti s otázkami týkajúcimi sa spracúvania osobných údajov vrátane predchádzajúcej konzultácie podľa § 43 Zákona a podľa potreby aj konzultácie v iných veciach.

Zodpovedná osoba pri výkone svojich úloh náležite zohľadňuje riziko spojené so spracovateľskými operáciami, pričom berie do úvahy povahu, rozsah, kontext a účel spracúvania osobných údajov.

Kódex správania, Certifikát

Ďalšou novinkou v novej právnej úprave je inštitút Kódexu správania a Certifikátu.

Združenie zastupujúce kategóriu prevádzkovateľov alebo sprostredkovateľov alebo iný subjekt zastupujúci kategóriu prevádzkovateľov alebo sprostredkovateľov môže prijať kódex správania, a to najmä na účely spresnenia uplatňovania Zákona v súvislosti s predmetom kódexu správania. V takýchto kódexoch správania sa majú nastaviť povinnosti prevádzkovateľov a sprostredkovateľov so zreteľom na riziko, ktoré pravdepodobne vyplýva zo spracúvania, pokiaľ ide o práva a slobody fyzických osôb. Schválením kódexu správania zo strany Úradu nie je dotknutá zodpovednosť prevádzkovateľa alebo zodpovednosť sprostredkovateľa dodržiavať Zákon ako aj Nariadenie.

S cieľom zlepšiť transparentnosť a posilniť súlad s Nariadením by sa malo podporiť vytvorenie mechanizmov certifikácie a pečatí a značiek ochrany údajov, aby sa dotknutým osobám umožnilo rýchlo posúdiť úroveň ochrany osobných údajov v prípade relevantných produktov a služieb. Certifikácia by mala byť vykonaná na účely preukázania súladu s Nariadením, pokiaľ ide o spracovateľské operácie vykonávané prevádzkovateľmi a sprostredkovateľmi. Certifikáciou sa však neznižuje zodpovednosť prevádzkovateľa alebo sprostredkovateľa dodržiavať Nariadenie a Zákon.

Správne delikty

Úrad môže za porušenie povinností bližšie definovaných v § 104 ods. 1 Zákona uložiť pokutu do 10.000.000,-Eur, alebo ak ide o podnik do 2 % celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia.

Úrad môže za porušenie povinností bližšie definovaných v § 104 ods. 2 Zákona uložiť pokutu do 20.000.000,-Eur, alebo ak ide o podnik do 4 % celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia.

III. Záver

S prihliadnutím na vyššie uvedené skutočnosti je potrebné, za účelom čo najúplnejšieho zistenia povinností, ktoré musí prevádzkovateľ splniť, vykonať nasledovné zistenia:

Potrebuje zistiť:

- a) či u neho dochádza k spracovaniu osobných údajov a ak áno, tak akých,
- b) za akým účelom dochádza k spracovaniu osobných údajov,
- c) na akom právnom základe dochádza k spracovaniu osobných údajov
- d) aké spracovateľské operácie vykonáva,
- e) komu poskytuje osobné údaje,
- f) akým spôsobom spracúva osobné údaje a súčasne aj kde spracúva,
- g) akým informačným systémom spracováva osobné údaje,
- h) okamih získania osobných údajov.

Prevádzkovateľ potrebuje:

- a) identifikovať všetky zmluvy, v ktorých vystupuje ako zmluvná strana, a ktoré majú odkaz na Pôvodný zákon,
- a) identifikovať všetky jeho interné smernice, v ktorých je odkaz na Pôvodný zákon,
- b) urobiť zoznam sprostredkovateľov,
- c) zistiť v ktorých prípadoch má k dispozícii súhlasy so spracúvaním osobných údajov (a to bez ohľadu na formu súhlasov) podľa Pôvodného zákona a zistiť v akom sú rozsahu,
- d) pripraviť na webovom portáli záložku/kolónku ohľadne ochrany osobných údajov a pripraviť špeciálnu emailovú adresu na zodpovednú osobu.

Po zistení vyššie uvedených skutočností je potrebné, aby prevádzkovateľ minimálne vykonal nasledovné úkony:

- a) zistil (v súlade s ustanoveniami Nariadenia a Zákona) či je potrebné aby mal ustanovenú zodpovednú osobu,
- b) pripravil si v prípade potreby nové poučenia pre dotknuté osoby a to v súlade s Nariadením a Zákonom a v prípade potreby tieto zaslal dotknutým osobám,
- c) zistil, či je potrebné vykonať Záznam o spracovateľských činnostiach,
- d) vykonať posúdenie vplyvu na ochranu osobných údajov,
- e) v prípade ak sú osobné údaje spracovávané sprostredkovateľom je potrebné zvážiť uzavretie novej zmluvy, ktorá bude reflektovať znenie Zákona a Nariadenia.

Nakoľko ustanovenia Zákona a Nariadenia sú vcelku obširne, pričom neexistuje zatiaľ žiadna právna prax ohľadne ich aplikácie v praxi, je potrebné u každého prevádzkovateľa a sprostredkovateľa osobitne posúdiť rozsah činností, ktoré majú tieto subjekty vykonať za účelom splnenia si svojich povinností vyplývajúcich z Nariadenia a Zákona.