DRUH PREDPISU	ČÍSLO	Účinnosť od	25.5.2018
Smernica	253	Verzia	2
		Počet strán	27
		Počet príloh	1

OCHRANA OSOBNÝCH ÚDAJOV

Vypracoval:	Gestorský útvar:	Schválil:
JUDr. Martin Grešo Dátum: 7.5.2018 Podpis:	Úsek právny a compliance JUDr. Martin Grešo Dátum: 7.5.2018 Podpis:	predstavenstvo Dátum: 22.5.2018
Predpisom sa mení:	predchádzajúca verzia (1) smernice o ochrane osobných údajov	
Predpisom sa ruší:		
Predpis je určený pre:	Všetkých zamestnancov	

Kľúčové slová	osobný údaj, prevádzkovateľ, sprostredkovateľ, spracúvanie osobných údajov, marketingový súhlas, PIA, vlastníci údajov, Big data, cookies

Obsah

Článok I
Účel úpravy

Účelom tejto smernice je upraviť pravidlá pre ochranu osobných údajov fyzických osôb pri spracúvaní ich osobných údajov v podmienkach spoločnosti Union zdravotná poisťovňa, a.s (ďalej len „zdravotná poisťovňa").

Článok II
Právny rámec

Na ochranu osobných údajov sa vzťahuje nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 zo dňa 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane osobných údajov), smernica Európskeho parlamentu a Rady (EÚ) 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), zákon č. 351/2011 Z.z. o elektronických komunikáciách a zákon č. 18/2018 Z.z. o ochrane osobných údajov (ďalej spolu len „právne predpisy pre oblasť ochrany osobných údajov").
Táto smernica vychádza z predpisu na ochranu osobných údajov materskej spoločnosti (Privacy Policy Achmea B.V.).

Článok III
Predmet úpravy

Táto smernica upravuje:

a) zásady spracúvania osobných údajov,
b) organizačné zabezpečenie ochrany osobných údajov,
c) účel spracúvania osobných údajov,
d) okruhy dotknutých osôb,
e) ochranu práv dotknutých osôb,
f) základné zásady bezpečnosti spracúvania osobných údajov,
g) prenos osobných údajov do tretích krajín,
h) pravidlá pre nahlasovanie porušení ochrany osobných údajov,
i) následky porušenia pravidiel určených v tejto smernici.

Článok IV
Definícia pojmov

Osobné údaje sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby, pričom takou osobou 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, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.
Štandardne sa za osobné údaje považuje súbor informácií o dotknutej osobe, ktoré umožňujú jej identifikáciu. V niektorých prípadoch je údaj osobným údajom aj ak obsahuje len niektorý prvok, ako napríklad uchovávanie logov za účelom sledovania a zaznamenávania zmien v informačnom systéme alebo odhaľovania podvodov alebo vytvorenie personalizovanej ponuky na webe zdravotnej poisťovne. Prostriedok, na ktorom sú osobné údaje spracúvané nie je dôležitý, môže byť použitá klasická papierová forma, alebo obrázok, zvukový záznam, zvukovo-obrazový záznam a pod. Vždy však musí ísť o informáciu o určitej alebo určiteľnej osobe. Medzi osobné údaje nepatrí napríklad poštové smerové číslo, pokiaľ k nemu nie sú priradené ďalšie údaje. Rovnako osobnými

údajmi nie sú anonymizované údaje. Konkrétny údaj, ktorý nie je považovaný za osobný údaj, sa môže v budúcnosti stať osobným údajom, vzhľadom na neustály technologický rozvoj, ktorý môže priniesť ďalšie možnosti pre identifikáciu dotknutej osoby.

Dotknutá osoba je každá fyzická osoba, ktorej sa osobné údaje týkajú (najmä poistenec a jeho zástupcovia, poistenci iného členského štátu EÚ, tretia osoba, voči ktorej má zdravotná poisťovňa pohľadávku, svedok, regresovaný, zamestnanec zdravotnej poisťovne, pre účely výkonu agendy súvisiacej s pracovnoprávnymi vzťahmi, osoba žalovaná, osoba žalujúca).

Spracúvanie je 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 poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.

Prevádzkovateľ je osoba, ktorá sama alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene. Pre účely tejto smernice je zdravotná poisťovňa prevádzkovateľom, ak nie je vyslovene uvedené inak.

Sprostredkovateľ je osoba, ktorá spracúva osobné údaje v mene prevádzkovateľa (zdravotnej poisťovne).

Súhlas dotknutej osoby je akýkoľvek slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej týkajú.

Zodpovedná osoba (Data Protection Officer) je zamestnanec zdravotnej poisťovne na pracovnej pozícii riaditeľ úseku právneho a compliance. Pre viac informácií viď článok VII ods. 4 tejto smernice. Zodpovednosť za ochranu osobných údajov v rámci zdravotnej poisťovne majú všetci zamestnanci.

Článok V
Základné zásady spracúvania osobných údajov

1. Pri spracúvaní osobných údajov je zdravotná poisťovňa, jej zamestnanci a tiež jej zmluvní partneri povinní dbať na dodržiavanie základných zásad pri spracúvaní osobných údajov, ktorými sú:

   1.1. Zákonnosť, spravodlivosť a transparentnosť - osobné údaje musia byť spracúvané zákonný spôsobom, spravodlivo a transparentne. Inými slovami táto zásada je dodržaná, ak na spracúvanie osobných údajov existuje právny základ,

   1.2. Obmedzenie účelu - zdravotná poisťovňa je oprávnená získavať a spracúvať osobné údaje dotknutých osôb iba na konkrétny legitímny účel a spracúvať ich iba takým spôsobom a v rozsahu, ktorý je zlučiteľný s týmto účelom. Týmto nie je dotknutá možnosť spracúvania osobných údajov za účelom archivácie a štatistického spracúvania,

   1.3. Minimalizácia údajov - zdravotná poisťovňa je oprávnená získavať a spracúvať iba tie osobné údaje, ktoré sú relevantné a nevyhnutné pre účel spracovania,

   1.4. Správnosť - zdravotná poisťovňa je povinná zabezpečiť, aby osobné údaje boli správne a aktualizované a aby nesprávne, resp. neaktuálne údaje, ktoré nie sú z hľadiska účelu spracovania viac potrebné, bezodkladne zlikvidovala, resp. opravila.

   1.5. Minimalizácia uchovávania - zdravotná poisťovňa je povinná uchovávať osobné údaje iba dovtedy, pokým sú potrebné pre účel, na ktorý sa spracúvajú.

   1.6. Integrita, dôvernosť a dostupnosť - zdravotná poisťovňa je povinná pri spracúvaní osobných údajov zabezpečiť ich ochranu a bezpečnosť pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením.

   1.7. Zodpovednosť - zdravotná poisťovňa je zodpovedná za dodržiavanie týchto zásad a musí vedieť preukázať ich dodržiavanie a súlad.

Článok VI
Základné povinnosti pri spracúvaní osobných údajov

1. Každý zamestnanec zdravotnej poisťovne je povinný pri spracúvaní osobných údajov dodržiavať ustanovenia tejto smernice a právne predpisy pre oblasť ochrany osobných údajov.
2. Vedúci zamestnanci sú v rozsahu vecnej pôsobnosti nimi riadeného organizačného útvaru povinní v súlade s účelom spracúvania osobných údajov podľa článku VIII tejto smernice a s ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb prijať vhodné technické a organizačné opatrenia, aby zabezpečili a boli schopní preukázať, že spracúvanie sa vykonáva v súlade s touto smernicou a právnymi predpismi pre oblasť ochrany osobných údajov. Uvedené opatrenia sa podľa potreby preskúmajú a aktualizujú.
3. Vedúci zamestnanci sú v rozsahu vecnej pôsobnosti nimi riadeného organizačného útvaru povinní vykonať primerané technické a organizačné opatrenia, aby zabezpečili, že štandardne sa spracúvajú len osobné údaje, ktoré sú nevyhnutné pre každý konkrétny účel spracúvania. Uvedená povinnosť sa vzťahuje na množstvo získaných osobných údajov, rozsah ich spracúvania, dobu ich uchovávania a ich dostupnosť. Konkrétne sa takýmito opatreniami zabezpečí, aby osobné údaje neboli bez zásahu fyzickej osoby štandardne prístupné neobmedzenému počtu fyzických osôb.
4. V prípade pochybností ohľadne práv a povinností zdravotnej poisťovne pri spracúvaní osobných údajov sú zamestnanci povinní sa obrátiť na úsek právny a compliance a riadiť sa jeho usmerneniami.

Článok VII
Organizačné zabezpečenie ochrany osobných údajov

1. Poučenie zamestnancov o právach a povinnostiach pri spracúvaní osobných údajov

1.1. Odborná príprava zamestnancov sa realizuje formou:
   a) písomného poučenia o právach a povinnostiach ustanovených v tejto smernici a v právnych predpisoch pre oblasť ochrany osobných údajov a o zodpovednosti za ich porušenie, a to pred začatím výkonu, prác predmetom ktorých sú spracovateľské operácie s osobnými údajmi (teda v deň nástupu do zamestnania),
   b) školení realizovaných prostredníctvom e-Learningu raz za dva kalendárne roky,
   c) inými formami v prípade potreby, najmä ak dôjde k zásadnej zmene v spracovateľských operáciách alebo k zmene tejto smernice alebo právnych predpisoch pre oblasť ochrany osobných údajov.

1.2. Odborná príprava osôb pracujúcich na základe dohôd o prácach vykonávaných mimo pracovného pomeru sa realizuje formou:
   a) písomného poučenia o právach a povinnostiach ustanovených v tejto smernici a v právnych predpisoch pre oblasť ochrany osobných údajov a o zodpovednosti za ich porušenie, a to pred začatím výkonu, prác predmetom ktorých sú spracovateľské operácie s osobnými údajmi (teda v deň nástupu do zamestnania),
   b) inými formami v prípade potreby, najmä ak dôjde k zásadnej zmene v spracovateľských operáciách alebo k zmene tejto smernice alebo právnych predpisoch pre oblasť ochrany osobných údajov.

1.3. Odbornej prípravy sú povinní zúčastniť sa všetci zamestnanci (vrátane osôb pracujúcich na základe dohôd o prácach vykonávaných mimo pracovného pomeru).

1.4. Odbornú prípravu vykoná úsek riadenia ľudských zdroj na základe pravidiel určených úsekom právnym a compliance.

1.5. Úsek právny a compliance vytvorí formulár pre poučenie zamestnancov. Poučenie o právach a povinnostiach sa vyhotovuje dvojmo, z toho jedno vyhotovenie je určené pre zdravotnú poisťovňu a druhé pre zamestnanca. Vyhotovenie pre zdravotnú poisťovňu sa zakladá do osobného spisu zamestnanca na úseku riadenia ľudských zdrojov.

2. Mlčanlivosť

2.1. Zamestnanci sú povinní zachovávať mlčanlivosť o osobných údajoch, ktoré spracúvajú. Táto povinnosť trvá aj po ukončení spracúvania.

2.2. Povinnosť mlčanlivosti sa na zamestnancov nevzťahuje, len ak je to nevyhnutné na plnenie úloh orgánov činných v trestnom konaní.

2.3. Zamestnanci, ktorí prišli do styku s osobnými údajmi, nesmú tieto využiť pre osobnú potrebu a bez súhlasu zdravotnej poisťovne ich zverejniť a nesmú ich nikomu poskytnúť ani sprístupniť.

2.4. Povinnosť mlčanlivosti trvá aj po ukončení pracovného pomeru alebo obdobného pracovného vzťahu.

3. Vlastník osobných údajov

3.1. Vlastník osobných údajov je osoba zodpovedná za manažment osobných údajov, pričom určuje rozsah spracúvaných osobných údajov a spôsob ich spracúvania, vrátane podmienok pre ich sprístupnenie zamestnancom poisťovne alebo tretím stranám (konkrétne napr. odsúhlasuje matice prístupových práv, schvaľuje špeciálne prístupové práva a výnimky k prístupovým právam, schvaľuje udelenie hromadného prístupového práva). Pri tejto činnosti im pomáha Data Governance Manager spoločnosti.

3.2. Vlastníkom osobných údajov získaných v súvislosti s prijímaním prihlášok na verejné zdravotné poistenie a správou registra poistencov je riaditeľ úseku služieb klientom.

3.3. Vlastníkom osobných údajov získaných v súvislosti so zúčtovaním zdravotnej starostlivosti, schvaľovaním liečby a vykonávaním revíznych činností je riaditeľ úsek revíznych a zdravotných činností.

3.4. Vlastníkom osobných údajov, ktorými sú online identifikátory (napr. IP adresa, cookies) je riaditeľ úseku digitálneho marketingu.

3.5. Vlastníkom osobných údajov získaných a spracúvaných na pracovnoprávne účely je riaditeľ úseku riadenia ľudských zdrojov.

4. Zodpovedná osoba (Data Protection Officer)

4.1. Zodpovednou osobou je riaditeľ úseku právneho a compliance. Úlohy pri plnení tejto funkcie vykonávajú jednotliví zamestnanci úseku právneho a compliance, podľa pokynov riaditeľa úseku právneho a compliance. Kontaktné údaje zodpovednej osoby je zdravotná poisťovňa povinná zverejniť a oznámiť Úradu na ochranu osobných údajov.

4.2. Riaditeľ úseku právneho a compliance vykonáva svoju činnosť nezávisle a za plnenie úloh podľa tejto smernice zodpovedá predstavenstvu zdravotnej poisťovni.

4.3. Riaditeľ úseku právneho a compliance má neobmedzený prístup ku všetkým informáciám týkajúcich sa spracovateľských operácií.

4.4. Riaditeľ úseku právneho a compliance je oprávnený požadovať spoluprácu od všetkých zamestnancov zdravotnej poisťovne; v prípade ak zamestnanci zdravotnej poisťovne neposkytnú požadovanú súčinnosť riadne a/alebo včas, informuje riaditeľ úseku právneho a compliance generálneho riaditeľa a priameho nadriadeného dotknutého zamestnanca, za účelom prijatia ďalších opatrení.

4.5. Zdravotná poisťovňa kladie zvýšené hodnotové a vzdelanostné požiadavky na osobu, ktorá je zamestnaná na pracovnej pozícii riaditeľ úseku právneho a compliance, ktoré sú opísané

v osobitnej smernici s názvom Požiadavky na odbornú spôsobilosť a dôveryhodnosť členov predstavenstva spoločnosti a zamestnancov spoločnosti.

4.6. Riaditeľ úseku právneho a compliance ako zodpovedná osoba má najmä tieto úlohy:
   a) poskytuje informácie a poradenstvo zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa právnych predpisov pre oblasť ochrany osobných údajov,
   b) monitoruje súlad s touto smernicou, s právnymi predpismi pre oblasť ochrany osobných údajov a s pravidlami zdravotnej poisťovne v súvislosti s ochranou osobných údajov, vrátane rozdelenia povinností,
   c) určuje zodpovednosti jednotlivých organizačných útvarov alebo pracovných pozícií pri spracúvaní osobných údajov,
   d) zvyšuje povedomie a odbornú prípravu zamestnancov, ktorí sú zapojení do spracovateľských operácií,
   e) poskytuje poradenstvo orgánom zdravotnej poisťovne a zamestnancom,
   f) poskytuje poradenstvo pri vykonávaní posúdenia vplyvu na ochranu údajov a monitorovanie jeho vykonávania,
   g) spolupracuje s Úradom na ochranu osobných údajov,
   h) plní úlohy kontaktného miesta pre Úrad na ochranu osobných údajov a pre dotknuté osoby.

5. Model trojúrovňovej obrany

5.1. Prvou úrovňou obrany sú jednotlivé organizačné útvary zdravotnej poisťovne (vlastníci procesu a rizík), pričom tieto nesú primárnu každodennú zodpovednosť za dodržiavanie pravidiel na ochranu osobných údajov, vrátane tejto smernice, za výkon vnútornej kontroly v rámci svojho organizačného útvaru a za nastavenie a zlepšovanie procesov a kontrol.

5.2. Úsek právny a compliance poskytuje organizačným útvarom zdravotnej poisťovne poradenstvo. Zároveň úsek právny a compliance pri vykonávaní funkcie druhej obrannej línie dohliada, podporuje a monitoruje jednotlivé organizačné útvary pri dodržiavaní pravidiel na ochranu osobných údajov a pri napĺňaní ich úloh pri výkone vnútornej kontroly. Rovnako sekcia riadenia rizík pri vykonávaní funkcie druhej obrannej línie plní významnú úlohu pri dohliadaní, monitorovaní a podpore bezpečnosti spracúvania osobných údajov.

5.3. Treťou úrovňou obrany je odbor vnútornej kontroly a vnútorného auditu, ktorého úlohou je nezávislé a objektívne posudzovanie rámca vnútornej kontroly, teda posudzuje, či sú kontroly vhodne navrhnuté, implementované a účinné, a v prípade nedostatkov pripravuje odporúčania ako zlepšiť vnútornú kontrolu.

Článok VIII
Účel spracúvania osobných údajov

1. Zdravotná poisťovňa môže spracúvať osobné údaje len na konkrétne určené, výslovne uvedené a legitímne (zákonné) účely, čo znamená, že pred akýmkoľvek spracúvaním osobných údajov musí byť určený konkrétny účel takéhoto spracúvania. V tomto článku sú opísané povolené účely spracúvania osobných údajov v podmienkach zdravotnej poisťovne. V prípade, ak chce zamestnanec alebo organizačný útvar spracúvať osobné údaje na iné účely ako je opísané nižšie, je vždy povinný vopred vec konzultovať s riaditeľom úseku právneho a compliance ako zodpovednou osobou, ktorý posúdi zákonnosť takéhoto spracúvania. Jeho inštrukcia je záväzná.
2. Osobné údaje je možné spracúvať len na účely, pre ktoré boli získané. Osobné údaje môžu byť spracúvané na iné účely iba po posúdení nižšie uvedených skutočností:
   a) existuje priame prepojenie medzi účelmi, na ktoré sa osobné údaje získali, a účelmi zamýšľaného ďalšieho spracúvania,

b) aké sú možné následky takéhoto ďalšieho spracúvania pre dotknutú osobu,
c) povaha spracúvaných osobných údajov,
d) okolnosti, za ktorých boli osobné údaje získané,
e) existencia primeraných bezpečnostných záruk.

3. Zdravotná poisťovňa spracúva osobné údaje predovšetkým za účelom vykonávania verejného zdravotného poistenia a plnenia povinností vyplývajúcich jej zo zákona č. 580/2004 Z. z. o zdravotnom poistení a zákona č. 581/2004 Z. z. o zdravotných poisťovniach, dohľade nad zdravotnou starostlivosťou, pričom konkrétne ide najmä o nasledovné činnosti:
   a) prijímanie a potvrdzovanie prihlášok na verejné zdravotné poistenie,
   b) vydávanie preukazov na verejné zdravotné poistenie,
   c) vydávanie európskych preukazov na zdravotné poistenie,
   d) prijímanie poistného,
   e) uplatňuje nárok na úhradu zdravotnej starostlivosti,
   f) poskytovanie poradenskej činnosti pre poistencov a platiteľov,
   g) uzatváranie zmlúv s poskytovateľmi zdravotnej starostlivosti,
   h) vymáhanie pohľadávok na poistnom vrátane úrokov z omeškania,
   i) poskytovanie príspevkov na úhradu zdravotnej starostlivosti a
   j) vedenie zoznamu poistencov čakajúcich na poskytnutie zdravotnej starostlivosti.

   Zdravotná poisťovňa môže spracúvať osobné údaje aj za iným účelom a to za podmienok uvedených v tomto článku.
4. Zdravotná poisťovňa môže spracúvať osobné údaje dotknutých osôb za účelom ich informovania o produktoch a službách poskytovaných zdravotnou poisťovňou s cieľom vzniku poistného vzťahu v zdravotnej poisťovni (ďalej len „marketingový účel"), avšak iba za podmienky, ak dotknuté osoby s týmto vyslovene súhlasili.
   4.1. Marketingové informácie môžu byť dotknutej osobe doručené poštovou zásielkou, telefonickým oslovením, elektronickou poštou alebo priamym oslovením prostredníctvom spolupracujúcich sprostredkovateľov. *Informovanie dotknutej osoby sa nesmie šíriť automatickým telefonickým volacím systémom (systém, ktorý automaticky vytočí telefónne číslo z databázy a následné pridelí hovor prvému voľnému operátorovi), telefaxom, elektronickou poštou alebo správami sms bez predchádzajúceho súhlasu ich užívateľa, ktorý je príjemcom informácií.*
   4.2. Žiadosť o vyjadrenie súhlasu musí byť predložená tak, aby bola jasne odlíšiteľná od iných skutočností, v zrozumiteľnej a ľahko dostupnej forme a formulovaná jasne a jednoducho. Platný súhlas je súhlas daný v písomnej forme (vlastnoručne podpísaný osobou, ktorá tento súhlas dáva) alebo zodpovedajúcim zvukovým alebo obrazovo zvukovým záznamom alebo čestným vyhlásením toho, kto poskytol osobné údaje do informačného systému, prípadne iným hodnoverným spôsobom. Pre dokument obsahujúci osobné údaje v elektronickej forme je možné použiť elektronický podpis podľa zákona č. 215/2002 Z.z. o elektronickom podpise.
   4.3. Zdravotná poisťovňa prioritne zbiera súhlas na marketingové účely pre celú skupinu Union (Union poisťovňa, a.s., Union zdravotná poisťovňa, a.s. a ich dcérske spoločnosti), aby sa tak zvýšili možnosti krížového predaja produktov a služieb skupiny Union.
   4.4. Dôkaz o súhlase musí obsahovať informácie o tom, kto súhlas poskytol, že je súhlas poskytnutý zdravotnej poisťovni, účel poskytnutia, zoznam osobných údajov, dobu platnosti súhlasu a podmienky odvolania.
   4.5. Súhlas dotknutej osoby musí byť získaný slobodne a nesmie sa uzatváranie poistnej zmluvy či poskytovanie inej služby podmieňovať súhlasom so spracúvaním osobných údajov na marketingový účel.
   4.6. Pokiaľ súhlas na spracúvanie osobných údajov na marketingový účel vyjadrilo dieťa staršie ako 16 rokov, je takýto súhlas považovaný za platný a nie je potrebné, aby súhlas vyjadril alebo schválil nositeľ rodičovských práv dieťaťa.

4.7. Spôsob spracúvania (najmä získavania, uchovávania a používania) osobných údajov na marketingové účely určujú príslušní vedúci zamestnanci organizačných útvarov, ktorí spracúvajú osobné údaje na tento účel. Pred takýmto spracúvaním, najmä v prípadoch ak dochádza k zmene v spôsobe spracúvania, je vedúci zamestnanec príslušného organizačného útvaru povinný svoj postup konzultovať s úsekom právnym a compliance.

4.8. Dotknutá osoba môže kedykoľvek odvolať daný súhlas so spracúvaním osobných údajov na marketingový účel. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania vychádzajúceho zo súhlasu pred jeho odvolaním. Odvolanie súhlasu musí byť pre dotknutú osobu jednoduché.

4.9. Odvolanie súhlasu so spracúvaním osobných údajov na marketingové účely ruší všetky súhlasy dané v predchádzajúcom období, či už bol súhlas poskytnutý pri podpisovaní prihlášky na verejné zdravotné poistenie alebo počas propagačných kampaní. Odvolanie súhlasu so spracúvaním osobných údajov na marketingové účely môže byť realizované okrem písomnej formy, aj elektronickou poštou, telefonicky alebo sms správou.

4.10. Odvolanie súhlasu na marketingové účely vyznačí:

a) v produkčnom informačnom systéme zdravotnej poisťovne (Mediform) zamestnanec odboru zákazníckeho centra, pokiaľ sa o odvolaní súhlasu dozvie z vlastnej činnosti,

b) v produkčnom informačnom systéme zdravotnej poisťovne (Mediform) zamestnanec úseku služieb klientom, oddelenie správy registrov v iných prípadoch ako uvedených pod písmenom a),

c) v iných informačných systémoch (DWH) zamestnanec úseku marketingu, odbor business intelligence.

5. Zdravotná poisťovňa môže spracúvať osobné údaje dotknutých osôb (svojich poistencov) aj na účely priameho marketingu vo vzťahu k produktom, ktoré súvisia s verejným zdravotným poistením, pokiaľ zdravotná poisťovňa vopred dotknutú osobu o tomto účele informovala. Rovnako môže zdravotná poisťovňa v takomto prípade pre účely priameho marketingu podobných produktov poskytnúť osobné údaje spoločnostiam zo skupiny Union, a to z dôvodu, že takéto spracúvanie neprimerane nezasahuje do práv a očakávaní dotknutej osoby a je v konečnom dôsledku v jej prospech.

5.1. Ako príklad možno uviesť situáciu, keď Union zdravotná poisťovňa, a.s. poskytne osobné údaje svojich (nových) poistencov Union poisťovni, a.s. za účelom ponuky produktov individuálneho zdravotného poistenia alebo životného poistenia. Pri takomto spracúvaní však je potrebné prihliadať na zásadu primeranosti a očakávanie dotknutej osoby.

5.2. Príjemcovi elektronickej pošty sa musí poskytnúť možnosť jednoducho a bezplatne kedykoľvek odmietnuť také používanie jeho údajov pri každej doručenej správe. Zároveň je zakázané zasielanie elektronickej pošty, z ktorej nie je známa totožnosť a adresa odosielateľa.

5.3. Pokiaľ zdravotná poisťovňa spracúva osobné údaje na účely priameho marketingu, má dotknutá osoba vždy právo namietať voči takémuto spracúvaniu, pričom zdravotná poisťovňa je povinná bezodkladne skončiť s takýmto spracúvaním jej osobných údajov.

6. Zdravotná poisťovňa môže spracúvať osobné údaje aj na ďalšie účely, pričom najčastejšie sú tieto prípady:

6.1. Štatistické účely (napr. pre výpočet nákladovosti kmeňa). Pri takomto spracúvaní je možné spracúvať len nevyhnutné údaje na dosiahnutie účelu (zásada minimalizácie údajov), nepotrebné údaje musia byť anonymizované alebo agregované a to tak, aby nebolo možné priradiť údaje ku konkrétnej dotknutej osobe. Spracúvanie osobných údajov na štatistické účely nikdy nemôže viesť k prijatiu opatrení alebo rozhodnutiu voči konkrétnej dotknutej osobe.

6.2. Reporting z dôvodu plnenia zákonných oznamovacích povinností.

6.3. Vedenie účtovníctva.

6.4. Prevencia a odhaľovanie protispoločenskej činnosti (fraud assessment).
6.5. Predchádzanie a odhaľovanie legalizácie príjmov z trestnej činnosti a financovania terorizmu.
6.6. Vymáhanie občianskoprávnych nárokov zdravotnej poisťovne.
6.7. Obrana práv zdravotnej poisťovne (napr. pasívne súdne spory).
6.8. Vybavovanie sťažností.
6.9. Plnenie zákonných povinností zdravotnej poisťovne (napr. poskytovanie súčinnosti orgánom verejnej správy).
6.10. Vykonávania prieskumu trhu, pričom voči takémuto spracúvania má dotknutá osoba právo namietať, pričom zdravotná poisťovňa je povinná bezodkladne skončiť s takýmto spracúvaním jej osobných údajov.
6.11. Prieskum spokojnosti dotknutých osôb so službami zdravotnej poisťovne, pričom voči takémuto spracúvania má dotknutá osoba právo namietať, pričom zdravotná poisťovňa je povinná bezodkladne skončiť s takýmto spracúvaním jej osobných údajov.
6.12. Zabezpečenie bezpečnosti a funkčnosti webových služieb (cookies, IP adresy).
6.13. Vyhodnocovania správania sa návštevníkov webových stránok a personalizovania obsahu webových stránok. Takéto cookies je možné spracúvať len na základe súhlasu dotknutej osoby. Je možné ustáliť, že pokiaľ webová stránka obsahuje jasnú a odlíšiteľnú informáciu ohľadne spracúvania cookies, potom dotknutá osoba ďalším používaním webovej stránky vyjadrila súhlas s takýmto spracúvaním. Zároveň je dotknutá osoba informovaná o tom ako si vo svojom internetovom prehliadači môže nastaviť blokovanie cookies.

7. Zdravotná poisťovňa spracúva osobné údaje dotknutých osôb (zamestnancov) na pracovnoprávne účely. V takomto prípade je právnym základom spracúvania:
   a) pracovná zmluva (pre účely pracovnoprávne, zúčtovania miezd, daní a sociálneho poistenia a vzdelávania zamestnancov na základe Zákonníka práce, zákona o zdravotnom poistení, zákona o sociálnom poistení, zákona o starobnom dôchodkovom sporení, zákona o správe daní a poplatkov a zákona o dani z príjmov), alebo
   b) oprávnený záujem zdravotnej poisťovne ako zamestnávateľa (napr. monitoring dochádzky, kamerový systém, softvér na monitorovanie emailov alebo používania internetu, zaznamenávanie telefonických rozhovorov, sledovanie jázd, výkon kontroly, mystery shopping, prístup k adresárom/emailom odídeného zamestnanca), pričom takýmto spracúvaním osobných údajov nesmie dôjsť k neprimeranému zásahu do súkromia dotknutých osôb. Zároveň platí, že v niektorých prípadoch takéhoto spracúvania osobných údajov zamestnancov je potrebné predchádzajúce prerokovanie alebo súhlas odborovej organizácie, alebo
   c) súhlas zamestnanca, pričom v takomto prípade je vždy potrebná konzultácia s úsekom právnym a compliance (je vždy potrebné posudzovať okolnosti prípadu, keďže vzhľadom na silnejšie postavenie zamestnávateľa by súhlas mohol byť posúdený ako nie slobodne získaný). Osobné údaje záujemcov o zamestnanie v poisťovni je možné spracúvať na základe ich súhlasu.

Článok IX
Okruhy dotknutých osôb

1. Osobné údaje na účely vykonávania verejného zdravotného poistenia

1.1. Dotknutými osobami, ktorých osobné údaje sú spracúvané na účely vykonávania verejného zdravotného poistenia, sú
- poistenci
- zákonní zástupcovia poistencov
- platitelia poistného – fyzické osoby

- osoby oprávnené konať v mene poistenca (napr. zákonný zástupca poistenca, splnomocnenec).

1.2. Na účely vykonávania verejného zdravotného poistenia zdravotná poisťovňa spracúva osobné údaje v rozsahu stanovenom v zákone č. 581/2004 Z.z. o zdravotnom poistení a v zákone č. 580/2004 Z.z. o zdravotných poisťovniach.

1.3. Zdravotná poisťovňa spracúva osobné údaje uvedené na prihláške na vznik alebo zmenu verejného zdravotného poistenia v rozsahu: meno, priezvisko, rodné priezvisko, rodné číslo, číslo identifikačnej karty alebo číslo pasu, pohlavie, adresu trvalého pobytu, prechodný pobyt, ak ho dotknutá osoba má, kontaktnú adresu, kontaktné telefónne číslo, faxové číslo a adresa elektronickej pošty, ak ich dotknutá osoba má; u cudzinca sa uvádza aj adresa trvalého pobytu v cudzine, doba trvalého pobytu na území Slovenskej republiky, štátna príslušnosť a dátum narodenia, ak mu rodné číslo nebolo pridelené.

1.4. Osobné a doplňujúce údaje vedené na účte poistenca spracúva zdravotná poisťovňa v rozsahu stanovenom zákonom o zdravotných poisťovniach v rozsahu uvedenom v § 16 ods. 2 zákona č. 581/2004 Z. z. (konkrétne: a) meno, priezvisko, rodné číslo a trvalý pobyt poistenca, b) údaje o poskytnutých zdravotných výkonoch, liekoch, dietetických potravinách a zdravotníckych pomôckach, c) údaje o poskytnutých službách súvisiacich s poskytovaním zdravotnej starostlivosti, d) výšku úhrady za poskytnutú zdravotnú starostlivosť v členení podľa písmena b) a za poskytnuté služby súvisiace s poskytovaním zdravotnej starostlivosti, e) dátum poskytnutia zdravotnej starostlivosti v členení podľa písmena b) a služieb súvisiacich s poskytovaním zdravotnej starostlivosti, f) označenie poskytovateľov zdravotnej starostlivosti, ktorí poskytli poistencovi zdravotnú starostlivosť podľa písmena b), a označenie poskytovateľov služieb, g) údaj o zaradení poistenca do zoznamu poistencov čakajúcich na poskytnutie zdravotnej starostlivosti h) údaj o zaradení poistenca na dispenzarizáciu, i) označenie platiteľa poistného, j) údaje o predpísanom poistnom v členení na uhradené a neuhradené podľa platiteľa poistného za každý kalendárny mesiac, údaje o úrokoch z omeškania v členení na uhradené a neuhradené a údaje o výsledku ročného zúčtovania v členení na uhradené a neuhradené, k) údaje o výške úhrady za zdravotnú starostlivosť, ktorá sa poskytla poistencovi preukázateľne v dôsledku porušenia liečebného režimu alebo užitia návykovej látky, v členení uhradená a neuhradená poistencom, l) údaje o výške úhrady za prvé poskytnutie neodkladnej zdravotnej starostlivosti poistencovi, ktorý nemá podanú prihlášku na verejné zdravotné poistenie, m) údaje o výške úhrady za ďalšie poskytnutie neodkladnej zdravotnej starostlivosti poistencovi podľa písmena l) v členení uhradená a neuhradená poistencom, n) údaje o výške prepočítaného doplatku poistenca za najlacnejší náhradný liek podľa osobitného predpisu, o) údaj o zaradení poistenca do farmaceuticko-nákladovej skupiny.).

1.5. K osobným údajom nevyhnutným na dosiahnutie účelu spracúvania môže zdravotná poisťovňa priradiť ďalšie osobné údaje dotknutej osoby, ktoré bezprostredne súvisia s daným účelom spracúvania. Takéto osobné údaje musia byť označené ako nepovinné, napríklad na prihláške verejného zdravotného poistenia.

2. Osobné údaje na marketingové účely a účel priameho marketingu

2.1. Na marketingové účely spracúva zdravotná poisťovňa osobné údaje dotknutých osôb v rozsahu priezvisko, meno, titul, adresa trvalého pobytu, kontaktná adresa, telefónne číslo, a e-mailová adresa.

2.2. Úsek marketingu, odbor business inteligence si vedie evidenciu tých osobných údajov, ktoré poskytol iným organizačným útvarom, najmä úseku internej siete, oddeleniu kontaktných miest, úseku získavania klientov, úseku digitálneho marketingu a odboru zákazníckeho centra.

3. Osobné údaje ostatných osôb

3.1. Osobné údaje členov orgánov zdravotnej poisťovne, ktorí nie sú zamestnancami zdravotnej poisťovne spracúva zdravotná poisťovňa v rozsahu stanovenom osobitným zákonom, napr. Obchodným zákonníkom. Rozsah spracúvaných osobných údajov je meno a priezvisko, trvalý pobyt a rodné číslo alebo dátum narodenia zahraničnej fyzickej osoby, pokiaľ nemá pridelené rodné číslo a údaje o odbornej spôsobilosti a dôveryhodnosti.

4. Osobné údaje na pracovnoprávne účely

4.1. Dotknutými osobami, ktorých osobné údaje sú spracúvané na pracovnoprávne účely , sú
   a) zamestnanci v pracovnom pomere,
   b) zamestnanci vykonávajúci práce mimo pracovného pomeru,
   c) uchádzači o zamestnanie.

4.2. Spracúvanie osobných údajov zamestnancov z výpisu z registra trestov môže zdravotná poisťovňa spracúvať len v prípadoch ustanovených osobitným zákonom a v prípadoch ak sa vzhľadom na druh vykonávanej práce vyžaduje preukázanie bezúhonnosti. Pracovné pozície, pri ktorých sa vyžaduje preukázanie bezúhonnosti, sú určené v smernici s názvom Požiadavky na odbornú spôsobilosť a dôveryhodnosť členov predstavenstva spoločnosti a zamestnancov spoločnosti a v katalógu pracovných pozícií. Výpis z registra trestov ukladá úsek riadenia ľudských zdrojov do osobného spisu dotknutej osoby.

4.3. Žiadosti o zamestnanie a ďalšia korešpondencia obsahujúca osobné údaje uchádzača sa spracúva so súhlasom dotknutej osoby výlučne za účelom konkrétneho výberového konania, do času, kedy sa korektne ukončí dané výberové konanie. Písomnosti obsahujúce osobné údaje uchádzačov sa uchovávajú oddelene od osobných údajov zamestnancov. Po uplynutí uvedenej doby, je zamestnanec úseku riadenia ľudských zdrojov poverený evidenciou žiadostí povinný dokumentáciu obsahujúcu osobné údaje zlikvidovať.

Článok X
Minimalizácia údajov

1. Pred každou spracovateľskou operáciou je potrebné posúdiť rozsah spracúvaných osobných údajov potrebných na dosiahnutie účelu, pričom je možné spracúvať len taký rozsah osobných údajov, ktorý je nevyhnutný na dosiahnutie účelu spracúvania. Zdravotná poisťovňa má za týmto účelom vytvorený register osobných údajov (Data Register). Za vedenie registra osobných údajov je zodpovedný Data Governance Manager.
2. Rovnako je potrebné posúdiť aj rozsah osobných údajov prístupných pre jednotlivých zamestnancov a užívateľov zdravotnej poisťovne. Zamestnanci môžu spracúvať len nevyhnutný rozsah osobných údajov. V prílohe č. 1 tejto smernice sú uvedené situácie, v ktorých je možné zriadiť hromadný prístup k databáze osobných údajov dotknutých osôb a pravidlá pre jej aktualizáciu.
3. Osobitná pozornosť sa venuje spracúvaniu osobitnej kategórie osobných údajov, keďže tieto požívajú zvýšenú ochranu. Osobitnou kategóriou osobných údajov sú údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie, členstvo v odborovej organizácii, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia, údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie dotknutej osoby. Rovnako do tej kategórie patria aj údaje týkajúce sa uznania viny za trestné činy.
4. V podmienkach zdravotnej poisťovne je možné spracúvať osobitnú kategóriu osobných údajov v týchto prípadoch:
   a) údaje o zdravotnom stave,
   b) údaje týkajúce sa uznania viny za trestné činy – zdravotná poisťovňa ako zamestnávateľ vyžaduje od zamestnancov pracujúcich na vybraných pracovných pozíciách preukázanie ich bezúhonnosti (o.i. aj predložením výpisu z registra trestov),

c) na základe súhlasu dotknutej osoby – napr. člen odborovej organizácie v súvislosti s vykonávaním zrážok členského príspevku zo mzdy.

Článok XI
Práva dotknutých osôb

1. Dotknuté osoby majú v súvislosti so spracúvaním ich osobných údajov nasledovné práva:
   a) právo na informácie,
   b) právo na prístup k svojim osobným údajom,
   c) právo na opravu svojich osobných údajov,
   d) právo na vymazanie svojich osobných údajov,
   e) právo na obmedzenie spracúvania svojich osobných údajov,
   f) právo na prenosnosť svojich osobných údajov,
   g) právo namietať proti spracúvaniu svojich osobných údajov.
2. Podmienkou pre uplatnenie práva dotknutej osoby je jej identifikácia a overenie identifikácie, aby sa tak zabránilo zneužitiu práv zo strany tretej osoby alebo nezákonnému poskytnutiu osobných údajov. Zároveň dotknutá osoba musí mať viac ako 16 rokov a mať spôsobilosť na právne úkony, inak za ňu musí konať jej zákonný zástupca. Výnimkou z podmienky potreby identifikovania a overenia identifikácie je, ak dotknutá osoba namieta voči spracúvaniu osobných údajov na marketingové účely, účely priameho marketingu, na účely vykonávania prieskumu trhu a prieskumu spokojnosti, kedy zdravotná poisťovňa doručenej žiadosti (odvolanie súhlasu, námietka voči spracúvaniu) vždy vyhovie bez ohľadu na formu žiadosti.
3. V prípade, ak je žiadosť dotknutej osoby nejasná, je príslušný organizačný útvar povinný bezodkladne túto osobu kontaktovať za účelom upresnenia jej požiadavky. Právo na prístup a prenosnosť osobných údajov nie je realizované, pokiaľ bolo uplatnené telefonicky alebo prostredníctvom sociálnych médií, ak nebolo uplatnené aj písomne. O tejto skutočnosti informuje dotknutú osobu príslušný zamestnanec.
4. Akékoľvek informácie a oznámenia v súvislosti so spracúvaním osobných údajov sú zamestnanci zdravotnej poisťovne povinní poskytovať:
   - v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme,
   - písomne alebo inými prostriedkami, vrátane v prípade potreby elektronickými prostriedkami a spravidla v rovnakej forme, v akej bola podaná žiadosť. Ak o to požiadala dotknutá osoba, informácie sa môžu poskytnúť ústne,
   - bezodplatne, to neplatí ak sú žiadosti dotknutej osoby zjavne neopodstatnené alebo neprimerané, najmä pre ich opakujúcu sa povahu, kedy môže zdravotná poisťovňa odmietnuť konať na základe žiadosti alebo požadovať primeraný poplatok zohľadňujúci administratívne náklady.
5. Zdravotná poisťovňa poskytne dotknutej osobe informácie o opatreniach, ktoré prijala na základe žiadosti, bez zbytočného odkladu a v každom prípade do jedného mesiaca od doručenia žiadosti. Uvedenú lehotu môže vedúci organizačného útvaru vybavujúceho žiadosť v prípade potreby predĺžiť o ďalšie dva mesiace, pričom sa zohľadní komplexnosť žiadosti a počet žiadostí. Príslušný organizačný útvar informuje o každom takomto predĺžení dotknutú osobu do jedného mesiaca od doručenia žiadosti spolu s dôvodmi zmeškania lehoty.
6. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa podľa možnosti poskytnú elektronickými prostriedkami, pokiaľ dotknutá osoba nepožiadala o iný spôsob.

7. **Právo na informácie (transparentnosť)**
   7.1. Dodržiavanie zásady transparentnosti pri spracúvaní osobných údajov je najväčšou prioritou zdravotnej poisťovne. Na to, aby dotknutá osoba mohla realizovať svoje práva je totiž nevyhnutné, aby táto o svojich právach vedela a tiež aby vedela ako má svoje práva uplatniť.

7.2. Zdravotná poisťovňa je povinná pri získavaní osobných údajov od dotknutej osoby poskytnúť dotknutej osobe informácie v rozsahu podľa článku 13 a 14 nariadenia č. 2016/679 (najmä svoje identifikačné údaje, kontaktné údaje na zodpovednú osobu, účel spracúvania osobných údajov, právny základ spracúvania osobných údajov, príjemcov osobných údajov, informáciu o prípadnom zamýšľanom prenose osobných údajov mimo krajín Európskej únie, dobu uchovávania osobných údajov, poučenie o právach dotknutej osoby, poučenie o možnosti podať sťažnosť úradu na ochranu osobných údajov, informáciu o existencii automatizovaného rozhodovania, vrátane profilovania). Informácie sa poskytujú priamo v prihláške, ako odkaz na tieto informácie na webovom sídle zdravotnej poisťovne alebo ústne pri telefonickom oslovení klienta (telemarketing), pričom konkrétna forma sa zvolí po zohľadnení spôsobu získavania osobných údajov. V podmienkach zdravotnej poisťovne sú osobné údaje získavané štandardne na prihláškach na verejné zdravotné poistenie alebo na kontaktných formulároch.

7.3. Informácie sa dotknutej osobe poskytnú pred začatím spracúvania osobných údajov (pred ich získaním), a v prípade ak to nie je možné (napr. z dôvodu, že osobné údaje neboli získané od dotknutej osoby) bez zbytočného odkladu po ich získaní, nie neskôr ako pri prvom kontakte s dotknutou osobou alebo do 3 mesiacov od ich získania, podľa toho ktorý okamih nastane skôr.

7.4. Dotknutej osobe nie je potrebné poskytnúť informácie, pokiaľ nastane niektorá z týchto situácií:

a) dotknutej osobe už informácie boli poskytnuté (napr. ak sú zdravotnej poisťovni osobné údaje poskytnuté od zamestnávateľa v súvislosti s jeho plnením povinností ako platiteľa poistného),
b) ak by poskytnutie takýchto informácii bolo objektívne nemožné alebo by si vyžiadalo neprimerané úsilie,
c) ak sa získanie alebo poskytnutie osobných údajov stanovuje v zákone,
d) pri spracúvaní osobných údajov za účelom predchádzania protispoločenskej činnosti, jej vyšetrovanie a odhaľovanie, vrátane prevencie a ochrany pred verejnými bezpečnostnými rizikami,
e) vymáhanie občianskoprávnych nárokov.

Pri poskytovaní informácií platí všeobecné pravidlo, že dotknutej osobe je potrebné poskytnúť informácie vždy ak je to možné. Využitie situácie podľa písmena b) je možné len po predchádzajúcej konzultácii so zodpovednou osobou. Ako príklad je možné použiť situáciu, keď zdravotná poisťovňa spracúva IP adresy návštevníkov svojich webových stránok v záujme predchádzania DDoS útokov. Všeobecným záujmom zdravotnej poisťovne je bezpečnosť spracúvania údajov, nie je preto potrebné, aby zdravotná poisťovňa vyslovene informovala dotknuté osoby o každom jednom spôsobe spracúvania osobných údajov pre tieto účely.

7.5. Úsek právny a compliance vytvorí štandardné doložky o informáciách, ktoré sa majú poskytovať pri získavaní osobných údajov od dotknutej osoby. Akékoľvek zmeny v štandardných doložkách podliehajú súhlasu zo strany úseku právneho a compliance.

7.6. Príslušní vedúci zamestnanci organizačných útvarov, ktorí sú zodpovední za tvorbu formulárov prihlášky a iných kontaktných formulárov (najmä úsek služieb klientom, úsek revíznych a zdravotných činností, úsek marketingu, úsek digitálneho marketingu), sú povinní zabezpečiť, aby príslušné formuláre a tlačivá obsahovali informáciu v rozsahu podľa tohto odseku, pokiaľ sú formuláre a tlačivá určené pre fyzické osoby.

7.7. Úsek právny a compliance je zodpovedný za aktualizáciu všeobecnej informácie pre dotknuté osoby na webovom sídle zdravotnej poisťovne.

8. Právo dotknutej osoby na prístup k svojim osobných údajom

8.1. Na základe žiadosti dotknutej osoby je zdravotná poisťovňa povinná poskytnúť dotknutej osobe potvrdenie o tom, či sa spracúvajú jej osobné údaje. Žiadosť je možné vybaviť aj poskytnutím kópie dokumentácie.

8.2. Súčasne s poskytnutím osobných údajov sa dotknutej osobe oznamujú aj tieto informácie:

a) účely spracúvania,
b) kategórie dotknutých osobných údajov,
c) príjemcovia alebo kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, najmä príjemcovia v tretích krajinách alebo medzinárodné organizácie,
d) ak je to možné, predpokladaná doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie,
e) existencia práva požadovať od zdravotnej poisťovne opravu osobných údajov týkajúcich sa dotknutej osoby alebo ich vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti takémuto spracúvaniu,
f) právo podať sťažnosť Úradu na ochranu osobných údajov,
g) ak sa osobné údaje nezískali od dotknutej osoby, akékoľvek dostupné informácie, pokiaľ ide o ich zdroj,
h) existencia automatizovaného rozhodovania vrátane profilovania; v týchto prípadoch poskytuje zdravotná poisťovňa aspoň informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.

8.3. Dotknutá osoba má tiež právo na vyhotovenie fotokópií osobných údajov, ktoré sa o nej spracúvajú (neznamená to automaticky, že dotknutá osoba má právo na fotokópie celého spisu). V niektorých prípadoch možno toto právo dotknutej osoby obmedziť, napr. z dôvodu verejného záujmu, z dôvodu vyšetrovania protispoločenskej činnosti alebo z dôvodu ochrany práv tretích osôb.

8.4. Žiadosti dotknutých osôb na prístup k ich údajom vybavuje úsek právny a compliance, pričom ostatné organizačné útvary sú mu povinné poskytnúť súčinnosť.

9. Právo dotknutej osoby na opravu svojich osobných údajov

9.1. Zdravotná poisťovňa je povinná opraviť nesprávne údaje, ktoré sa týkajú dotknutej osoby, alebo doplniť neúplne údaje tejto osoby, a to po tom ako sa o tom dozvie. Ak k zmene údajov dochádza na základe žiadosti dotknutej osoby, potom je potrebné aby mala zdravotná poisťovňa preukázanú totožnosť dotknutej osoby.

9.2. Za opravu alebo doplnenie údajov o dotknutej osobe je zodpovedný úsek služieb klientom, ak ide o žiadosť týkajúcu sa registra poistencov, resp. iný organizačný útvar, do ktorého zodpovednosti spadá príslušná agenda.

10. Právo dotknutej osoby na vymazanie svojich osobných údajov (právo na zabudnutie)

10.1. Zdravotná poisťovňa je povinná vymazať osobné údaje dotknutej osoby, ak o to požiada a ak je splnený niektorý z týchto dôvodov:

a) osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali,
b) dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie vykonáva, a ak neexistuje iný právny základ pre spracúvanie,
c) dotknutá osoba namieta voči spracúvaniu (viď odsek 11 tohto článku) a neprevažujú žiadne oprávnené dôvody na spracúvanie,
d) osobné údaje sa spracúvali nezákonne,
e) ak to vyplýva zo zákona alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

10.2. Žiadosti dotknutých osôb posudzuje úsek právny a compliance, pričom zohľadňuje najmä to, či má zdravotná poisťovňa právny základ na spracúvanie osobných údajov (napr. zákon č. 580/2004 Z.z. alebo 581/2004 Z.z.). Žiadosti dotknutej osoby nebude

vyhovené najmä v prípadoch, ak má zdravotná poisťovňa povinnosť ďalej spracúvať osobné údaje na splnenie svojich zákonných povinností alebo ak osobné údaje musí spracúvať na preukazovanie, uplatňovanie alebo obhajovanie svojich právnych nárokov. Všetky organizačné útvary zdravotnej poisťovne sú povinné úseku právnemu a compliance poskytnúť požadovanú súčinnosť.

10.3. V prípade, ak je žiadosť dotknutej osoby neopodstatnená, je úsek právny a compliance povinný o tom informovať dotknutú osobu spolu s uvedením dôvodov.

10.4. V prípade, ak je žiadosť dotknutej osoby opodstatnená, úsek právny a compliance bezodkladne informuje úsek informatiky a prípadne iné dotknuté organizačné útvary o potrebe vymazať osobné údaje dotknutej osoby z informačných systémov zdravotnej poisťovne. Úsek informatiky bezodkladne vymaže alebo anonymizuje osobné údaje zo všetkých informačných systémov zdravotnej poisťovne, pričom pri tom berie na zreteľ existujúce technologické možnosti. Úsek právny a compliance o prijatých opatreniach informuje dotknutú osobu a rovnako tak aj všetkých známych príjemcov osobných údajov, aby títo vykonali rovnaké opatrenia vo svojich informačných systémoch.

11. Právo dotknutej osoby na obmedzenie spracúvania svojich osobných údajov

11.1. Zdravotná poisťovňa je povinná obmedziť spracúvanie osobných údajov dotknutej osoby, ak o to požiada a pokiaľ ide o jeden z týchto prípadov

a) dotknutá osoba napadne správnosť osobných údajov, a to počas obdobia kedy zdravotná poisťovňa overuje správnosť osobných údajov,
b) spracúvanie je protizákonné a dotknutá osoba namieta proti vymazaniu osobných údajov a žiada namiesto toho obmedzenie ich použitia,
c) zdravotná poisťovňa už nepotrebuje osobné údaje na účely spracúvania, ale potrebuje ich dotknutá osoba na preukázanie, uplatňovanie alebo obhajovanie právnych nárokov,
d) dotknutá osoba namietala voči spracúvaniu (viď odsek 11 tohto článku), a to až do overenia, či oprávnené dôvody na strane zdravotnej poisťovne prevažujú nad oprávnenými dôvodmi dotknutej osoby.

11.2. Žiadosti dotknutých osôb posudzuje úsek právny a compliance. Úsek právny a compliance informuje dotknutú osobu o obmedzení spracúvania osobných údajov a o zrušení tohto obmedzenia.

11.3. Počas doby obmedzenia spracúvania osobných údajov dotknutej osoby nie je možné tieto osobné údaje spracúvať, s výnimkou ich uchovávania, spracúvania so súhlasom dotknutej osoby alebo na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov, alebo na ochranu práv inej fyzickej osoby alebo právnickej osoby, alebo z dôvodov dôležitého verejného záujmu.

12. Právo na prenosnosť osobných údajov

12.1. Na základe žiadosti dotknutej osoby poskytne zdravotná poisťovňa

a) dotknutej osobe a/alebo
b) ďalšiemu prevádzkovateľovi (najmä inej zdravotnej poisťovni)

osobné údaje, ktoré sa jej týkajú, a ktoré poskytla zdravotnej poisťovni a to v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte (napr. excel)

12.2. Za vybavovanie žiadostí dotknutých osôb je zodpovedný úsek služieb klientom, ak ide o žiadosť týkajúcu sa registra poistencov, resp. iný organizačný útvar, do ktorého zodpovednosti spadá príslušná agenda.

13. Právo namietať

13.1. Dotknutá osoba má právo namietať voči spracúvaniu svojich osobných údajov v týchto situáciách:

a) ak zdravotná poisťovňa spracúva osobné údaje za účelom splnenia úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci, alebo za účelom jej oprávnených záujmov (napr. prieskum spokojnosti)
b) ak zdravotná poisťovňa spracúva osobné údaje na účely priameho marketingu.

13.2. V prípade, ak dotknutá osoba vznesie námietku podľa bodu 13.1. písm. a), zdravotná poisťovňa nesmie ďalej spracúvať jej osobné údaje, pokiaľ nepreukáže nevyhnutné oprávnené dôvody na spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami dotknutej osoby, alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

13.3. V prípade, ak dotknutá osoba vznesie námietku podľa bodu 13.1. písm. b), zdravotná poisťovňa nesmie jej osobné údaje na tento účel ďalej spracovávať.

13.4. Zodpovednosť za vybavenie námietky dotknutej osoby má organizačný útvar, do ktorého zodpovednosti patrí namietaná vec, pričom v prípade potreby spôsob vybavenia námietky konzultuje s úsekom právnym a compliance.

14. Automatizované individuálne rozhodovanie vrátane profilovania

14.1. Profilovanie je akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom.

14.2. Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú. Uvedené pravidlo sa neuplatňuje v prípade ak na automatizované spracúvanie vrátane profilovania dotknutá osoba dala výslovný súhlas alebo sa automatizovane spracúvajú údaje pre odhaľovanie protispoločenského správania, napr. využitím analytických nástrojov. Pokiaľ po takomto automatizovanom detekovaní podozrivého prípadu tento posúdi zodpovedný zamestnanec už nejde o automatizované rozhodovanie, keďže rozhodnutie prijíma človek.
Dynamické zobrazovanie webovej stránky zdravotnej poisťovne na základe IP adresy v úmysle neukázať dotknutej osobe určité produkty alebo služby nie je dovolené.

14.3. Profilovanie musí byť založené na objektívnych kritériách a nesmie viesť k diskriminácii dotknutej osoby alebo skupiny dotknutých osôb.

14.4. V prípade zavedenia procesu založeného na automatizovanom individuálnom rozhodovaní je povinnosťou organizačného útvaru zodpovedného za tento proces (spravidla úsek digitálneho marketingu) nastaviť pravidlá tak, aby:
- dotknutá osoba dostala informáciu o existencii takéhoto rozhodovania,
- ak sú na takéto profilovanie použité údaje, ktoré sa nezískali od dotknutej osoby, aby dotknutá osoba dostala informáciu o zdroji týchto údajov,
- dotknutá osoba mala vždy právo na ľudský zásah zo strany zdravotnej poisťovne, právo vyjadriť svoje stanovisko a právo napadnúť takéto automatizované rozhodnutie (napr. možnosť kontaktovať zákaznícke centrum zdravotnej poisťovne).

Článok XII
Minimalizácia uchovávania osobných údajov

1. Zdravotná poisťovňa je oprávnená uchovávať osobné údaje iba dovtedy, pokým sú potrebné na účel, na ktorý sa spracúvajú. Po tom, ako pominie účel spracúvania osobných údajov, sa tieto osobné údaje zlikvidujú alebo anonymizujú, pričom

1.1. Anonymizácia osobných údajov je taká zmena osobných údajov, po ktorej už tieto osobné údaje nemožno prideliť určitej osobe alebo tak možno urobiť len s vynaložením nepomerne

veľkého úsilia z hľadiska času, nákladov a práce. Pre vylúčenie pochybností platí, že údaje po ich anonymizácii už viac nie sú osobné údaje, a teda sa na ne nevzťahujú pravidlá pre ochranu osobných údajov.

1.2. Likvidácia osobných údajov je ich zrušenie rozložením, vymazaním alebo fyzickým zničením hmotných nosičov (dokumentácie) tak, aby sa z nich osobné údaje nedali reprodukovať alebo odhaliť.

2. Úsek právny a compliance v spolupráci s príslušnými organizačnými útvarmi stanoví pravidlá pre likvidáciu a anonymizáciu osobných údajov v systémoch zdravotnejpoisťovne.
3. Pravidlá pre likvidáciu osobných údajov zaznamenaných na dokumente (v listinnej a aj elektronickej podobe) sú upravené v registratúrnom poriadku zdravotnej poisťovne.

Článok XIII
Bezpečnosti spracúvania osobných údajov

1. Všeobecné povinnosti

1.1. Za bezpečnosť osobných údajov zodpovedá zdravotná poisťovňa tým, že chráni spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania. Na tento účel je zdravotná poisťovňa povinná prijať primerané technické, organizačné a personálne opatrenia, pričom berie do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov, ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému zodpovedajúce úrovni zabezpečenia v podmienkach zdravotnej poisťovne.

1.2. Za primerané technické a organizačné opatrenia na zaistenie bezpečnosti osobných údajov a ich spracúvania sa považujú najmä:

a) pseudonymizácia (pseudonymizácia je spracúvanie osobných údajov spôsobom kedy osobné údaje nie je možné priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií za podmienky, že takéto dodatočné informácie sa uchovávajú oddelene) a šifrovanie osobných údajov,
b) schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb (napr. CIA analýza),
c) schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu (BCM proces),
d) proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania (BIA analýza).

Pre stanovenie konkrétnych bezpečnostných opatrení sa prihliada na úroveň technického pokroku (state of the art), náklady na ich implementáciu, povahu a rozsah spracúvaných osobných údajov, riziká spracúvania osobných údajov pre dotknuté osoby a účel spracúvania osobných údajov. Zároveň je potrebné prijať zvýšené bezpečnostné opatrenia v prípadoch, keď zdravotná poisťovňa spracúva citlivé údaje ako napr. údaje o finančnej situácii dotknutej osoby, údaje, ktoré môžu stigmatizovať dotknutú osobu (napr. pracovné alebo vzťahové problémy), údaje o zraniteľnej skupine osôb (napr. o deťoch), užívateľské meno, heslo alebo iné prihlasovacie údaje a údaje, ktoré môžu byť zneužité na identifikáciu (napr. kópia občianskeho preukazu).

1.3. Pravidlá na zaistenie bezpečnosti osobných údajov sú opísané v tejto smernici, a tiež v smerniciach vydávaných sekciou riadenia rizík a poistnej matematiky, najmä Politika informačnej bezpečnosti, Klasifikácia informácií a Manažment plánov náhradnej prevádzky (BCM).

2. Záznamy o spracovateľských operáciách

2.1. Sekcia riadenia rizík je povinná viesť v písomnej aj elektronickej podobe záznamy o spracovateľských činnostiach.

2.2. Záznamy o spracovateľských činnostiach musia obsahovať tieto informácie:

a) obchodné meno alebo názov a kontaktné údaje zdravotnej poisťovne, prípadného spoločného prevádzkovateľa, a zodpovednej osoby,
b) účely spracúvania,
c) opis kategórií dotknutých osôb a kategórií osobných údajov,
d) kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, vrátane príjemcov v tretích krajinách (mimo Európskej únie),
e) prenosy osobných údajov do tretej krajiny (mimo Európskej únie), ak je to relevantné,
f) podľa možností predpokladané lehoty na vymazanie rôznych kategórií osobných údajov,
g) podľa možností všeobecný opis technických a organizačných bezpečnostných opatrení,
h) v príslušných prípadoch informácie o použití profilovania,
i) uvedenie právneho základu pre spracovateľské operácie vrátane prenosov, pre ktoré sú osobné údaje určené.

2.3. Záznamy o spracovateľských operáciách musia byť priebežne aktualizované. V prípade, ak zdravotná poisťovňa má záujem vykonávať novú spracovateľskú operáciu, prípadne ak dôjde k zmene v informáciách podľa bodu 2.2. tohto odseku, je príslušný organizačný útvar povinný pred zmenou informovať sekciu riadenia rizík. Sekcia riadenia rizík následne zabezpečí aktualizáciu záznamov o spracovateľských operáciách, pričom o zmene informuje riaditeľa úseku právneho a compliance.

2.4. Záznamy o spracovateľských operáciách sú uložené na H:\EvidencneListyIS\UP.

3. Posúdenie vplyvu na ochranu údajov

3.1. Zdravotná poisťovňa je povinná vykonať vlastné posúdenie spracovateľských operácií na ochranu osobných údajov (Privacy Impact Assessment – PIA), ak spracúvanie osobných údajov môže viesť k vysokému riziku pre práva a slobody fyzických osôb, pričom toto posúdenie sa musí vykonať:

a) pred spracúvaním osobných údajov, pri zavádzaní nového typu spracovateľských operácií (v záujme eliminovania výšky dodatočných nákladov a rýchlosti dodania riešenia sa tak má stať v čo najskoršej fáze zmeny),
b) pred zásadnou zmenou v spracovateľských operáciách (v záujme eliminovania výšky dodatočných nákladov a rýchlosti dodania riešenia sa tak má stať v čo najskoršej fáze zmeny),
c) minimálne raz za tri roky pri existujúcich spracovateľských operáciách,
d) bezodkladne po tom ako sa zmenilo riziko ochrany osobných údajov.

3.2. Posúdenie vplyvu na ochranu osobných údajov je riziková analýza z pohľadu ochrany osobných údajov a obsahuje údaje v rozsahu podľa článku 35 nariadenia č. 2016/679. Sekcia riadenia rizík v spolupráci s úsekom právnym a compliance je zodpovedná za vytvorenie štandardných formulárov pre posúdenie vplyvu na ochranu osobných údajov.

3.3. Za vykonávanie posúdenia vplyvu na ochranu osobných údajov je zodpovedný vedúci organizačného útvaru, do ktorého zodpovednosti spadá, tá ktorá, spracovateľská operácia. Posúdenie vplyvu na ochranu osobných údajov je potrebné vykonávať minimálne na tieto spracovateľské operácie:

a) Posúdenie vplyvu na ochranu osobných údajov pri spracúvaní osobných údajov na účely vykonávania verejného zdravotného poistenia (Mediform), pričom za jeho vykonanie sú zodpovední
   - Riaditeľ úseku služieb klientom, v spolupráci s riaditeľom úseku revíznych a zdravotných činností ako vlastníci osobných údajov,
   - Riaditeľ úseku digitálneho marketingu,

- Riaditeľ úseku informatiky v rozsahu informačnej bezpečnosti,
- Riaditeľ odboru vnútorných služieb v rozsahu fyzickej bezpečnosti,
- Data Governance Manager,

b) Posúdenie vplyvu na ochranu osobných údajov pri spracúvaní osobných údajov na analytické, štatistické a marketingové účely (Business Intelligence), pričom za jeho vykonanie sú zodpovední
- Riaditeľ úseku služieb klientom a riaditeľ úseku revíznych a zdravotných činností ako vlastníci osobných údajov,
- Riaditeľ úseku marketingu,
- Riaditeľ úseku informatiky v rozsahu informačnej bezpečnosti,
- Data Governance Manager,

c) Posúdenie vplyvu na ochranu osobných údajov pri spracúvaní osobných údajov zamestnancov v súvislosti so zamestnaním (HUMAN), pričom za jeho vykonanie sú zodpovední
- Riaditeľ úseku riadenia ľudských zdrojov ako vlastník osobných údajov,
- Riaditeľ úseku informatiky v rozsahu informačnej bezpečnosti,
- Riaditeľ odboru vnútorných služieb v rozsahu fyzickej bezpečnosti,
- Data Governance Manager,

d) Posúdenie vplyvu na ochranu osobných údajov pri spracúvaní osobných údajov zamestnancov v súvislosti so zamestnaním (ICM2), pričom za jeho vykonanie sú zodpovední,
- Riaditeľ úseku riadenia ľudských zdrojov ako vlastník osobných údajov, v spolupráci s riaditeľom úseku získavania klientov,
- Riaditeľ úseku informatiky v rozsahu informačnej bezpečnosti,
- Data Governance Manager.

Pri vykonávaní posúdenia vplyvu na ochranu osobných údajov sa zodpovedné osoby radia s riaditeľom sekcie riadenia rizík a riaditeľom úseku právneho a compliance, prípadne inými relevantnými organizačnými útvarmi.

3.4. Ak sa zavádza nový systém alebo zdravotná poisťovňa bude vykonávať nové typy spracovateľských operácií, je vlastník údajov, ktoré sú zmenou dotknuté, zodpovedný za určenie, či je potrebné vykonať vlastné posúdenie spracovateľských operácií na ochranu osobných údajov, pričom sa pri tom radí s riaditeľom sekcie riadenia rizík a riaditeľom úseku právneho a compliance.

3.5. Ak z posúdenia vplyvu na ochranu údajov vyplýva, že toto spracúvanie by viedlo k vysokému riziku v prípade, ak by zdravotná poisťovňa neprijala opatrenia na zmiernenie tohto rizika, je zodpovedná osoba podľa predchádzajúceho bodu povinná zistenia konzultovať s riaditeľom sekcie riadenia rizík a riaditeľom úseku právneho a compliance. Ak je to potrebné, riaditeľ úseku právneho a compliance konzultuje zistenia s Úradom na ochranu osobných údajov. Pred ukončením týchto konzultácií nie je možné začať s posudzovanými spracovateľskými operáciami a ak už začaté boli, je potrebné ich bezodkladne ukončiť.

3.6. Dokumentácia k posúdeniu vplyvu na ochranu osobných údajov sa archivuje na sekcii riadenia rizík.

4. Sprostredkovateľ

4.1. Zdravotná poisťovňa nesmie poskytovať osobné údaje tretej strane, s výnimkou ak jej takéto oprávnenie alebo povinnosť vyplýva zo zákona alebo zo zmluvy.

4.2. Ak sa má spracúvanie uskutočniť v mene zdravotnej poisťovne, potom sú členovia predstavenstva a vedúci zamestnanci v rozsahu vecnej pôsobnosti nimi riadeného organizačného útvaru zodpovední za to, že poveria výkonom činnosti len takých sprostredkovateľov, ktorí poskytujú dostatočné záruky na to, že sa prijmú primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo požiadavky tejto smernice

a právnych predpisov pre oblasť ochrany osobných údajov, a aby sa zabezpečila ochrana práv dotknutej osoby. Pri tom najmä posudzujú:

a) vecné, personálne a organizačné predpoklady sprostredkovateľa na výkon činnosti, pričom príslušný organizačný útvar zohľadní povahu činnosti, ktorá sa má zveriť,
b) spôsob, akým bude zabezpečená ochrana osobných údajov v databázových systémoch sprostredkovateľa – príslušný organizačný útvar je povinný preveriť úroveň zabezpečenia u sprostredkovateľa.

Pokiaľ sprostredkovateľ nesplní tieto predpoklady, potom s ním nie je možné uzatvoriť zmluvu ani ho inak poveriť spracúvaním osobných údajov v mene zdravotnej poisťovne a to z dôvodu, že sprostredkovateľ spracúva osobné údaje v mene a na zodpovednosť poisťovne.

4.3. Zmluva so sprostredkovateľom musí byť v písomnej forme. Okrem štandardných zmluvných ustanovení musí takáto zmluva obsahovať:

a) Záväzok sprostredkovateľa spracúvať osobné údaje len na základe zdokumentovaných pokynov zdravotnej poisťovne,
b) Záväzok všetkých osôb oprávnených spracúvať osobné údaje zachovávať dôvernosť informácií,
c) Záväzok sprostredkovateľa vykonávať technické a organizačné opatrenia s cieľom zaistiť primeranú úroveň bezpečnosti pri spracúvaní osobných údajov,
d) Záväzok sprostredkovateľa po zohľadnení povahy spracúvania v čo najväčšej miere pomáhať zdravotnej poisťovni vhodnými technickými a organizačnými opatreniami pri plnení jej povinnosti reagovať na žiadosti o výkon práv dotknutej osoby,
e) Záväzok sprostredkovateľa pomáhať zdravotnej poisťovni pri zabezpečovaní plnenia povinností vyplývajúcich z právnych predpisov pre oblasť ochrany osobných údajov, a to s prihliadnutím na povahu spracúvania a informácie dostupné sprostredkovateľovi,
f) Záväzok sprostredkovateľa vymazať alebo vrátiť zdravotnej poisťovni všetky osobné údaje, a to po ukončení poskytovania služieb týkajúcich sa spracúvania a na základe rozhodnutia zdravotnej poisťovne, ak osobitný predpis nepožaduje uchovávanie týchto osobných údajov,
g) Záväzok sprostredkovateľa poskytovať zdravotnej poisťovni všetky informácie potrebné na preukázanie splnenia povinností stanovených v právnych predpisoch pre oblasť ochrany osobných údajov,
h) Záväzok sprostredkovateľa umožniť audity a kontroly zo strany zdravotnej poisťovne, jej externých audítorov a Úradu na ochranu osobných údajov, ako aj záväzok s týmito spolupracovať,
i) Záväzok sprostredkovateľa bezodkladne informovať zdravotnú poisťovňu, ak má za to, že sa jej pokynom porušujú právne predpisy pre oblasť ochrany osobných údajov,
j) Záväzok sprostredkovateľa podať zdravotnej poisťovni oznámenie o porušení ochrany osobných údajov a to bez zbytočného odkladu (spravidla do 24 hodín) po tom, čo sa o porušení ochrany osobných údajov dozvedel,
k) Záväzok sprostredkovateľa, že nepoverí výkonom činnosti ďalšieho sprostredkovateľa bez predchádzajúceho osobitného alebo všeobecného písomného súhlasu zdravotnej poisťovne,
l) V prípade, ak zdravotná poisťovňa dala sprostredkovateľovi všeobecný písomný súhlas s použitím ďalšieho sprostredkovateľa, záväzok sprostredkovateľa informovať zdravotnú poisťovňu o akýchkoľvek zamýšľaných zmenách v súvislosti s pridaním alebo nahradením ďalších sprostredkovateľov, čím sa zdravotnej poisťovni dá možnosť namietať voči takýmto zmenám,
m) V prípade, ak zdravotná poisťovňa dala sprostredkovateľovi súhlas s použitím ďalšieho sprostredkovateľa, je sprostredkovateľ povinný v zmluve s takýmto ďalším sprostredkovateľom mu uložiť rovnaké povinnosti týkajúce sa ochrany osobných údajov, ako sa stanovujú v zmluve medzi zdravotnou poisťovňou a sprostredkovateľom.

4.4. Úsek právny a compliance vytvorí štandardné zmluvné doložky pre zmluvy so sprostredkovateľom. Akékoľvek zmeny v štandardných zmluvných doložkách podliehajú súhlasu zo strany úseku právneho a compliance.

5. **Poskytovanie osobných údajov inému prevádzkovateľovi**

5.1. Zdravotná poisťovňa môže poskytovať osobné údaje inému prevádzkovateľovi, napr. na účely plnenia jej zákonných povinností (napr. orgánom dohľadu, daňovému úradu, sociálnej poisťovni, zdravotným poisťovniam) alebo zmluvných povinností (napr. poskytovateľ zdravotnej starostlivosti). V takomto prípade je za ochranu poskytnutých osobných údajov zodpovedný tento iný prevádzkovateľ. Zároveň ale je potrebné prijať primerané bezpečnostné opatrenia pre samotný prenos osobných údajov.

5.2. Rovnako iný prevádzkovateľ môže poskytovať osobné údaje zdravotnej poisťovni, napr. v prípade, ak zdravotná poisťovňa kúpi/získa databázu osobných údajov od inej osoby. V takomto prípade je potrebné zistiť:

- za akým účelom predávajúci získal osobné údaje za účelom preverenia, či účel na ktorý chce zdravotná poisťovňa osobné údaje spracúvať je primeraný účelu, za ktorým boli osobné údaje získané, a v súlade s očakávaniami dotknutej osoby,
- akým spôsobom a na akom právnom základe boli osobné údaje získané,
- akým spôsobom môže dotknutá osoba uplatňovať svoje práva a akým spôsobom bude zdravotná poisťovňa informovaná o uplatnení práva (napr. o odvolaní súhlasu na spracovanie osobných údajov),
- či bola dotknutá osoba informovaná o tom, že zdravotná poisťovňa je (môže) byť príjemcom jej osobných údajov, a ak sa tak nestalo potom zdravotná poisťovňa alebo prevádzkovateľ informuje dotknutú osobu o takomto poskytnutí jej údajov.

6. Spoloční prevádzkovatelia

6.1. Zdravotná poisťovňa môže spoločne s iným prevádzkovateľom určiť účely a prostriedky spracúvania osobných údajov. Podmienkou pre takúto spoluprácu je uzavretie písomnej zmluvy medzi spoločnými prevádzkovateľmi, v ktorej budú jasne vymedzené zodpovednosti za dodržiavanie pravidiel pre oblasť ochrany osobných údajov, najmä pokiaľ ide o vykonávanie práv dotknutej osoby a o poskytovanie informácií dotknutej osobe. Štandardne sa v takejto dohode tiež určí jedno kontaktné miesto pre dotknuté osoby, čo však neznamená, že dotknutá osoba stráca právo kontaktovať ktoréhokoľvek prevádzkovateľa.

6.2. Dotknutá osoba musí byť vždy informovaná o tom, že zdravotná poisťovňa spracúva osobné údaje spolu s iným prevádzkovateľom.

7. Zdravotná poisťovňa v postavení sprostredkovateľa

7.1. Vo výnimočných situáciách môže byť zdravotná poisťovňa v postavení sprostredkovateľa, a to v prípade, ak účel a prostriedky spracúvania osobných údajov určí iný prevádzkovateľ (napr. pri sprostredkovaní individuálneho zdravotného poistenia). Ak nastane takáto situácia, potom je zodpovednosťou tohto iného prevádzkovateľa určiť spôsob akým budú osobné údaje spracúvané. Pravidlá uvedené v tejto smernici sa použijú primerane.

7.2. Ak je zdravotná poisťovňa v postavení sprostredkovateľa, potom môže spracúvať osobné údaje len v rozsahu a na účel určený iným prevádzkovateľom. Zároveň informačné povinnosti voči dotknutým osobám (podľa článku XI tejto smernice) nemá zdravotná poisťovňa, ale tento iný prevádzkovateľ.

Článok XIV
Prenos osobných údajov do tretích krajín

1. Prenos osobných údajov do tretej krajiny (mimo Európskej únie) alebo medzinárodnej organizácii je možné uskutočniť ak Európska komisia rozhodla, že tretia krajina alebo medzinárodná organizácia zaručujú primeranú úroveň ochrany osobných údajov. Na takýto prenos nie je nutné žiadať osobitné povolenie.
   Zoznam tretích krajín, území a určených sektorov v danej krajine a medzinárodných organizácií, ktoré zaručujú primeranú úroveň ochrany osobných údajov, a v ktorých už prestala byť primeraná úroveň ochrany je uverejnený v Úradnom vestníku Európskej únie a na webovom sídle Európskej komisie (http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm). Ku dňu vydania tejto smernice medzi takéto tretie krajiny patria Andora, Argentína, Kanada, Faerské ostrovy, Izrael, Urugvaj, Spojené štáty americké (pri spoločnostiach, ktoré pristúpili k tzv. Privacy Shield - https://www.privacyshield.gov/list) a Švajčiarska.
2. Ak neexistuje rozhodnutie Európskej komisie podľa ods. 1, je možné uskutočniť prenos osobných údajov do tretej krajiny vtedy, ak prevádzkovateľ alebo sprostredkovateľ poskytol primerané záruky a za podmienky, že dotknuté osoby majú k dispozícii vymožiteľné práva a účinné právne prostriedky nápravy v rozsahu ako je uvedené v článku 46 nariadenia č. 2016/679.
3. Ak nie je splnená podmienka podľa odseku 1 alebo 2, je možné uskutočniť prenos osobných údajov do tretej krajiny len ak je to objektívne nevyhnutné a zároveň je splnená jedna z týchto podmienok:
   a) dotknutá osoba dala na takýto prenos vyslovený súhlas (napr. pri používaní WhatsApp, pričom zároveň WhatsApp nepristúpil na dodržiavanie Privacy Shield pravidiel, ak dotknutá osoba si pridá WhatsApp telefónne číslo poisťovne, potom vyjadruje súhlas s prenosom svojich osobných údajov do Spojených štátov amerických bez primeraných záruk ochrany súkromia),
   b) prenos je nevyhnutný pre plnenie zmluvy alebo na vykonanie predzmluvných opatrení prijatých na žiadosť dotknutej osoby,
   c) prenos je nevyhnutný pre uzavretie alebo plnenie zmluvy, ktorá bola uzatvorená v záujme dotknutej osoby,
   d) prenos je nevyhnutný na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov,
4. e) prenos je nevyhnutný na ochranu životne dôležitých záujmov dotknutej osoby.
5. Akýkoľvek prenos osobných údajov do tretích krajín (mimo Európskej únie) alebo medzinárodnej organizácii (s výnimkou prenosu ako je popísaný v odseku 3), a to či už priamo poisťovňou alebo prostredníctvom jej sprostredkovateľa je možný len po predchádzajúcej konzultácii s úsekom právny a compliance a so sekciou riadenia rizík.

Článok XV
Osobitné ustanovenia pri spracúvaní Big Data a pri používaní sociálnych sietí

1. Big Data

1.1. Pravidlá pre spracúvanie osobných údajov uvedené v tejto smernici je potrebné dodržiavať aj pri spracúvaní tzv. Big Data. O takéto spracúvanie ide vtedy, keď sa spracúvajú rôzne typy údajov, získané z interných aj externých zdrojov pre analytické účely. Takéto spracúvanie spravidla vedie k prijatiu opatrení alebo rozhodnutí (napr. cielenie reklamy, výpočet výšky poistného, odmietnutie služby) voči určitej porovnateľnej skupine dotknutých osôb, čo môže mať za následok dopad na jednotlivca a jeho základné práva a slobody. Pri takomto spracúvaní je vždy potrebné zohľadniť účel, na ktorý boli osobné údaje získané, a tiež poznať zdroj, z ktorých boli údaje získané,

2. Sociálne siete

2.1. Využívanie sociálnych sietí (napr. Facebook, LinkedIn) na komunikáciu s dotknutými osobami nesie v sebe riziká, najmä z dôvodu, že tieto nie vždy zaručujú primeranú úroveň ochrany osobných údajov a zároveň nie je možné s ich prevádzkovateľmi uzatvoriť zmluvu alebo inak ovplyvniť podmienky ich používania. Sociálne média zároveň používajú tzv. zásuvný modul (plug-in), ako napr. „share", „like" alebo „pin" tlačítka, ktoré pracujú ako cookies.

2.2. Zdravotná poisťovňa, pokiaľ má vytvorený profil na sociálnych sieťach, je povinná minimálne:

- poskytnúť informáciu dotknutej osobe o účele spolupráce so sociálnymi sieťami (dôvode vytvorenia konta),
- poskytnúť dotknutej osobe odkaz na informácie o spracúvaní osobných údajov zo strany príslušnej sociálnej siete,
- zabezpečiť, aby zásuvný modul (plug-in) bol aktívny až po tom, ako dotknutá osoba vyjadrí súhlas s používaním cookies.
- viesť si dokumentáciu a záznamy o jednotlivých obchodných podmienkach tej-ktorej sociálnej siete.

Za dodržiavanie pravidiel uvedených v tomto odseku ohľadom používania sociálnych sietí je zodpovedný úsek digitálneho marketingu.

2.3. Pri komunikácii so zákazníkom prostredníctvom sociálnych sietí (napr. Facebook messenger, WhatsApp, Twitter, Direct Message) je potrebné dodržať nasledovné pravidlá:

- spracúvať len naozaj nevyhnutné údaje a aktívne nekomunikovať zo strany zdravotnej poisťovne takýmto spôsobom citlivé údaje ako napr. údaje o finančnej situácii dotknutej osoby, údaje, ktoré môžu stigmatizovať dotknutú osobu (napr. pracovné alebo vzťahové problémy), údaje o zraniteľnej skupine osôb (napr. o deťoch), užívateľské meno, heslo alebo iné prihlasovacie údaje a údaje, ktoré môžu byť zneužité na identifikáciu (napr. kópia občianskeho preukazu),
- zdravotná poisťovňa nikdy nezačne sama komunikáciu s dotknutou osobou prostredníctvom sociálnych sietí, vždy je na rozhodnutí dotknutej osoby, že si vyberie toto médium na komunikáciu,
- zdravotná poisťovňa na svojej webovej stránke komunikuje dotknutým osobám aké sociálne siete využíva, vrátane odkazu na ich informácie o spracúvaní osobných údajov s upozornením, že poisťovňa nie je zodpovedná za spracúvanie osobných údajov zo strany tretích strán, pričom toto spracúvanie prebieha v tretích krajinách,
- údaje získané z takejto komunikácie nebudú použité na určenie hodnoty klienta alebo na reklamu,
- údaje získané prostredníctvom sociálnych sietí budú zlikvidované do šiestich mesiacov od ich získania.

Za dodržiavania pravidiel komunikácie prostredníctvom sociálnych sietí je zodpovedný odbor zákazníckeho centra a úsek digitálneho marketingu.

2.4. V prípade, ak zdravotná poisťovňa využíva údaje zverejnené (vo verejne časti) profilu dotknutej osoby na sociálnych sieťach (napr. Facebook, LinkedIn), je vždy pred takýmto spracúvaním potrebné posúdiť, či na to má zdravotná poisťovňa právny základ. Právnym základom môže byť súhlas dotknutej osoby alebo oprávnený záujem zdravotnej poisťovne. Pri oprávnenom záujme je potrebné vždy posúdiť, či nad záujmom zdravotnej poisťovne neprevažuje záujem dotknutej osoby. Napr. prezeranie verejnej časti profilu záujemcu o zamestnanie v zdravotnej poisťovni je v zhode s očakávaniami dotknutej osoby, a je teda povolené. Rovnako je povolené využívať verejnú časť profilu dotknutej osoby pre účely odhaľovania protispoločenskej činnosti.

Článok XVI
Oznámenie porušenia ochrany osobných údajov

1. **Akékoľvek porušenie ochrany osobných údajov (najmä únik, znehodnotenie, strata osobných údajov bez ohľadu na rozsah) je potrebné bezodkladne, do 24 hodín po zistení, oznámiť riaditeľovi úseku právneho a compliance na email dataprotection@union.sk.**
2. Primárnu zodpovednosť za oznámenie majú členovia stredného manažmentu. Nezbavuje to však zodpovednosti a povinnosti ostaných zamestnancov, aby včas incident rozpoznali a oznámili ho.
3. Oznámenie sa podáva e-mailom a musí obsahovať:
   a) opis povahy porušenia ochrany osobných údajov vrátane, podľa možnosti, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch, dátum vzniku udalosti, prípadnú dĺžku trvania udalosti, dátum zistenia udalosti, meno a priezvisko zamestnanca, ktorý udalosť zistil,
   b) opis pravdepodobných následkov porušenia ochrany osobných údajov;
   c) opis opatrení prijatých alebo navrhovaných s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.
3. Riaditeľ úseku právneho a compliance následne bezodkladne posúdi incident a:
   3.3. V prípade, ak incident spôsobilo aj technické zlyhanie bezpečnostných prvkov, oznámi incident sekcii riadenia rizík za účelom jeho prešetrenia a vyhodnotenia rizika,
   3.4. V prípade, ak je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb, oznámi incident Úradu na ochranu osobných údajov tak, aby oznámenie bolo tomuto úradu doručené do 72 hodín od zistenia incidentu,
   3.5. V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, rozhodne o tom, že incident bude oznámený dotknutej osobe, pričom zároveň určí organizačný útvar, ktorý bude povinný zabezpečiť komunikáciu s dotknutou osobou.
4. Právny odbor vedie register incidentov v oblasti ochrany osobných údajov minimálne v rozsahu podľa odseku 3 tohto článku.
5. Rovnako sa postupuje aj v prípade, ak incident oznámi zdravotnej poisťovni sprostredkovateľ.

Článok XVII
Sankcie

1. Porušenie mlčanlivosti a nedodržiavanie povinností určených touto smernicou a právnymi predpismi pre oblasť ochrany osobných údajov považuje zdravotná poisťovňa za závažné porušenie pracovnej disciplíny, na základe čoho môže byť so zamestnancom skončený pracovný pomer. Neoprávnené nakladanie s osobnými údajmi môže byť tiež trestným činom.
2. Úrad na ochranu osobných údajov môže zdravotnej poisťovni za porušenie právnych predpisov pre oblasť ochrany osobných údajov uložiť viaceré sankcie, z ktorých najzávažnejšie sú:
   a) nariadiť prevádzkovateľovi alebo sprostredkovateľovi, aby svoje spracovateľské operácie zosúladil s právnymi predpismi pre oblasť ochrany osobných údajov,
   b) nariadiť dočasné alebo trvalé obmedzenie spracúvania vrátane zákazu spracúvania,
   a) uložiť správnu pokutu až do výšky 20 000 000 eur alebo až do výšky 4 % celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia.

Článok XVIII
Záverečné ustanovenia

1. Táto smernica nadobudne účinnosť dňom 25.5.2018.
2. Táto smernica nahrádza predchádzajúcu verziu smernice o ochrane osobných údajov.
3. Za aktualizáciu tejto smernice je zodpovedný riaditeľ úseku právneho a compliance.

V Bratislave 22.5.2018

.....

Mgr. Michal Špaňár, MBA
predseda predstavenstva
Union zdravotná poisťovňa, a.s.

.....

Ing. Jozef Koma, PhD.
člen predstavenstva
Union zdravotná poisťovňa, a.s.

Príloha č. 1

Hromadný prístup k databáze osobných údajov v produkčnom systéme

Prístup k databázovým údajom informačného systému Mediform prostredníctvom SQL nástrojov majú okrem administrátorov a vývojárov informačného systému len presne vymedzené skupiny zamestnancov – užívateľov. Prístup užívateľov k databáze môže byť len v nevyhnutnom rozsahu na splnenie pracovných povinností a musí spĺňať podmienky na účel spracúvania osobných údajov.

Účel spracúvania osobných údajov v podmienkach zdravotnej poisťovne je špecifikovaný v článku VIII smernice. V prípade, ak chcú zamestnanci spracúvať osobné údaje na iné účely, je potrebné odsúhlasenie takéhoto spracúvania zo strany riaditeľa úseku právneho a compliance ako zodpovednej osoby a príslušných vlastníkov údajov.

Rozsah osobných údajov (OÚ), ku ktorým majú predstavitelia týchto skupín prístup prostredníctvom nástroja na výber dát, odsúhlasujú príslušní vlastníci údajov. Vlastníci údajov odsúhlasujú aj prístup k databáze pre užívateľov, ktorí nepatria do nižšie uvedených skupín. Žiadosť o prístup podáva vedúci zamestnanec zodpovedný za organizačný útvar, ktorého zamestnanci majú dostať prístup k databáze.

Touto smernicou sa schvaľujú prístupy k databáze systému Mediform prostredníctvom SQL nástrojov pre nasledovné skupiny:

- Odbor plánovania a controllingu
- Špecialista/-ka obchodných analýz