zákona o zdravotnom poistení]. Splnenie tejto povinnosti zamestnancom je pre zamestnávateľa ako platiteľa poistného na zdravotné poistenie dôležité. Z pôvodnej zdravotnej poisťovne, z ktorej zamestnanec odišiel, je zamestnávateľ povinný zamestnanca odhlásiť a prihlásiť ho do novej zdravotnej poisťovne, ktorú si zamestnanec vybral, a preto zamestnávatelia často dobrovoľne vyzývajú svojich zamestnancov na aktualizáciu toho údaja, aj keď nemusia.

4.4 Právo na vymazanie (právo „na zabudnutie")

Právo na výmaz prestavuje inými slovami vyjadrenú povinnosť prevádzkovateľa zlikvidovať osobné údaje. V súlade s čl. 17 nariadenia a § 23 nového zákona o ochrane osobných údajov má dotknutá osoba právo na to, aby prevádzkovateľ bez zbytočného odkladu vymazal osobné údaje, ktoré sa jej týkajú, a to v týchto prípadoch:

- osobné údaje už nie sú potrebné na účel, na ktorý prevádzkovateľ tieto údaje získal alebo spracúval;
- dotknutá osoba odvolá svoj súhlas a neexistuje iný právny základ pre spracúvanie osobných údajov;
- dotknutá osoba namieta spracúvanie osobných údajov a neprevažujú žiadne oprávnené dôvody na spracúvanie osobných údajov;
- osobné údaje sa spracúvajú nezákonne;
- dôvodom pre výmaz je splnenie povinnosti podľa zákona o ochrane osobných údajov, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná;
- osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti podľa čl. 8 ods. 1 nariadenia alebo § 15 ods. 1 nového zákona o ochrane osobných údajov.

Dotknutá osoba má právo kedykoľvek odvolať súhlas so spracúvaním osobných údajov, ktoré sa jej týkajú, pričom súhlas môže odvolať rovnakým spôsobom, akým súhlas udelila. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov založenom na súhlase pred jeho odvolaním. Odvolanie súhlasu nemusí vždy pre prevádzkovateľa predstavovať aj povinnosť zlikvidovať osobné údaje, keďže súhlas bol daný k určitým účelom. Po odvolaní súhlasu je prevádzkovateľ povinný prestať

4.7 Právo namietať

Právo namietať spracúvanie osobných údajov patrí dotknutej osobe vtedy, ak sa domnieva, že spracúvanie už obmedzuje jej práva alebo do nich zasahuje a ak sa spracúvanie uskutočňuje:

- na právnom základe podľa čl. 6 ods. 1 písm. e) nariadenia alebo § 13 ods. 1 písm. e) nového zákona o ochrane osobných údajov, t. j. spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi;
- na právnom základe podľa čl. 6 ods. 1 písm. f) nariadenia alebo § 13 ods. 1 písm. f) nového zákona o ochrane osobných údajov, t. j. spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany; alebo
- na účel priameho marketingu vrátane profilovania v rozsahu, v akom súvisí s priamym marketingom.

Dôsledkom namietania spracúvania je to, že prevádzkovateľ ďalej nesmie spracúvať osobné údaje dotknutej osoby, pokiaľ nepreukáže nevyhnutné oprávnené záujmy na spracúvanie osobných údajov, ktoré prevažujú nad právami alebo záujmami dotknutej osoby, alebo dôvody na uplatnenie právneho nároku. V prípade spracúvania osobných údajov na účely priameho marketingu výnimka neexistuje a namietanie spracúvania na tieto účely má vždy za následok zastavenie ďalšieho spracúvania osobných údajov.

Dotknutá osoba nemá právo namietať spracúvanie osobných údajov, ak ide o spracúvanie nevyhnutné na plnenie úlohy z dôvodov verejného záujmu a spracúvanie na vedecký účel, na účel historického výskumu alebo na štatistický účel, t. j. na tzv. privilegované účely.

Certifikačným subjektom, ktorý zabezpečuje vydanie, obnovu alebo odňatie certifikátu, môže byť právnická osoba alebo fyzická osoba — podnikateľ, ktorým bola úradom udelená akreditácia. Certifikačný subjekt musí mať primeranú úroveň odborných znalostí vo vzťahu k ochrane osobných údajov a vo svojom prostredí musí mať vytvorené technické a organizačné podmienky na certifikačný postup. V čase prípravy publikácie boli podrobnejšie podmienky pre certifikačné kritériá, akreditačné kritériá, postupy, dokumentáciu audítorov vo fáze prípravy, a preto ich nemožno bližšie konkretizovať.

Vychádzajúc z ustanovení čl. 64 nariadenia, ktorý požaduje návrh rozhodnutia v súvislosti s návrhom kritérií na akreditáciu monitorovacieho subjektu alebo akreditáciu certifikačného subjektu pred ich prijatím v členskom štáte, bude môcť právnická osoba alebo fyzická osoba — podnikateľ požiadať o akreditáciu až po ich schválení výborom[75] a následnom vydaní vo vykonávacom predpise (pred ich schválením by to mohlo byť neefektívne vzhľadom na to, že subjekty nebudú vedieť, aké kritériá majú splniť). Vzhľadom na to, že výbor začne fakticky existovať a pracovať až od 25. mája 2018, kedy sa začne uplatňovať nariadenie, berúc do úvahy aj proces posudzovania udelenia akreditácie, bude existencia akreditovaného monitorovacieho alebo certifikačného subjektu reálne pravdepodobná najskôr ku koncu roka 2018. Udeľovanie certifikácie bude do schválenia postupov výborom výlučne v právomoci úradu na základe certifikačných kritérií vydaných vo vykonávacom predpise.

7.3 Pseudonymizácia

Pseudonymizácia ako jeden z prvokov špecificky navrhnutej ochrany osobných údajov (čl. 25 nariadenia) slúži na zvýšenie bezpečného spracúvania osobných údajov prevádzkovateľom alebo sprostredkovateľom. Zavedenie pseudonymizácie ako prvku ochrany a bezpečnosti by malo podliehať dôslednému posúdeniu stavu spracúvania osobných údajov (napr. audit spracúvania osobných údajov), pričom dôležitým faktorom je posúdenie, či pseudonymizácia reálne povedie k zvýšeniu bezpečnosti spra-

[75] Európsky výbor pre ochranu údajov zriadený podľa čl. 68 nariadenia ako orgán únie s právnou subjektivitou.

cúvaných osobných údajov. Pseudonymizáciu nemožno vnímať ako opatrenie, ktoré zaručene povedie k zvýšeniu bezpečnosti, vždy treba posúdiť všetky okolnosti aplikácie, aby sa predišlo napr. situácii, že osoba, ktorá je prevádzkovateľom poverená spracúvaním osobných údajov, nebude mať potrebné osobné údaje dostupné v čase, kedy budú nevyhnutné na vykonanie spracovateľských operácií (porušenie jedného zo základných princípov bezpečnosti — dostupnosť údajov). Pseudonymizácia by teda mala byť aplikovaná len tam, kde existuje reálny predpoklad ohrozenia osobných údajov (napr. pri prenášaní údajov na externom dátovom nosiči). Aplikácia akýchkoľvek bezpečnostných prvkov mi mala zodpovedať reálnej potrebe, podmienkam spracúvania a mala by byť primeraná.

Príklad č. 18:

Prevádzkovateľ, ktorý poskytuje služby v oblasti poistenia, požiada externú spoločnosť o vytvorenie skóringového modelu, ktorý vytvára na základe existujúcich informácií o klientoch. Vzhľadom na to, že ide o extrémne citlivé údaje (vrátane údajov o zdraví), prevádzkovateľ pseudonymizuje údaje takým spôsobom, že všetky identifikátory, ktoré nie sú potrebné k vypracovaniu skóringového modelu, prevedie do kódu, ku ktorému bude kľúčom disponovať výlučne vo svojich podmienkach. Externý subjekt, ktorému budú informácie poskytnuté, tak bude disponovať množstvom dát (napr. číslo — údaje o zdraví, údaje o platobnej schopnosti, údaje o iných využívaných službách a pod.), pričom ich nikdy, za žiadnych podmienok nebude schopný priradiť k dotknutej osobe. Pre externý subjekt tak pôjde o anonymizované údaje a prevádzkovateľ ani externý subjekt nemusia hľadať právny základ na ich poskytnutie. Avšak prevádzkovateľ musí mať právny základ pre vyhotovenie skóringového modelu. Pre prevádzkovateľa to budú vždy osobné údaje, ktoré po vytvorení skóringového modelu nadobudnú inú kvalitu.

Pseudonymizácia je tak spracúvaním osobných údajov v takej forme, že dotknutú osobu je vždy možné identifikovať, avšak až po aplikácii dodatočných informácií, napr. kľúča. Pseudonymizované údaje sú stále osobnými údajmi a vzťahujú sa na ne všetky podmienky nariadenia.