Slovenská komora sociálnych pracovníkov a asistentov sociálnej práce
Mokrohájska cesta 3, 841 04 Bratislava, IČO: 50012592; DIČ: 2120158645

INTERNÁ SMERNICA č. OCK / 6-2016
Ochrana osobných údajov v pôsobnosti Slovenskej komory SP a ASP

Spracoval/a:	Mgr. Martina Gymerská	Podpísal a schválil:	Mgr. Peter Kulifaj, Predseda komory
Počet strán:	37	Počet príloh:	10
Účinnosť od:	6.9.2016	Dátum schválenia Predstavenstvom komory	6.9.2016

Čl. 1 Pôsobnosť internej smernice

1. Táto interná smernica upravuje podrobnosti o ochrane osobných údajov spracovávaných Slovenskou komorou sociálnych pracovníkov a asistentov sociálnej práce, o povinnostiach komory pri spracúvaní osobných údajov v informačnom systéme, o rozsahu povinností a zodpovednosti oprávnenej osoby a zodpovednej osoby za dohľad nad ochranou osobných údajov a ďalšie súvisiace náležitosti.
2. Táto interná smernica o ochrane osobných údajov v pôsobnosti Slovenskej komory sociálnych pracovníkov a asistentov sociálnej práce bola vypracovaná v súlade § 19 ods. 2 a § 20 zákona č. 122/2013 Z. z. o ochrane osobných údajov, na ktorý sa často v texte odvoláva. Pre zjednodušenie sa v texte pri odvolávke používa označenie len „Zákon“ s veľkým písmenom na začiatku – pre odlíšenie od odvolávky na iné zákony.
3. Interné smernice, upravujúce postup pri činnosti komory vydáva a schvaľuje predstavenstvo komory.

Čl. 2 Definícia základných pojmov a používaných skratiek

1. ***Adresa*** – je súbor údajov o pobyte fyzickej osoby, do ktorého patria názov ulice, orientačné, prípadne súpisné číslo domu, názov obce, prípadne názov časti obce, poštové smerovacie číslo, názov okresu, názov štátu.
2. ***Audit bezpečnosti informačného systému*** – nezávislé odborné posúdenie spoľahlivosti a celkovej bezpečnosti informačného systému z hľadiska zabezpečenia dôvernosti, integrity a dostupnosti spracúvaných údajov.
3. ***Automatizovaný informačný systém*** (ďalej aj „AIS“) – súhrn technických prostriedkov výpočtovej techniky, programové a aplikačné vybavenie, údajová základňa, pamäťové médiá s údajmi, inštalačné médiá, dokumentácia súvisiaca s technickým a programovým vybavením určeným na automatizované spracovanie údajov.
4. ***Cezhraničný tok osobných údajov*** – je prenos osobných údajov mimo územia Slovenskej republiky a na územie Slovenskej republiky.
5. ***Informačný systém*** (ďalej aj „IS“) – jedná sa o akýkoľvek usporiadaný súbor, sústavu alebo databázu, v ktorých sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií, bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe. Informačným systémom sa na účely Zákona rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania (napríklad kartotéka, zoznamy členov, register povolení na výkon samostatnej praxe sociálneho pracovníka, záznam alebo sústava obsahujúca spisy, doklady, zmluvy, potvrdenia, hodnotenia a pod).
6. ***Likvidácia osobných údajov*** – zrušenie osobných údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať.
7. ***Osoba dotknutá*** (ďalej aj „dotknutá osoba“) – je každá fyzická osoba, o ktorej sa spracúvajú osobné údaje.
8. ***Osoba oprávnená*** (ďalej aj „oprávnená osoba“) – je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania alebo v rámci výkonu verejnej funkcie, a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v poučení podľa § 21 Zákona.

9. ***Osoba zodpovedná*** (ďalej aj „zodpovedná osoba“) – je odborne vyškolená osoba zodpovedná v rámci komory za ochranu osobných údajov, ktorú prevádzkovateľ informačného systému (v našom prípade komora) písomne poveril dozerať na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov.
10. ***Osobné údaje*** – údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takouto osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.
11. ***Poskytovanie osobných údajov*** – pre účely tejto internej smernice sa rozumie odovzdávanie osobných údajov na spracúvanie v rámci komory. Podľa Zákona v širšom kontexte ide aj o odovzdávanie osobných údajov na spracúvanie inej právnickej alebo fyzickej osobe, prípadne subjektu v cudzine.
12. ***Poskytovateľ osobných údajov*** – je každá oprávnená osoba v rámci komory, ktorá zberá, spracúva a zadáva osobné údaje do informačného systému.
13. ***Používateľ*** – je právnická alebo fyzická osoba, prípadne subjekt v cudzine, ktorému sú sprístupnené osobné údaje z informačného systému, resp. má oprávnený prístup do IS s osobnými údajmi.
14. ***Používateľ oprávnený*** (ďalej aj „oprávnený používateľ“) – zamestnanec / člen komory, ktorému bol zriadený používateľský účet a pridelené príslušné prístupové práva umožňujúce mu plnenie pracovných povinností.
15. ***Používateľský účet*** – slúži na identifikáciu používateľa v automatizovanom informačnom systéme, umožňuje správne priradenie pridelených používateľských práv prihlásenému používateľovi, tvorí ho názov účtu a heslo.
16. ***Prevádzkovateľ*** – je každý, kto sám alebo spoločne s inými vymedzí účel spracúvania osobných údajov, určí podmienky ich spracúvania a spracúva osobné údaje vo vlastnom mene; ak účel, prípadne aj podmienky spracúvania osobných údajov ustanovuje zákon, priamo vykonateľný právne záväzný akt Európskej únie alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, prevádzkovateľom je ten, kto je na plnenie účelu spracúvania za prevádzkovateľa ustanovený alebo kto spĺňa zákonom, priamo vykonateľným právne záväzným aktom Európskej únie alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná, ustanovené podmienky. To znamená, že pred Zákonom je Slovenská komora sociálnych pracovníkov a asistentov sociálnej práce (ďalej len „komora“) prevádzkovateľom informačného systému s osobnými údajmi.
17. ***Spracúvanie osobných údajov*** – je vykonávanie operácií alebo súboru operácií s osobnými údajmi, najmä ich získavanie, zhromažďovanie, šírenie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, blokovanie, likvidácia, ich (cezhraničný) prenos, poskytovanie, sprístupňovanie alebo zverejňovanie.
18. ***Sprístupňovanie osobných údajov*** – je oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva.
19. ***Sprostredkovateľ*** – je každý, kto spracúva osobné údaje v mene prevádzkovateľa, v rozsahu a za podmienok dojednaných s prevádzkovateľom v písomnej zmluve podľa § 8 Zákona a v súlade so Zákonom.

20. ***Súhlas dotknutej osoby*** – akýkoľvek slobodne daný, výslovný a zrozumiteľný prejav vôle, ktorým dotknutá osoba na základe poskytnutých informácií vyjadruje súhlas so spracúvaním svojich osobných údajov.
21. ***Tretia strana*** – je každý, kto nie je dotknutou osobou, prevádzkovateľom poskytujúcim osobné údaje, jeho zástupcom, sprostredkovateľom alebo oprávnenou osobou.
22. ***Úrad na ochranu osobných údajov Slovenskej republiky*** (ďalej aj „Úrad“) – orgán štátnej správy s celoslovenskou pôsobnosťou so sídlom v Bratislave, ktorý vykonáva nezávislý dozor nad ochranou osobných údajov a podieľa sa na ochrane základných práv a slobôd fyzických osôb pri spracúvaní ich osobných údajov.
23. ***Zverejňovanie osobných údajov*** – je publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri alebo v operáte, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste.

Čl. 3 Podmienky spracúvania osobných údajov

1. Účel a prostriedky spracúvania osobných údajov stanovuje komora pre tie IS, ktorých je prevádzkovateľom, pokiaľ účel a prostriedky spracúvania osobných údajov pre konkrétny IS nie je stanovený osobitným zákonom.
2. Ak účel spracúvania osobných údajov stanovuje osobitný zákon, v takom prípade zabezpečí komora jeho primeranú aplikáciu v rámci vlastných podmienok.
3. Účelom spracúvania osobných údajov je vopred jednoznačne vymedzený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.
4. Spôsob a podmienky spracúvania osobných údajov musí vždy zodpovedať stanovenému účelu ich spracúvania a musí byť v súlade so zákonmi.
5. Pred začatím každého spracúvania osobných údajov musia byť vopred stanovené:
   a) identifikácia IS, v ktorom budú údaje spracúvané,
   b) účel spracúvania osobných údajov,
   c) zoznam spracúvaných údajov,
   d) okruh dotknutých osôb,
   e) právny základ IS,
   f) dátum začatia spracúvania osobných údajov,
   g) organizačná zložka, ktorá riadi spracúvanie osobných údajov,
   h) ďalšie organizačné zložky alebo zamestnanci, ktorí sa podieľajú na spracúvaní údajov, s uvedením povolených činností pri spracúvaní osobných údajov,
   i) spôsob získavania osobných údajov,
   j) spôsob nakladania s údajmi po splnení a skončení účelu ich spracúvania,
   k) doba archivácie osobných údajov po skončení účelu ich spracúvania,
   l) okruh príjemcov, ktorým sú osobné údaje sprístupnené,
   m) tretie strany, ktorým sú osobné údaje poskytnuté,
   n) forma a právny základ zverejnenia osobných údajov,
   o) tretie krajiny do ktorých je uskutočňovaný cezhraničný prenos osobných údajov a právny základ cezhraničného toku.
6. Vyplnenie a aktualizáciu údajov uvedených v predchádzajúcom bode do formulára podľa prílohy č. 1 tejto smernice (*Príloha č. 1 Evidencia informačného systému osobných údajov*) zabezpečuje

zodpovedná osoba za komoru, ktorá na základe poverenia štatutárneho zástupcu vykonáva dohľad nad ochranou osobných údajov pri ich spracúvaní.

7. Navrhované podmienky spracúvania osobných údajov posúdi pred začatím ich spracúvania poverená zodpovedná osoba z pohľadu zaistenie ich súladu so Zákonom. V odôvodnených alebo komplikovaných prípadoch posúdenia súladu podmienok spracúvania osobných údajov so Zákonom spolupracuje poverená zodpovedná osoba za komoru so štatutárnym zástupcom komory.
8. V prípade kladného posúdenia podľa predchádzajúceho bodu a zabezpečenia zákonných podmienok pri spracúvaní osobných údajov povolí spracúvanie osobných údajov štatutárny zástupca komory na základe predloženého a schváleného Formulára evidencie informačného systému (Príloha č. 1 Evidencia informačného systému osobných údajov).
9. Ak v priebehu spracúvania osobných údajov príde k zmene spôsobu a podmienkam spracúvania osobných údajov, posúdenie uvedené v bode 5 – 7 tohto článku sa zopakuje.
10. Účel spracúvania osobných údajov v rámci komory musí byť v súlade s jej pôsobnosťou určenou zriaďovacou listinou, organizačným poriadkom, štatútom a zákonom č. 219/2014 Z.z. o sociálnej práci a o podmienkach na výkon niektorých odborných činností v oblasti sociálnych vecí a rodiny a o zmene a doplnení niektorých zákonov. Spracúvanie osobných údajov za iným účelom sa zakazuje.
11. Bez predchádzajúceho schválenia a ďalších obmedzení je možné spracúvať osobné údaje, ktoré boli získané náhodne, bez predchádzajúceho určenia účelu a prostriedkov spracúvania, bez zámeru ich ďalšieho spracúvania v usporiadanom systéme podľa osobitných kritérií, ak nie sú ďalej systematicky spracúvané. Prevádzkovateľ takéto údaje nezverejní ani neposkytne ďalším subjektom.
12. Spracúvanie osobných údajov iným spôsobom, ako stanovuje táto interná smernica sa zakazuje.

Čl. 4 Získavanie osobných údajov

1. Získavanie osobných údajov je vykonávanie akýchkoľvek operácií, ktoré vedú k nadobudnutiu osobných údajov o dotknutej osobe na ich systematické spracúvanie v IS, ktoré sa vykonáva v zmysle vopred stanoveného účelu ich spracúvania.
2. Dotknutá osoba musí byť pred poskytnutím svojich osobných údajov vopred oboznámená s podmienkami ich spracúvania v IS a to v rozsahu stanovenom Zákonom. Takéto oboznámenie nie je potrebné, ak s ohľadom na všetky okolnosti vie komora na žiadosť Úradu kedykoľvek preukázať, že v čase získavania osobných údajov boli všetky potrebné informácie o dotknutej osobe už známe.
3. Pri získaných osobných údajoch musí byť uvedený zdroj od ktorého boli získané, s výnimkou tých údajov, pre ktoré je ich zdroj evidentný aj bez jeho explicitného uvedenia.
4. V prípade, ak komora získa osobné údaje z iného zdroja ako od samotnej dotknutej osoby, musí byť pred ich vložením do IS rozhodnuté o spôsobe oboznámenia dotknutej osoby s podrobnosťami ich spracúvania v súlade so Zákonom.
5. Pri získavaní osobných údajov je možné vytvárať kópie úradných dokladov iba ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby alebo s písomným súhlasom dotknutej osoby. Takýto súhlas si nemožno vynucovať ani jeho získanie ináč podmieňovať.
6. Do IS možno poskytnúť len pravdivé osobné údaje. Za pravdivosť osobných údajov zodpovedá ten, kto ich do informačného systému poskytol. Komora považuje poskytnutý osobný údaj za pravdivý, kým sa nepreukáže opak.

7. Opravu nepravdivých, nesprávnych alebo neaktuálnych osobných údajov oznámi komora do 30 dní od jej vykonania dotknutej osobe a každému, komu ich poskytol. Od oznámenia možno upustiť, ak sa tým neporušia práva dotknutej osoby.
8. Pri získavaní osobných údajov musí byť vždy zachovaná ich diskrétnosť.
9. Ustanovenia bodu 2 až 7 tohto článku internej smernice sa nepoužijú pri spracúvaní osobných údajov k nasledovným účelom:
   a.) ak osobné údaje spracúva prevádzkovateľ, ktorému to vyplýva z predmetu jeho činnosti;
   b.) spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, v ktorej vystupuje dotknutá osoba ako jedna zo zmluvných strán, na zavedenie predzmluvných vzťahov alebo opatrení vykonávaných na žiadosť dotknutej osoby;
   c.) pre potreby poštového styku a evidencie údajov v rozsahu titul, meno, priezvisko a adresa dotknutej osoby bez možnosti priradiť k nim ďalšie jej osobné údaje;
   d.) ak predmetom spracúvania sú už zverejnené osobné údaje; v týchto prípadoch je potrebné osobné údaje náležite označiť.
10. Pokiaľ získavanie a následné spracúvanie osobných údajov nie je vykonávané podľa osobitných zákonov, ktoré stanovujú účel a podmienky ich spracúvania alebo pri ich získavaní nie je možné uplatniť výnimky stanovené Zákonom, musí byť vždy pred ich zaradením do IS získaný predchádzajúci písomný súhlas dotknutej osoby podľa vzoru uvedeného v prílohe č. 7 tejto smernice (Príloha č. 7 Súhlas dotknutej osoby so spracúvaním osobných údajov).
11. Získavanie osobných údajov dotknutých osôb iným, ako vyššie uvedeným spôsobom sa zakazuje.

Čl. 5 Nakladanie s osobnými údajmi po splnení účelu spracúvania

1. Po splnení účelu spracúvania sú osobné údaje archivované a neskôr vyraďované podľa platných interných predpisov komory.
2. Úschovné lehoty písomných, obrazových, zvukových a iných záznamov, ktoré obsahujú osobné údaje a sú zaradené do predarchívnej starostlivosti, možno stanoviť len na dobu nevyhnutnú na uplatnenie práv alebo povinností ustanovených Zákonom.
3. Likvidáciu osobných údajov oznámi komora do 30 dní od jej vykonania dotknutej osobe a každému, komu ich poskytla. Od oznámenia možno upustiť, ak sa tým neporušia práva dotknutej osoby.

Čl. 6 Prístup k osobným údajom

1. Prístup zamestnancov komory k spracúvaným osobným údajom dotknutých osôb je možný len za účelom plnenia určených pracovných povinností. Prístup nad uvedený rámec sa zakazuje.
2. Uložené pracovné povinnosti musia byť vždy v súlade s účelom spracúvania osobných údajov vymedzenom Bezpečnostným projektom na ochranu osobných údajov a v súlade s legislatívnymi normami vzťahujúcimi sa na daný účel spracúvania osobných údajov, najmä so Zákonom.
3. Pre každý účel spracúvania osobných údajov musí byť určené a zrejmé, ktorý zamestnanec / člen komory takéto spracúvanie zabezpečuje. Prístup k osobným údajom majú iba určené osoby, ktoré spracúvanie osobných údajov za daným účelom zabezpečujú.
4. Podmienkou určenia oprávnenej osoby s prístupom k osobným údajom dotknutých osôb je jej poučenie o právach a zodpovednosti za ochranu osobných údajov, ktorého súčasťou je poučenie o rozsahu povolených spracovateľských operácií a zásadách prístupu k IS, v ktorom sa spracúvanie osobných údajov vykonáva.

5. Sprístupnenie osobných údajov ďalším zamestnancom / členom komory schvaľuje štatutárny zástupca komory. Poverená zodpovedná osoba za komoru vedie agendu žiadostí o prístup k osobným údajom, zoznam oprávnených osôb s prístupom k osobným údajom a na základe predložených požiadaviek vykonáva jeho aktualizáciu podľa vzoru uvedeného v prílohe č. 5 tejto smernice (Príloha č. 5 Určenie oprávnených osôb s prístupom k osobným údajom).
6. Prístup k spracúvaným osobným údajom nad vymedzený rámec sa zakazuje.

Čl.7 Sprostredkovateľ

1. Sprostredkovateľ je povinný spracúvať osobné údaje len v rozsahu a za podmienok dojednaných s komorou v písomnej zmluve.
2. Zmluva musí byť uzavretá pred začiatkom spracúvania osobných údajov sprostredkovateľom a musí podľa § 8 ods. 4 Zákona obsahovať:
   a) údaje o zmluvných stranách, teda identifikačné údaje komory a sprostredkovateľa;
   b) deň, od ktorého je sprostredkovateľ oprávnený začať so spracúvaním osobných údajov v mene komory;
   c) účel spracúvania osobných údajov;
   d) názov informačného systému;
   e) zoznam osobných údajov, ktoré sa budú spracúvať; zoznam osobných údajov možno nahradiť rozsahom osobných údajov podľa § 10 ods. 4 Zákona;
   f) okruh dotknutých osôb;
   g) podmienky spracúvania osobných údajov vrátane zoznamu povolených operácií s osobnými údajmi;
   h) vyhlásenie komory, že pri výbere sprostredkovateľa dbala na jeho odbornú, technickú, organizačnú a personálnu spôsobilosť a jeho schopnosť zaručiť bezpečnosť spracúvaných osobných údajov opatreniami podľa § 19 ods. 1 Zákona;
   i) dobu, na ktorú sa zmluva uzatvára;
   j) dátum uzatvorenia zmluvy a podpisy zmluvných strán.
3. Sprostredkovateľ musí poskytovať záruky bezpečnosti pri spracúvaní osobných údajov, najmä v oblasti technickej, organizačnej a personálnej bezpečnosti. Komora pred uzavretím zmluvy alebo poverenia so sprostredkovateľom primeraným spôsobom zhodnotí dostatočnosť a mieru naplnenia týchto záruk, za týmto účelom môže požadovať od sprostredkovateľa súčinnosť.
4. Sprostredkovateľ musí spĺňať ďalšie legislatívne požiadavky kladené na spracúvanie osobných údajov, vyplývajúce najmä zo Zákona.

Čl.8 Dohľad nad ochranou osobných údajov

1. Komora zabezpečuje výkon dohľadu nad ochranou osobných údajov v rozsahu a za podmienok určených Zákonom. Komora písomne poverí výkonom dohľadu zodpovednú osobu.
2. Písomné poverenie zodpovednej osoby alebo viacerých zodpovedných osôb vykonáva štatutárny zástupca komory, pritom postupuje podľa Zákona.
3. Vzor písomného poverenia zodpovednej osoby je uvedený v prílohe č.2 tejto smernice (Príloha č. 2 Poverenie zodpovednej osoby). Zakladá sa do osobného spisu zamestnanca, jeho kópia sa zakladá do dokumentácie Bezpečnostného projektu na ochranu osobných údajov komory.
4. Komora písomne informuje Úrad o poverení všetkých zodpovedných osôb za komoru, formou a spôsobom požadovanými Zákonom, to do 30 dní odo dňa jej poverenia alebo po zmene zodpovednej osoby, ktorá bola skôr nahlásená Úradu.

5. Každá zodpovedná osoba poverená výkonom dohľadu nad ochranou osobných údajov musí byť bezúhonná, musí mať spôsobilosť na právne úkony v plnom rozsahu a musí absolvovať skúšku na výkon funkcie zodpovednej osoby, o čom má platné potvrdenie. Doklad o absolvovaní skúšky alebo jeho kópia je súčasťou osobného spisu zamestnanca, kópia potvrdenia o skúške na výkon funkcie zodpovednej osoby sa taktiež zakladá do Bezpečnostného projektu na ochranu osobných údajov komory.
6. Zodpovedná osoba poverená k výkonu dohľadu nad ochranou osobných údajov v podmienkach komory má najmä nasledovné povinnosti zodpovednej osoby, ktoré sú vymedzené v § 27 Zákona a zahŕňajú nasledujúce činnosti:
   a) zodpovedná osoba je povinná pred začatím spracúvania osobných údajov v informačnom systéme posúdiť, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb. Zistenie narušenia práv a slobôd dotknutých osôb pred začatím spracúvania alebo porušenia zákonných ustanovení v priebehu spracúvania osobných údajov je zodpovedná osoba povinná bez zbytočného odkladu písomne oznámiť štatutárnemu orgánu komory; ak štatutárny orgán komory po upozornení bez zbytočného odkladu nevykoná nápravu, oznámi to zodpovedná osoba Úradu;
   b) zabezpečuje potrebnú súčinnosť s Úradom pri plnení úloh patriacich do jeho pôsobnosti; na požiadanie je zodpovedná osoba povinná Úradu kedykoľvek predložiť svoje písomné poverenie a písomné oznámenia podľa písmena a);
   c) zabezpečuje dohľad nad plnením základných povinností prevádzkovateľa podľa § 6 Zákona;
   d) zabezpečuje poučenie oprávnených osôb podľa § 21 Zákona, pred vydaním prvého pokynu na realizáciu spracovateľských operácií, o čom vedie písomný záznam, ktorý sa v jednom výtlačku ukladá v osobnom spise zamestnanca a v jednom výtlačku v dokumentácii Bezpečnostného projektu na ochranu osobných údajov komory, podľa vzoru uvedeného v prílohe č. 4 tejto smernice (Príloha č. 4 Záznam o poučení oprávnenej osoby);
   e) zabezpečuje vybavovanie žiadostí dotknutých osôb podľa § 28 až 30 Zákona;
   f) zabezpečuje prijatie bezpečnostných opatrení podľa § 19 ods. 1 až 3 Zákona, dohliada na ich aplikáciu v praxi a zabezpečuje ich aktualizáciu podľa § 19 ods. 4 Zákona;
   g) zabezpečuje dohľad pri výbere Sprostredkovateľa, prípravu písomnej zmluvy so Sprostredkovateľom a zodpovedá za jej obsah. Počas trvania zmluvného vzťahu preveruje dodržiavanie dohodnutých podmienok;
   h) ak sa uskutočňuje cezhraničný tok osobných údajov, vykonáva dohľad nad jeho realizáciou;
   i) zabezpečuje prihlásenie IS na osobitnú registráciu, oznamovanie zmien a odhlásenie IS z osobitnej registrácie. O IS, ktoré registrácii nepodliehajú vedie centrálnu evidenciu v rozsahu a za podmienok stanovených Zákonom;
   j) vyjadruje sa k navrhovaným zmenám, pracovným postupom a procedúram týkajúcim sa spracúvania osobných údajov v podmienkach komory;
   k) metodicky usmerňuje ďalšie zodpovedné osoby komory v otázkach výkonu dohľadu nad ochranou osobných údajov;
   l) o zistených skutočnostiach pri výkone dohľadu nad ochranou osobných údajov, o stave spracúvania osobných údajov a prípadných návrhoch písomne informuje predsedu komory – min. 1 krát za kalendárny rok. Bezodkladne informuje predsedu komory o zistení porušenia Zákona pri spracúvaní osobných údajov. K predmetným činnostiam poverená zodpovedná osoba využíva prílohy č. 9 a 10 tejto smernice.
   m) pred začatím nového spracúvania osobných údajov alebo pri zmene spôsobu ich spracúvania posúdi, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb;

n) zabezpečuje výkon práv dotknutých osôb podľa článku 12 tejto smernice;
o) vedie a sprístupňuje evidenciu o IS, v ktorých komora vykonáva spracúvanie osobných údajov podľa článku 10 tejto internej smernice.

Čl.9 Práva, povinnosti a určenie oprávnených osôb

1. Fyzická osoba navrhovaná na oboznamovanie sa s osobnými údajmi v rámci jej pracovného zaradenia absolvuje poučenie oprávnenej osoby prijímanej do pracovného pomeru spravidla ku dňu vzniku pracovného pomeru, avšak vždy pred vydaním prvého pokynu k spracovateľskej operácii.
2. Poučenie oprávnenej osoby vykonáva poverená zodpovedná osoba za IS alebo iná ňou určená osoba, ktorá je kompetentná podať všetky nasledovné informácie v požadovanom rozsahu:
   a) o právach a povinnostiach ustanovených Zákonom, inými právnymi predpismi a o zodpovednosti za ich porušenie;
   b) o rozsahu oprávnení;
   c) o rozsahu a popise povolených činností pri prístupe k osobným údajom;
   d) o podmienkach spracúvania osobných údajov;
   e) o spôsobe výkonu uložených činností pri práci s informačným systémom;
   f) o pravidlách a spôsobe ochrany osobných údajov pred ich stratou, poškodením alebo neautorizovaným prístupom;
   g) o povinnosti mlčanlivosti o osobných údajov v súlade s §22 Zákona, ktoré trvá aj po zániku funkcie oprávnenej osoby, ale aj po skončení pracovného pomeru.
3. Absolvovanie poučenia potvrdí oprávnená osoba vlastnoručným podpisom. Evidenciu písomného poučenia oprávnenej osoby zabezpečuje zodpovedná osoba, ktorá poučenie vykonala, prípadne iná ňou určená osoba. Poučenie sa vyhotovuje v jednom výtlačku, ktorý sa zakladá do osobného spisu, alebo priamo do dokumentácie Bezpečnostného projektu na ochranu osobných údajov komory, ktorú vedie a aktualizuje zodpovedná osoba za IS.
4. Písomný zoznam určených oprávnených osôb s prístupom k osobným údajom vedie a aktualizuje poverená zodpovedná osoba za komoru. Zoznam je uložený v dokumentácii Bezpečnostného projektu na ochranu osobných údajov komory a vyhotovuje sa podľa vzoru vedeného v prílohe č. 5 tejto smernice (Príloha č. 5 Určenie oprávnených osôb s prístupom k osobným údajom).
5. Písomný zoznam určených oprávnených osôb s prístupom k osobným údajom je platný po jeho schválení štatutárnym zástupcom komory.
6. Každá iná fyzická osoba a pracovník tretej strany (subdodávateľa), ktorému budú sprístupnené osobné údaje spracúvané komorou, musí byť informovaný o:
   a) rozsahu oprávnení a povolených činností pri prístupe k osobným údajom;
   b) spôsobe výkonu uložených činností pri práci s informačným systémom;
   c) pravidlách a spôsobe ochrany osobných údajov pred ich stratou, poškodením alebo neautorizovaným prístupom;
   d) poučený o mlčanlivosti v súlade s §22 Zákona.
7. Oprávnená osoba musí byť informovaná o zodpovednej osobe poverenej dohľadom nad ochranou osobných údajov v rámci komory.
8. V prípade zmeny spôsobu spracúvania osobných údajov v IS je oprávnená osoba, ktorá tieto zmeny vykonala, povinná toto bezodkladne ohlásiť poverenej zodpovednej osobe za komoru.
9. Oprávnená osoba má právo vykonávať spracovateľské operácie s osobnými údajmi spracúvanými v informačných systémoch, v ktorých bola určená ako oprávnená osoba na základe pokynu štatutárneho zástupcu komory, výlučne v súlade s právnym základom, od ktorého komora odvodzuje oprávnenie spracúvať osobné údaje, a to len v rozsahu

a spôsobom, ktorý je nevyhnutný na dosiahnutie ustanoveného alebo vymedzeného účelu spracúvania a je v súlade so Zákonom a inými zákonmi, všeobecne záväznými právnymi predpismi a internými smernicami komory.

10. Oprávnená osoba má právo najmä na:
    a) pridelenie prístupových práv do určených informačných systémov osobných údajov komory v rozsahu nevyhnutnom na plnenie jej úloh; nevyhnutnosť priamo determinuje pracovné zaradenie oprávnenej osoby v rozsahu opisu činností jej pracovného miesta;
    b) opätovné poučenie, ak došlo k podstatnej zmene jej pracovného alebo funkčného zaradenia a tým sa významne zmenil obsah náplne jej pracovných činností, alebo sa podstatne zmenili podmienky spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov v rámci jej pracovného alebo funkčného zaradenia;
    c) porušenie povinnosti mlčanlivosti uloženej podľa § 22 ods. 2 Zákona, ak je to nevyhnutné na plnenie úloh súdov a orgánov činných v trestnom konaní podľa osobitného zákona alebo vo vzťahu k Úradu pri plnení jeho úloh podľa Zákona; ustanovenia o povinnosti mlčanlivosti podľa osobitných predpisov tým nie sú dotknuté;
    d) vykonávanie spracovateľských operácii s osobnými údajmi v mene komory, vrátane osobitnej kategórie osobných údajov, v rozsahu nevyhnutnom na plnenie pracovných úloh určených opisom pracovného miesta oprávnenej osoby;
    e) odmietnutie vykonať pokyn k spracúvaniu osobných údajov, ktorý je v rozpore so všeobecne záväznými právnymi predpismi alebo dobrými mravmi;
    f) na vydanie dokladu (poverenia), ktorým bude preukazovať svoju pracovnú príslušnosť k zamestnávateľovi /ku komore v prípade, že získava osobné údaje mimo sídla komory.
11. Vo vzťahu ku kontrole vykonávanej podľa Zákona oprávnená osoba má právo najmä:
    a) na profesionálny prístup kontrolného orgánu pri výkone kontroly;
    b) vyžadovať od kontrolného orgánu preukázať sa poverením na vykonanie kontroly a svojou príslušnosťou k Úradu, ak je oprávnenou osobou štatutárny orgán, alebo osoba oprávnená konať v mene štatutárneho orgánu; to platí aj v prípade, ak sa na kontrole zúčastňuje aj prizvaná osoba;
    c) oboznamovať sa s kontrolnými zisteniami a písomne sa k nim vyjadrovať, ak je oprávnenou osobou štatutárny orgán alebo osoba oprávnená konať v mene štatutárneho orgánu;
    d) podávať písomné námietky po oboznámení sa s kontrolnými zisteniami, ak je oprávnenou osobou štatutárny orgán alebo osoba oprávnená konať v mene štatutárneho orgánu;
    e) vyžadovať plnenie povinností kontrolného orgánu pri výkone kontroly podľa § 55 Zákona, ak je oprávnenou osobou štatutárny orgán alebo osoba oprávnená konať v mene štatutárneho orgánu.
12. Rozsah konkrétnych spracovateľských operácií, ktorý bude oprávnená osoba vykonávať, je definovaný úrovňou prístupu k jednotlivým informačným systémom osobných údajov, ktorá je zaznamenaná v formulári s názvom Určenie oprávnených osôb s prístupom k osobným údajom (viď. Príloha č. 5 tejto smernice).
13. Oprávnená osoba je v súvislosti so spracúvaním osobných údajov povinná rešpektovať príslušné povinnosti formulované komorou najmä v rámci:
    a) bezpečnostnej dokumentácie informačných systémov osobných údajov,
    b) interných predpisov ktoré súvisia s výkonom pracovnej pozície a s ktorými bola oboznámená pred prvým pokynom k spracovateľskej operácii.
14. Oprávnená osoba spracúva osobné údaje len na základe pokynu prevádzkovateľa IS prostredníctvom svojho priameho nadriadeného, ktorý je povinný oprávnenú osobu oboznámiť aj s rozsahom spracovateľských operácií.

15. Oprávnená osoba nesmie osobné údaje spracúvané komorou využiť pre osobnú potrebu, či potrebu inej osoby alebo na iné, než služobné účely. Je zakázané poskytovať alebo sprístupňovať osobné údaje dotknutých osôb iným osobám ako oprávneným alebo subjektom určeným osobitným zákonom, poskytovať osobné údaje a dôverné informácie k nim prostredníctvom telefónu, kedy nie je možné overiť totožnosť prijímateľa a jeho faktické oprávnenie na oboznamovanie sa so spracúvanými osobnými údajmi. V prípade pochybnosti o správnosti postupu je oprávnená osoba povinná vopred informovať poverenú zodpovednú osobu a vyžiadať si jej stanovisko.
16. Oprávnená osoba je povinná:
    a) stanovovať úschovné lehoty záznamov, ktoré obsahujú osobné údaje, v súlade s Registratúrnym poriadkom a registratúrnym plánom komory a u záznamov, ktoré sú zaradené do predarchívnej starostlivosti stanovovať len dobu nevyhnutnú na uplatnenie práv alebo povinností ustanovených osobitným zákonom (napr. Antidiskriminačný zákon);
    b) poznať poverenú zodpovednú osobu za komoru a poverenú zodpovednú osobu za jednotlivé IS, v ktorých vystupuje ako oprávnená osoba;
    c) poverenej zodpovednej osobe a v prípade nebezpečenstva z omeškania najbližšiemu nadriadenému bezodkladne oznámiť skutočnosti o porušení ustanovení Zákona alebo o vzniku bezpečnostného incidentu;
    d) získavať na základe svojho pracovného zaradenia pre komoru len nevyhnutné osobné údaje výlučne na zákonom ustanovený alebo vymedzený účel; je neprípustné, aby oprávnená osoba získavala osobné údaje pod zámienkou iného účelu spracúvania alebo inej činnosti;
    e) vykonávať povolené spracovateľské operácie len so správnymi, úplnými a podľa potreby aktualizovanými osobnými údajmi vo vzťahu k účelu spracúvania;
    f) nesprávne a neúplné osobné údaje je bez zbytočného odkladu povinná opraviť alebo doplniť; nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné je povinná blokovať, kým sa rozhodne o ich likvidácii v súlade s Registratúrnym poriadkom a registratúrnym plánom komory;
    g) pred získavaním osobných údajov od dotknutej osoby ju oboznámiť s názvom a sídlom komory, účelom spracúvania osobných údajov, rozsahom spracúvania osobných údajov, predpokladanom okruhu tretích strán pri poskytovaní osobných údajov alebo príjemcov pri sprístupňovaní osobných údajov, o forme zverejnenia, ak sa osobné údaje zverejňujú a o tretích krajinách, ak sa predpokladá, alebo je zrejmé, že sa do týchto krajín uskutoční cezhraničný prenos osobných údajov a o ďalších informáciách v súlade s §15 Zákona;
    h) poučiť dotknutú osobu o dobrovoľnosti, alebo povinnosti poskytnutia osobných údajov a o existencii jej práv podľa § 28 Zákona;
    i) zabezpečiť preukázateľný súhlas na spracúvanie osobných údajov dotknutej osoby v informačnom systéme osobných údajov komory, ak sa osobné údaje spracúvajú na základe súhlasu dotknutej osoby, alebo ak to vyžaduje zákon č. 122/2013 Z. z. alebo osobitný zákon;
    j) preukázať príslušnosť oprávnenej osoby ku komore hodnoverným dokladom;
    k) získavať osobné údaje nevyhnutné na dosiahnutie účelu spracúvania kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií len vtedy, ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby alebo na základe písomného súhlasu dotknutej osoby, ak je to nevyhnutné na dosiahnutie účelu spracúvania;
    l) postupovať výlučne v súlade s technickými, organizačnými a personálnymi opatreniami prijatými komorou podľa § 19 a 20 Zákona a ostatnými internými normami komory;

m) vykonať likvidáciu osobných údajov, ktoré sú súčasťou už nepotrebných pracovných dokumentov (napr. rôzne pracovné súbory, pracovné verzie dokumentov v listinnej podobe) rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať; to neplatí vo vzťahu k osobným údajom, ktoré sú súčasťou obsahu registratúrnych záznamov komory;
n) v prípade nejasností pri spracúvaní osobných údajov sa obrátiť na štatutárneho zástupcu komory alebo zodpovednú osobu;
o) chrániť prijaté dokumenty a súbory pred stratou, poškodením, zneužitím, odcudzením, neoprávneným sprístupnením, poskytnutím alebo inými neprípustnými formami spracúvania;
p) dodržiavať mlčanlivosť o osobných údajoch podľa § 22 ods. 2 Zákona, s ktorými oprávnená osoba v rámci svojho pracovného pomeru prichádza do styku, a to aj po zániku jej statusu, okrem zákonom priznaných výnimiek podľa § 22 ods. 5 Zákona;
q) dodržiavať všetky povinnosti, o ktorých bola oprávnená osoba poučená.

17. Vo vzťahu ku kontrole vykonávanej podľa Zákona oprávnená osoba kontrolovanej osoby je povinná najmä:
    a) poskytnúť Úradu potrebnú súčinnosť pri výkone jeho dozoru podľa Zákona;
    b) strpieť overenie totožnosti a preukázanie príslušnosti ku kontrolovanej osobe kontrolným orgánom pri výkone kontroly podľa Zákona;
    c) zdržať sa konania, ktoré by mohlo zmariť výkon kontroly;
    d) dostaviť sa na predvolanie Úradu s cieľom podať vysvetlenia v určenom čase na určené miesto, ak je oprávnenou osobou štatutárny orgán alebo osoba oprávnená konať v mene štatutárneho orgánu;
    e) umožniť kontrolnému orgánu výkon iných oprávnení kontrolného orgánu podľa § 56 Zákona, ak je oprávnenou osobou štatutárny orgán alebo osoba oprávnená konať v mene štatutárneho orgánu;
    f) oboznámiť sa s obsahom protokolu a na požiadanie kontrolného orgánu dostaviť sa na jeho prerokovanie, ak je oprávnenou osobou štatutárny orgán alebo osoba oprávnená konať v mene štatutárneho orgánu.
18. Oprávnená osoba je v zmysle § 22 Zákona povinná zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva a s ktorými príde do styku. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov. Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona, alebo vo vzťahu k Úradu pri plnení jeho úloh podľa Zákona; ustanovenia o povinnosti mlčanlivosti podľa osobitných predpisov tým nie sú dotknuté.
19. Porušením povinností alebo zneužitím oprávnení pri spracúvaní osobných údajov môže oprávnená osoba naplniť skutkovú podstatu správnych deliktov podľa § 68 ods. 7 písm. a) až e) a g) Zákona, a to nasledovným konaním:
    a) poskytnutím osobných údajov v rozpore s § 12 ods. 1 Zákona;
    b) poskytnutím nepravdivých osobných údajov podľa § 16 ods. 1 Zákona;
    c) nepostupovaním v súlade s technickými, organizačnými alebo personálnymi opatreniami prijatými prevádzkovateľom alebo sprostredkovateľom podľa § 19 a 20 Zákona;
    d) porušením svojich povinností uložených v zázname o poučení oprávnenej osoby podľa § 21 Zákona;
    e) porušením povinnosti mlčanlivosti o osobných údajoch podľa § 22 Zákona;
    f) neposkytnutím úradu požadovanú súčinnosť pri výkone dozoru podľa Zákona.

20. Oprávnená osoba môže v súvislosti s protiprávnym nakladaním s osobným údajmi čeliť aj trestnému stíhaniu za trestné činy podľa § 247 a § 374 zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov alebo môže voči nej byť vedené disciplinárne konanie.

Čl.10 Ochrana práv dotknutých osôb a vybavovanie žiadostí dotknutých osôb

1. Ochranu práv dotknutých osôb upravuje § 28 Zákona, ktorý dotknutej osobe umožňuje na základe písomnej žiadosti od komory požadovať vo všeobecne zrozumiteľnej forme najmä:
   a) informácie o stave spracúvania jej osobných údajov v informačnom systéme;
   b) informácie o zdroji, z ktorého boli osobné údaje získané;
   c) odpis spracúvaných osobných údajov;
   d) opravu nesprávnych, neúplných alebo neaktuálnych osobných údajov, ktoré sú v informačnom systéme spracúvané;
   e) likvidáciu osobných údajov, ak bol splnený účel ich spracúvania alebo pri spracúvaní došlo k porušeniu Zákona.
2. Práva dotknutej osoby popísané v bode 1 tohto článku možno obmedziť iba v rozsahu a za podmienok stanovených osobitným zákonom.
3. Dotknutá osoba má taktiež právo na základe bezplatnej písomnej žiadosti namietať voči komore a spracúvaniu jej osobných údajov, ktoré:
   a) boli, sú alebo budú predmetom priameho marketingu bez jej súhlasu;
   b) ktorými sa zasahuje do jej práv a právom chránených záujmov a ktoré môžu byť takýmto spôsobom poškodené;
   c) by pre ňu malo právne účinky alebo významný dosah, ak sa takéto rozhodnutie vydá výlučne na základe úkonov automatizovaného spracúvania jej osobných údajov v informačnom systéme;
4. Dotknutá osoba má právo nesúhlasiť s rozhodnutím komory a odmietnuť prenos svojich osobných údajov do tretej krajiny, ktorá nezabezpečuje primeranú úroveň ochrany osobných údajov.
5. Požiadavky dotknutej osoby splní komora bezplatne v zákonnej lehote do 30 dní od ich prijatia.
6. V prípade, že nastane obmedzenie práv dotknutej osoby podľa § 28 ods. 2 Zákona, komora túto skutočnosť oznámi bez zbytočného odkladu dotknutej osobe a Úradu (napríklad ak dotknutá osoba žiadala o likvidáciu osobných údajov a nie je možné ju vykonať, lebo osobitný predpis nám nariaďuje archiváciu do 70. rokov fyzického veku osoby, alebo po dobu 20 rokov od skončenia pracovného pomeru a podobne).
7. Vedúci zamestnanec alebo oprávnená osoba, ktorej bola doručená písomná žiadosť dotknutej osoby (napr. žiadosť o odpis osobných údajov spracúvaných v informačnom systéme) ju postúpi zodpovednej osobe, ktorá vykoná jej prvotnú evidenciu a následne zabezpečí splnenie zákonnej lehoty na informovanie dotknutej osoby.
8. Zodpovedná osoba žiadosť prvotne vyhodnotí a zabezpečí jej pridelenie vecne kompetentnej oprávnenej osobe, ktorá v zmysle žiadosti pripraví návrh písomnej informácie pre dotknutú osobu (žiadateľa), zabezpečí preverenie a nápravu stavu, na ktorý si dotknutá osoba sťažuje a o vykonaných opatreniach informuje zodpovednú osobu a dotknutú osobu.
9. Agendu o písomnom vybavovaní žiadostí dotknutých osôb vedie poverená zodpovedná osoba. V prípade obmedzenia práv dotknutej osoby informuje Úrad na ochranu osobných údajov SR (napríklad nemožnosť likvidovať mzdové listy a pod.).

Čl.11 Bezpečnosť osobných údajov pri ich spracúvaní

1. Komora zodpovedá za bezpečnosť spracúvaných osobných údajov tým, že ich chráni pred náhodným ako aj nezákonným poškodením a zničením, náhodnou stratou, zmenou, nedovoleným prístupom a sprístupnením, ako aj pred akýmikoľvek inými neprípustnými formami spracúvania.
2. Komora zabezpečuje rovnakú úroveň bezpečnosti osobných údajov spracúvaných v listinnej forme, ako aj osobných údajov spracúvaných s využitím automatizovaných prostriedkov ich spracúvania (informačno-komunikačných technológií).
3. Základné zásady bezpečnosti pri práci s písomnosťami obsahujúcimi osobné údaje sú nasledovné:
   a) vytváranie, evidencia, ukladanie, obeh, prenos, archivácia, likvidácia, prípadne ďalšie činnosti s písomnosťami prebiehajú podľa platného Registratúrneho poriadku a registratúrneho plánu komory a schválených zásad tvorby a obehu písomností;
   b) písomnosti obsahujúce osobné údaje môžu byť uložené iba v priestoroch, ktoré sú primerane chránené pred prístupom alebo násilným vniknutím neoprávnenej osoby, pred ich zničením alebo poškodením ako následku vzniku mimoriadnej situácie. Ochrana priestoru sa zabezpečuje primeranými technickými, organizačnými a personálnymi opatreniami komory a ich vzájomnou kombináciou;
   c) vynášanie písomností obsahujúcich osobné údaje mimo priestorov komory podlieha schváleniu štatutárnym zástupcom komory, prípadne stanovisku poverenej zodpovednej osoby za komoru;
   d) pri prenose písomností v rámci priestorov komory, ako aj pri schválenom prenose písomností mimo priestorov komory je potrebné dbať na primeranú ochranu dôvernosti prenášaných písomností (uzavreté a nepriehľadné transportné obaly);
   e) prístup k písomnostiam obsahujúcim osobné údaje majú iba na to určení zamestnanci / členovia v postavení oprávnenej osoby,
   f) v prítomnosti neoprávnených osôb sa práca s písomnosťami obsahujúcimi osobné údaje zakazuje;
   g) vyhotovené písomnosti obsahujúce osobné údaje sú po ich vyradení z evidencií likvidované skartáciou, znemožňujúcou spätnú rekonštrukciu písomností.
4. Základné zásady bezpečnosti pri spracúvaní osobných údajov v elektronickej forme sú nasledovné:
   a) každý počítač musí byť vybavený aplikáciou na antivírusovú kontrolu, táto aplikácia musí byť pravidelne aktualizovaná;
   b) pri prístupe k počítaču je vždy vyžadovaná identifikácia a autentifikácia používateľa;
   c) fyzický prístup k počítaču a jeho vstupno-výstupným zariadeniam má iba určený zamestnanec, výpočtové zariadenia musia byť umiestnené v zamykaných priestoroch;
   d) používateľské a prístupové heslá musia byť zvolené tak, aby boli ťažko uhádnuteľné, musia byť pravidelne obmieňané a držané v tajnosti;
   e) prenosné médiá, ktoré obsahujú osobné údaje musia byť chránené pred stratou, poškodením a neoprávneným prístupom;
   f) v aplikáciách je používané riadenie prístupu, rozsah povoleného prístupu k osobným údajom je iba v miere nevyhnutnej na výkon pracovných činností používateľa;
   g) spracúvané osobné údaje musia byť pravidelne zálohované, zálohovanie je zabezpečované centrálnou správou alebo lokálnym zálohovaním, podľa podmienok, obsahu a rozsahu spracúvaných osobných údajov;

h) používateľ dodržiava stanovené pravidlá práce s počítačom, aplikáciou a počítačovou sieťou;
i) voľné vystavenie osobných údajov na webstránkach komory je považované za zverejnenie osobných údajov.

5. Každý zamestnanec komory pri podozrení z narušenia bezpečnosti osobných údajov spracúvaných v elektronickej forme, alebo pri podozrení z narušenia bezpečnosti zvereného počítača upovedomí o tejto skutočnosti bezodkladne najbližšieho nadriadeného a poverenú zodpovednú osobu za komoru.
6. Kontrolu zamestnancov pri dodržiavaní týchto pravidiel vykonáva ich priamy nadriadený a osoba poverená výkonom dohľadu nad ochranou osobných údajov za komoru. K záznamu o priebehu a výsledku kontroly dodržiavania stanovených zásad ochrany osobných údajov sa využíva na to určený formulár, ktorého vzor je prílohou č. 9 tejto smernice.
7. Kontrolu dodržiavania zavedených bezpečnostných mechanizmov pri práci s počítačom, s aplikáciami obsahujúcimi osobné údaje a počítačovou sieťou zabezpečuje poverený správca počítačovej siete.

Čl.12 Cezhraničný prenos osobných údajov

1. Pre každý účel spracúvania osobných údajov komorou musí byť formálne rozhodnuté, či je vykonávaný ich cezhraničný prenos.
2. Komora môže vykonávať prenos osobných údajov iba do krajín, ktoré zabezpečujú primeranú úroveň ochrany osobných údajov.
3. Komora nepoverí spracúvaním osobných údajov subjekt v cudzine.
4. Ochrana osobných údajov spracúvaných komorou, prenesených na územie Slovenskej republiky od subjektov so sídlom alebo s trvalým pobytom v cudzine, sa vykonáva v súlade so Zákonom a touto internou smernicou.
5. Komora zaručí bezpečnosť osobných údajov, ktoré odovzdáva na cezhraničné spracúvania aj pri ich tranzite.

Čl.13 Evidencia a registrácia IS

1. Povinnosť registrácie sa vzťahuje na všetky IS, v ktorých sa spracúvajú osobné údaje úplne alebo čiastočne automatizovanými prostriedkami spracúvania. Komora je povinná prihlásiť IS na registráciu pred začatím spracúvania osobných údajov. Spracúvanie osobných údajov nepodlieha povinnosti registrácie podľa Zákona, ak informačné systémy podliehajú dohľadu zodpovednej osoby na základe ustanovenia § 34 ods. 2, písm. b) Zákona.
2. O všetkých IS, v ktorých sú spracúvané osobné údaje, vedie komora evidenciu podľa ustanovení § 43 Zákona a to najneskôr odo dňa začatia spracúvania údajov.
3. Výnimkou z ustanovenia predchádzajúceho bodu sú IS, v ktorých spracúvané osobné údaje slúžia výlučne pre potreby poštového styku s dotknutými osobami a evidencie týchto údajov alebo obsahujú osobné údaje, ktoré sa spracúvajú výlučne na účely identifikácie osôb pri ich jednorazovom vstupe do priestorov prevádzkovateľa.
4. Evidenciu IS vypracúva a za jej aktualizáciu zodpovedá zodpovedná osoba poverená za komoru.
5. Aktuálna evidencia všetkých IS je uložená u zodpovednej osoby poverenej za komoru.
6. Podľa § 44 Zákona je evidencia verejná. Údaje z evidencie komora sprístupní bezplatne komukoľvek, kto o to požiada v zmysle zákona NR SR č.211/2000 Z.z. v znení neskorších predpisov, v spolupráci so zodpovednou osobou poverenou za komoru.

Čl.14 Technická bezpečnosť neautomatizovaných IS

1. Technická bezpečnosť neautomatizovaných IS (ďalej len „NIS“) je tvorená systémom manažérsko-technických a logistických opatrení zabezpečujúcich elimináciu a minimalizáciu hrozieb a rizík pôsobiacich na NIS pri spracúvaní osobných údajov.
2. Technická bezpečnosť NIS musí byť zameraná najmä na:
   a) riadenie ochrany osobných údajov v systéme celkovej bezpečnostnej politiky, hodnotenie a riadenie technických bezpečnostných rizík, interný a externý audit bezpečnosti;
   b) kontrolnú činnosť zameranú na aktuálnosť a dodržiavanie prijatých noriem, ktorými sa v komore vykonáva ochrana osobných údajov pri ich spracúvaní;
   c) správnosť a bezpečnosť pri používaní technických prostriedkov na realizáciu administratívnych činností, ktorými je kopírovanie a tlač písomností obsahujúcich osobné údaje, ich reprodukcia;
   d) správnosť postupov pri ničení vyradených písomností obsahujúcich osobné údaje na určených zariadeniach (skartačné zariadenia);
   e) účinnosť použitých mechanických zábranných prostriedkov na vytváranie dostatočných prekážok k zamedzeniu neoprávneného prístupu a násilného vniknutia do miest spracúvania a ukladania osobných údajov;
   f) splnenie požiadavky na ukladanie písomností a dátových nosičov v uzamykateľných uzáveroch za účelom zamedzenia prístupu neoprávnených osôb.
3. Pri ničení vyradených písomností a ich konceptov musia byť správne používané inštalované zariadenia na ich skartáciu, ktoré dostatočným spôsobom musia zamedziť rekonštrukcii skartovaných písomností.
4. Vo vyhodnotených miestach koncentrácie osobných údajov v pôsobnosti komory musí byť zaistené používanie základných mechanických zábranných prostriedkov a používanie primeraných zariadení na uzamykanie dokumentov obsahujúcich osobné údaje, ktoré sú použité primerane koncentrácii a rozsahu spracúvania osobných údajov od trezorov, cez plechové skrine až po uzamykateľné skrinky.
5. Kancelárske priestory sú v prípade neprítomnosti zamestnancov uzamykané.

Čl.15 Technická bezpečnosť automatizovaných IS

1. Všeobecné požiadavky na bezpečnosť počítačových systémov komory sú riešené v súlade s technickými bezpečnostnými opatreniami podľa odsekov 2.18 až 2.31 Európskeho štandardu pre hodnotenie bezpečnosti informačných systémov ITSEC zaradené do nasledujúcich skupín opatrení:
   a) Úlohy, funkcie a zodpovednosti osôb v IS;
   b) Identifikácia a autentifikácia;
   c) Riadenie prístupu;
   d) Účtovateľnosť;
   e) Opakované použitie;
   f) Výmena dát.

Čl.16 Úlohy, funkcie a zodpovednosti osôb v IS

1. Rozlišujeme nasledujúce funkcie osôb v IS:
   a) Oprávnení používatelia niektorého z počítačových informačných systémov – musia rozumieť základným pravidlám počítačovej bezpečnosti. Sú prvým stupňom ochrany a musia aktívne spolupracovať so správcom počítačovej siete pri tvorbe a aktualizácii bezpečnostných postupov a pravidiel.

b) Správcovia IS – zodpovedajú za každodennú, rutinnú implementáciu bezpečnostných pravidiel a štandardov. Spoločne so štatutárnym orgánom komory aktívne navrhujú najúčinnejšie bezpečnostné riešenia a striktne dodržiavajú odsúhlasené postupy a pravidlá. Sú povinní dokonale poznať systémy, ktoré spravujú.
c) Štatutárny orgán komory – rozhoduje o potrebe a obsahu informačných systémov, oprávňuje organizačné štruktúry a jednotlivcov k prístupu do informačných systémov. Rozhoduje o investíciách do bezpečnosti a posudzuje strategické bezpečnostné zámery.
d) Správca počítačovej siete plní funkciu bezpečnostného správcu aj administrátora informačného systému a je zodpovedný za:
   - konfiguráciu operačného systému a zálohovanie centrálnych systémov;
   - správu prístupových práv (zakladanie, zmeny a rušenie užívateľov);
   - nastavenie bezpečnostnej politiky na pracovných staniciach;
   - udržiavanie predpísaného programového vybavenia jednotlivých staníc;
   - pridávanie (registráciu) sieťových objektov v doméne.

2. Každý zamestnanec a člen volených orgánov komory je náležite poučený a má počas trvania pracovnoprávneho resp. funkčného obdobia nasledovné povinnosti:
   a) dodržiavať bezpečnostnú politiku IS komory a vnútorné predpisy komory;
   b) dodržiavať pokyny a usmernenia štatutárneho orgánu komory, bezpečnostného správcu IS a zodpovednej osoby poverenej výkonom dohľadu nad ochranou osobných údajov;
   c) dodržiavať pravidlá ochrany údajov a služieb IS pred stratou, poškodením alebo neoprávneným prístupom;
   d) využívať služby IS v súlade so svojim pracovným zaradením / svojou funkciou a podľa pokynov štatutárneho orgánu komory;
   e) dodržiavať povinnosť mlčanlivosti o skutočnostiach dôvernej povahy, s ktorými sa oboznámil, a to aj po ukončení pracovnoprávneho alebo obdobného vzťahu / funkčného obdobia v komore.
3. Správca počítačovej siete v úlohe bezpečnostného správcu IS zaisťuje odborné úlohy a riadenie informačnej bezpečnosti. Jeho povinnosťami sú hlavne:
   a) pripravovať hodnotenie stavu informačnej bezpečnosti;
   b) pôsobiť v oblasti operatívneho riadenia informačnej bezpečnosti, napríklad v nevyhnutných prípadoch povoľovať výnimky z bezpečnostnej politiky a bezpečnostných smerníc;
   c) podieľať sa na hodnotení nových produktov a systémov z hľadiska informačnej bezpečnosti,
   d) sústreďovať informácie, evidovať a vyhodnocovať riešenie bezpečnostných incidentov a bezpečnostných nedostatkov,
   e) riadiť a vykonávať vyšetrovanie bezpečnostných incidentov a nadväzujúce činnosti, navrhovať a prijímať bezpečnostné opatrenia v oblasti informačnej bezpečnosti,
   f) kontrolovať dodržovanie tejto internej smernice, vykonávať kontroly prijatých bezpečnostných opatrení vrátane kontrol na pracoviskách jednotlivých užívateľov,
   g) spolupracovať pri vykonávaní externého prípadne interného bezpečnostného auditu,
   h) spolupracovať s externými špecialistami na informačnú bezpečnosť.
4. Za správu infraštruktúry IT zodpovedá správca počítačovej siete, ktorý vedie dokumentáciu o nastaveniach parametrov systému. Táto dokumentácia obsahuje najmä:
   a) konfiguráciu serverov,
   b) konfiguráciu pracovných staníc (typové nastavenie),
   c) zoznam aktívnych a pasívnych prvkov siete,
   d) konfiguráciu aktívnych prvkov (router, firewall),
   e) schémy zapojenia.

5. Vytváranie, rušenie a zmenu užívateľských účtov rieši správca počítačovej siete, ktorý tieto požiadavky vykonáva výhradne na základe písomných požiadaviek predsedu komory (okrem generovania nového hesla, kedy sa súhlas predsedu komory nevyžaduje). Správca počítačovej siete je povinný uvedené písomné požiadavky evidovať.

Čl.17 Identifikácia a autentifikácia

1. Identifikácia a autentizácia zahŕňa jednoznačné zistenie identity užívateľa a overenie, že identita užívateľa je správna. Identifikácia a autentizácia pokrýva všetky funkcie, ktoré súvisia so správou užívateľov, t.j. ich pridávanie, rušenie a úprava užívateľov.
2. Systém jednoznačne identifikuje a autentizuje oprávnených užívateľov. Táto identifikácia a autentizácia predchádza všetkým interakciám medzi systémom a užívateľom. Iné aktivity sú možné len po úspešnej identifikácii a autentizácii. Pri identifikácii a autentizácii musí užívateľ zadať svoju jednoznačnú užívateľskú identifikáciu a dodatočnú autentizačnú informáciu, v tomto prípade heslo.
3. Všetky informačné systémy komory musia byť konfigurované tak, aby sa ľubovoľné operácie s klasifikovanými údajmi dali priradiť jednoznačne unikátnej osobe.
4. Základnou požiadavkou na každého používateľa je zákaz poskytovať dôvernú znalosť k účtu (heslo) ľubovoľnej inej osobe alebo funkcii v informačnom systéme. Všetky heslá sú definované ako citlivé a dôverné informácie.
5. Zoznam zakázaných činností:
   - Neposkytni nikomu heslo cez telefón.
   - Neposkytni heslo prostredníctvom email-ovej správy.
   - Neposkytni heslo nadriadenému.
   - Nehovor o hesle pred niekým iným.
   - Neposkytuj heslo na dotazníkoch, alebo bezpečnostných formulároch.
   - Neposkytni heslo rodinným príslušníkom.
   - Neposkytni heslo spolupracovníkom ani počas neprítomnosti.
   - Nepoužívaj „Zapamätať heslo“ do aplikácií.
   - Nezapisujte svoje heslá nikam a neskladujte ich niekde vo vašej kancelárii. Neskladujte heslá v súboroch na nejakom počítačovom systéme (vrátane pocked PC alebo podobných zariadeniach) bez zakódovania, alebo šifrovania.
6. Ak má používateľ podozrenie, že jeho účet, alebo heslo bolo kompromitované, oznámi toto podozrenie správcovi počítačovej siete a zmení všetky prístupové heslá.
7. Každý používateľ nesie zodpovednosť za svoje autentifikačné údaje a tým aj za činnosť vykonanú pod jemu prideleným účtom.
8. Systém po každom používateľovi požaduje, aby mu oznámil svoju identitu a túto identitu rovnako preukázal, t.j. aby sa autentizoval. Pre oznámenie identity používateľ používa meno používateľa, ktoré zavádza správca. Pre preukázanie identity (autentizáciu) používateľ používa heslo. Prvotné heslo stanovuje správca počítačovej siete, ktoré používateľ po prvom prihlásení musí zmeniť.
9. Heslo si oprávnený používateľ stanovuje sám. Všetky heslá užívateľskej úrovne (email, web, desktop, atď. – zavedené v Active directory, alebo doméne) musia byť zmenené minimálne jeden krát za 90 dní. Odporúčaný interval je však 60 dní. Silné heslá majú nasledovné charakteristiky:
   - Musia obsahovať malé aj veľké písmeno (a-z, A-Z)
   - Musia obsahovať číslicu alebo nealfanumerické znaky (0-9, !@#$%^&*()_+|~-=\‘{}[]:";’<>?,./)
   - Musia byť minimálne 8 znakov dlhé

- Nesmú byť slovom zo slovníku ani inej reči, slangu, dialektu, žargónu a pod.
- Nesmú byť založené na osobných informáciách, mien členov rodiny a pod.
- Heslo by nemalo byť nikdy napísané ani inak zaznamenané. Snažte sa tvoriť heslá, ktoré sú ľahko zapamätateľné avšak ťažko uhádnuteľné.
- Heslo nesmie byť počas zadávania nikdy užívateľovi zobrazované.

10. Uvedený spôsob identifikácie a autentizácie platí pre všetky pracovné stanice v pôsobnosti komory.
11. Pre identifikáciu a autentizáciu na úrovni OS servera sú využité prostriedky konkrétneho operačného systému. Vo všetkých lokálnych sieťach je vyžadované povinné zadávanie hesla pre všetkých užívateľov. Pre všetky servery v pôsobnosti a správe komory platia rovnaké požiadavky na silu a bezpečnosť, popísaní v bode 9 tohto článku.
12. Po identifikácii a autentizácii užívateľov do siete je používateľ povinný sa identifikovať a autentizovať aj do aplikácie, ak to táto umožňuje.

Čl.18 Riadenie prístupu

1. V pôsobnosti komory je realizované riadenie prístupu k jednotlivým objektom v súlade s bezpečnostnými štandardami a odporučeniami. Pokrýva všetky funkcie, ktoré riadia tok informácií a použitia zdrojov medzi oprávnenými používateľmi, procesmi a objektmi. Správa (t.j. udeľovanie a odvolávanie) prístupových práv a ich verifikácia je realizovaná aj na úrovni aplikácie, aj na úrovni jednotlivých modulov.
2. Systém zaisťuje, že oprávnení používatelia a procesy, bežiace pod ich menom, nemôžu získať prístup k dátam alebo prostriedkom, pre ktorý nie sú autorizované. Systém je schopný prideľovať prístupové práva až na úrovni jednotlivých oprávnených používateľov. Identifikácia a autentizácia predchádza akejkoľvek interakcii medzi systémom a oprávneným používateľom.

Čl.19 Účtovateľnosť / Záznam o aktivitách užívateľov

1. Účtovateľnosť a audit na úrovni serverov je riešený štandardnými prostriedkami použitého operačného systému.
2. Účtovateľnosť a audit na úrovni pracovnej stanice je riešený štandardnými prostriedkami operačného systému Windows.
3. Základom riešenia účtovateľnosti na úrovni aplikácie je protokolovanie všetkých, z hľadiska bezpečnosti podstatných udalostí. Základom auditu na úrovni aplikácie je funkcia preverujúca stav informačného systému a databáz.

Čl.20 Opakované použitie

1. Komora zabezpečuje opakované použitie zdrojov, ako sú operačná pamäť, oblasti diskovej pamäti, monitory pracovných staníc a pod., pričom zachováva požadovanú úroveň bezpečnosti prostriedkami prideľovanými pri činnosti IS jednotlivým oprávneným používateľom, ktoré neobsahujú žiadne informácie ich predchádzajúceho vlastníka.
2. Pre implementáciu bezpečnostných funkcií riadenia opakovaného použitia na úrovni systémových zdrojov (operačná pamäť, disková pamäť) sa využívajú štandardné funkcie použitého operačného systému.
3. Na úrovni aplikácie je treba zaistiť riadenie opakovaného použitia pre displeje pracovných staníc. Na úrovni aplikácie je treba konkrétne použiť šetrič obrazovky a autentizované zamykanie klávesnice heslom. Pre implementáciu šetriča obrazovky a autentizovaného zamykania klávesnice heslom sú použité štandardné prostriedky operačného systému Windows 10 na pracovných staniciach.

Čl.21 Manipulácia s médiami

1. Medzi médiá používané komorou patria všetky papierové médiá, ako tlačové výstupy, písomné dokumenty a rôzne koncepty, elektronické média ako USB kľúče, externé disky a ďalšie médiá slúžiace na zaznamenávanie a zálohovanie dát. Všetky typy týchto médií je potrebné chrániť rovnako dôsledne ako dáta v automatizovanom informačnom systéme.
2. Elektronické médiá, ktoré obsahujú osobné údaje musia byť označené evidenčným číslom a zaevidované, každé také médium musí byť pridelené konkrétnej oprávnenej osobe, ktorá za manipuláciu s ním a jeho bezpečné uloženie zodpovedá.
3. Pokiaľ majú byť elektronické médiá pre záznam dát distribuované mimo sídlo komory, musí sa použiť vždy nové médium a na sprievodnom spise musí byť vyznačené evidenčné číslo média.
4. V prípade odovzdávania médií musí byť súčasťou odovzdania odovzdávací protokol s potvrdením preberajúcej osoby, podateľne alebo doklad o postúpení využitého transportného média iným bezpečným spôsobom (doporučenou poštovou zásielkou, kuriérom a pod.).

Čl.22 Používanie elektronickej pošty

1. Pre všetkých oprávnených používateľov, ktorí používajú elektronickú poštu komory a pre oprávnené osoby, ktoré prenášajú osobné údaje prostredníctvom elektronickej pošty, platia tieto zásady:
   a) užívatelia zodpovedajú za používanie pridelených schránok elektronickej pošty;
   b) schránku iného užívateľa je možné používať výhradne s jeho súhlasom;
   c) prostredníctvom elektronickej pošty je zakázané prenášať osobné údaje mimo sídla komory, ktoré nie sú chránené heslom alebo iným primeraným spôsobom (šifrovanie);
   d) elektronickú poštu používať obozretne, aby neboli ohrozené prenášané informácie, ak je nutné prenášať citlivé informácie použije sa šifrovanie alebo kompresia chránená heslom s požadovanou silou;
   e) elektronická pošta je určená k pracovným účelom, používať elektronickú poštu pre mimopracovné aktivity možno iba pri zachovaní stanovených pravidiel.

Čl.23 Používanie ďalších komunikačných kanálov

1. Medzi ďalšie komunikačné kanály komory patria predovšetkým:
   a) listové zásielky,
   b) mobilný telefón,
   c) osobný styk.
2. Pre zasielanie osobných údajov formou listovej zásielky sa môže používať:
   a) doporučená listová zásielka,
   b) dôveryhodná kuriérska služba.
3. Odovzdávanie osobných údajov mobilným telefónom sa ako významné riziko zakazuje.
4. Ukladanie osobných údajov v záznamníkoch a hlasových schránkach je ako významné riziko zakázané.
5. Pri osobnom styku je rozhovor o osobných údajoch dotknutých osôb možný len v prípade, že tento nemôže vypočuť nepovolaná osoba. Je zakázané hovoriť o osobných údajoch v dopravných prostriedkoch, vo verejných miestnostiach, na pracoviskách komory a sprostredkovateľov, pokiaľ ich okná sú orientované do verejne prístupných miest a v čase rozhovoru sa využívajú na vetranie a podobne.

Čl.24 Používanie internetu

1. Pre všetkých oprávnených používateľov, ktorí majú prístup k internetu platia tieto zásady:
   a) pripojenie je možné realizovať len prostredníctvom určeného kanálu;
   b) je zakázané kopírovať a spúšťať programy a iné potenciálne nebezpečné dáta;
   c) je zakázané navštevovať stránky s obsahom, ktorý nesúvisí s ich pracovnou činnosťou;
   d) prostredníctvom internetu je zakázané šíriť osobné údaje;
   e) výmena súborov s osobnými údajmi prostredníctvom voľne prístupných adresárov alebo archívov je zakázaná.

Čl.25 Používanie mobilných počítačov a práca doma

1. Osobné údaje a prevádzkové informácie je možné spracovávať na mobilných počítačoch mimo pracovisko za týchto podmienok:
   a) môžu sa používať iba autorizované mobilné počítače komory, ktoré sú primeraným spôsobom chránené pred prístupom neoprávnenej osoby,
   b) užívatelia sú poučení o rizikách používania mobilných počítačov zodpovednou osobou,
   c) na mobilnom počítači je nainštalovaný aktuálny antivírový program,
   d) pravidelne je vykonávané zálohovanie dát uložených na mobilnom počítači.
2. Práca na domácich a iných počítačoch nepatriacich do správy komory je zakázaná.

Čl.26 Vzdialený prístup

1. Vzdialený prístup k technickým zariadeniam komory je možný výhradne po schválení štatutárnym orgánom a môže ho vytvoriť výhradne správca počítačovej siete za nasledovných podmienok:
   a) Dátové spojenie je počas celej relácie šifrované minimálne prostredníctvom algoritmu AES, s použitím 256 bitového kľúča, negociovaného pomocou algoritmu RSA.
   b) Integrita a dôveryhodnosť prípadnej špecializovanej aplikácie spustenej na počítači musí byť zabezpečená elektronickým podpisom overenej certifikačnej autority.

Čl.27 Ochrana počítača počas neprítomnosti užívateľa

1. Oprávnený používateľ je povinný primerane chrániť pridelené automatizované prostriedky na spracúvanie osobných údajov pred neoprávnenou manipuláciou s nimi v čase jeho neprítomnosti.
2. Predtým, ako oprávnený používateľ opustí pracovisko, je povinný:
   a) ak odchádza na dlhší čas - vypnúť počítač (pracovnú stanicu),
   b) ak odchádza na kratšiu dobu - odhlásiť sa, alebo zamknúť pracovnú stanicu.

Čl.28 Antivírová ochrana

1. V súčasnosti využíva komora antivírovú ochranu postavenú na produktoch ESET Smart Security od spoločnosti ESET, spol. s r.o. s automatickým update, ktoré poskytuje pracovným staniciam s OS WINDOWS pokročilú ochranu pred všetkými typmi škodlivých kódov, identifikuje, hlási, čistí, odstraňuje a bráni známym i neznámym škodlivým kódom i nežiaducim aplikáciám infikovať počítače a servery v sieti.
2. Pravidelný automatizovaný upgrade vírusovej databázy zabezpečuje dostatočnú ochranu klientov proti vírusom.
3. Požiadavky na antivírusový systém:
   a) musí byť nainštalovaný na všetkých pracovných staniciach, serveroch a prenosných počítačoch,

b) musí byť nainštalovaná jeho aktuálna verzia,
c) musí umožňovať nepretržitú kontrolu kritických častí disku, súborov a správ elektronickej pošty na pozadí,
d) musí umožňovať periodické vykonanie antivírovej kontroly celého systému,
e) musí umožňovať užívateľom antivírovú kontrolu zvolených médií, adresárov a súborov.

4. Za inštaláciu, aktualizáciu a aktiváciu antivírusového systému zodpovedá správca počítačovej siete. Pri práci s prijatými správami elektronickej pošty sú aplikované nasledovné pravidlá pre používateľov (vo väčšine prípadov sú uvedené pravidlá už aplikované priamo na filtroch k elektronickej pošte):
   - Zákaz otvárať prílohy správ, ktoré pochádzajú z neznámych alebo podozrivých adries v internete.
   - Zákaz otvárať spustiteľné súbory (obsahujú koncovky .exe, .com. .bat, .vbs, .scr). Správy, ktoré obsahujú takéto súbory okamžite zmažte. Informujte odosielateľa a informujte zodpovednú osobu.
   - V žiadnom prípade nevykonávajte sami odstraňovanie počítačových vírusov. V prípade zistenia vírusu prostredníctvom antivírusového program, alebo ak sami máte podozrenie na prítomnosť vírusu okamžite to oznámte zodpovednej osobe.
5. Oprávnení používatelia majú zakázané vypínať antivírusovú ochranu. V prípade výskytu a detekcie počítačového vírusu sú povinní informovať zodpovednú osobu, ktorá rozhodne o ďalšom postupe.

Čl.29 Riešenie bezpečnostných incidentov

1. Zamestnanci / členovia volených orgánov komory, ktorí zistia bezpečnostný incident alebo bezpečnostný nedostatok okamžite toto oznámia zodpovednej osobe. V prípade závažného bezpečnostného incidentu okamžite kontaktujú štatutárneho zástupcu komory, ktorý informuje správcu IS.
2. Po oznámení sa spracuje Záznam o bezpečnostnom incidente v IS podľa vzoru v prílohe č.10 tejto smernice (Príloha č. 10 Záznam o bezpečnostnom incidente v informačnom systéme). Vyhodnotenie vykoná správca počítačovej siete alebo poverená zodpovedná osoba na základe údajov z vyplneného formulára, prípadne poskytnutých doplňujúcich informácií.
3. V prípade havarijného stavu, ohrozenia a pod. prechádza činnosť IS do núdzového režimu. V tomto režime sú jednotlivé funkcie oprávnených používateľov obmedzené. Úlohou IS je zabezpečiť ochranu osobných údajov. Činnosť IS v tomto režime zabezpečuje správca počítačovej siete, ktorý:
   - zabezpečí znemožnenie prístupu všetkých používateľov k prostriedkom IS,
   - je zodpovedný za núdzovú prevádzku,
   - v prípade zničenia systému je zodpovedný za obnovenie najnovšej zálohy,
   - zabezpečí odstránenie príčiny havárie alebo ohrozenia,
   - po ukončení havarijného stavu povolí prístup oprávnených používateľov k prostriedkom IS.

Čl.30 Archivácia, zálohovanie a obnova

1. Archiváciou a zálohovaním rozumieme uloženie všetkých, alebo vybraných dát na pevný disk, alebo iné pamäťové médium.
2. Záloha je v pôsobnosti komory riešená len prostredníctvom oprávnených osôb na USB pamäťové médiá a sieťové disky. Uvedené zálohy sa ukladajú na bezpečnom mieste s riadeným prístupom.

3. Záloha web a mail serverov je vykonávaná prostredníctvom sprostredkovateľa, ktorý má priamo v zmluve bezpečnosť uvedených serverov.
4. Obnovou rozumieme obnovenie všetkých, alebo vybraných dát po bezpečnostnom incidente, alebo po inej strate dát z bezpečnostnej zálohy. Obnova je riešená prostredníctvom obnovy z vytvorených záloh.

Čl.31 Spôsob, forma a periodicita výkonu kontrolných činností

1. Medzi priebežné kontrolné činnosti, vykonávané oprávnenými osobami patria:
   a) kontrola zabezpečenia písomného súhlasu so spracúvaním osobných údajov od dotknutých osôb na začiatku spracúvania agendy;
   b) kontrola dodržiavania politiky čistého stola, t.j. uloženie dokumentov s obsahom osobných údajov do určených uzamykateľných úschovných objektov;
   c) kontrola, či sú vypnuté elektrické spotrebiče a ďalšie zariadenia, ktoré by mohli spôsobiť poškodenie alebo zničenie kancelárskych priestorov kde sú spracúvané osobné údaje;
   d) kontrola úplnosti spracúvaných osobných údajov a kontrola úplnosti a správnosti spracovania osobných údajov.
2. Medzi priebežné kontrolné činnosti, vykonávané zodpovednou osobou patria:
   a) kontrola dodržiavania zmluvných ustanovení pri výkone činností zamestnancov dodávateľa informačného systému (napr. pri legislatívnych zmenách, vylepšeniach systému a pod.);
   b) kontrola uzatvorenia dohody o mlčanlivosti pri výkone činností v informačnom systéme;
   c) kontrola dodržiavania procesu prideľovania prístupových práv a kontrola úrovne prístupových práv oprávnených osôb v informačnom systéme.
3. Medzi priebežné kontrolné činnosti, vykonávané správcom počítačovej siete, patria:
   a) kontrola vykonaných záznamov (logov) operačného systému a ostatného softwaru (SW) na pracovných staniciach oprávnených osôb;
   b) kontrola dodržiavania informačnej bezpečnosti.
4. Medzi periodické kontroly, vykonávané zodpovednou osobou patria:
   a) kontrola dodržiavania ustanovení tejto internej smernice vykonávaná minimálne 2x ročne;
   b) kontrola súladu spracúvania osobných údajov s ustanoveniami legislatívy SR vykonávaná minimálne raz ročne;
   c) kontrola pridelených prístupov oprávnených osôb do systému Synology.
5. Medzi periodické kontroly, vykonávané správcom počítačovej siete, patrí kontrola úspešnosti aktualizácie pracovných staníc (aplikácie záplat operačných systémov a nainštalovaného aplikačného programového vybavenia).
6. Medzi náhodné kontroly, vykonávané zodpovednou osobou patria:
   a) kontrola dodržiavania požiadavky dohľadu pri výkone servisných a/alebo iných činností – vykonávaná v prípade upratovania priestorov spracúvania osobných údajov;
   b) kontrola dodržiavania požiadavky na likvidáciu poškodených, neúplných a ďalej nepotrebných osobných údajov, ako aj nevyžiadaných dokumentov žiadateľov o zamestnanie na skartovacích zariadeniach.
7. Medzi náhodné kontroly, vykonávané správcom počítačovej siete, patrí kontrola dodržiavania zákazu neautorizovanej zmeny HW a SW konfigurácie.
8. Medzi kontrolné mechanizmy patria aj následné kontroly, vykonávané spravidla zodpovednou osobou za účelom overenia stavu odstránenia nedostatkov zistených pri výkone niektorej z predchádzajúcich typov kontrol.
9. O vykonaní kontroly v oblasti osobných údajov je vedený písomný záznam minimálne v nasledujúcom rozsahu:

a) dátum kontroly;
b) predmet kontroly, t.j. kontrolovaná oblasť resp. ciele kontroly;
c) kto kontrolu vykonal;
d) zistený stav;
e) vyjadrenie kontrolovaného;
f) úlohy na odstránenie zistených nedostatkov;
g) záznam o odstránení zistených nedostatkov.

Čl.32 Postupy pri haváriách, poruchách a iných mimoriadnych situáciách

1. Za účelom minimalizácie rizika výskytu a potenciálnych dopadov pri výskyte havárií, porúch a iných mimoriadnych udalostí, sú v organizácii zavedené nasledujúce preventívne opatrenia:
   a) na bezpečné uchovávanie osobných údajov v papierovej forme sú určené uzamykateľné úschovné objekty (skrinky), kde sú po ukončení práce a pri opustení pracoviska uchovávané spracúvané osobné údaje;
   b) pri opustení pracoviska je oprávnená osoba povinná vykonať kontrolu, či sú vypnuté elektrické a ďalšie zariadenia, ktoré by mohli spôsobiť poškodenie alebo zničenie priestorov organizácie, ako aj v nich uchovávaných osobných údajov;
   c) oprávnené osoby sú pri opustení pracoviska povinné zatvoriť a uzamknúť úschovný objekt a pri odchode bezpečne uzatvoriť pracovisko;
   d) výkon servisných zásahov a zmien v hardvérovej a softvérovej konfigurácii technických prostriedkov (pracovných staníc a komponentov zostavy, ako napr. lokálna tlačiareň) sú vykonávané len autorizovaným odborným personálom; pričom neautorizované zmeny hardvéru a softvéru (napr. inštalácia SW, pripájanie externých zariadení) sú zakázané;
   e) na zabezpečenie dostupnosti osobných údajov v elektronickej forme pre prípad obnovy je vykonávané ich zálohovanie.
2. V prípade havárie alebo poruchy pracovnej stanice oprávneného používateľa je v závislosti od jej rozsahu vykonaný servisný zásah, pričom chybný komponent je nahradený a systém je reinštalovaný, resp. je zabezpečená náhradná pracovná stanica.
3. V prípade havárie alebo poruchy niektorého z kľúčových komponentov IT infraštruktúry (napr. databázový server) je v závislosti od jej rozsahu vykonaný odborný servisný zásah, pričom chybný komponent je nahradený a systém reinštalovaný, prípadne je zabezpečený náhradný technický prostriedok s následnou obnovou osobných údajov z vykonaných záloh, pričom tieto aktivity sú vykonávané v rámci plnenia servisných alebo iných zmluvných vzťahov medzi komorou a dodávateľom služieb.
4. V prípade výskytu havárie infraštruktúry budovy (napr. prerušenie vodovodu alebo ústredného kúrenia s následným zatopením priestorov), v závislosti od jej rozsahu, zabezpečí zodpovedná osoba a/alebo oprávnené osoby prítomné na pracovisku prenesenie osobných údajov z postihnutých priestorov mimo dosah havárie, pričom musí byť zabezpečená ich primeraná ochrana (napr. formou dohľadu oprávnenou osobou).
5. V prípade havárie väčšieho rozsahu a výskytu mimoriadnej situácie (napr. požiaru budovy), zodpovedná osoba alebo oprávnené osoby prítomné na pracovisku v závislosti od rozsahu udalosti a v prípade, že nie sú ohrozené ľudské životy, zabezpečia prenesenie spracúvaných osobných údajov z postihnutých priestorov mimo dosah havárie, pričom musí byť zaistená ich primeraná ochrana. Tiež je potrebné zabezpečiť ochranu osobných údajov v prípade zásahu pri výkone záchranných prác.
6. Pre prípad úplného zničenia kancelárie, musia byť záložné dáta uložené aj mimo priestorov kancelárie.

Čl.33 Spolupráca s Úradom na ochranu osobných údajov SR

1. Úrad môže v komore vykonávať kontrolu spracúvania osobných údajov v IS. Priebeh kontrolnej činnosti je stanovený Zákonom.
2. Pri výkone kontroly súčinnosť s Úradom zabezpečuje predseda komory v súčinnosti so zodpovednou osobou, ak boli splnené podmienky na jej poverenie v zmysle Zákona.
3. Osoby uvedené v predchádzajúcom bode majú byť oboznámené s protokolom o vykonaní kontroly a túto skutočnosť potvrdia podpisom protokolu.
4. Účastníkom konania za komoru je štatutárny zástupca komory, alebo ním písomne poverená osoba.
5. Počas výkonu kontroly alebo počas konania Úradu poskytujú zamestnanci komory Úradu a ním povereným kontrolným osobám potrebnú súčinnosť, najmä vstup do priestorov, prístup k materiálom, údajom a prístup do prevádzkovaných IS.
6. Zodpovedná osoba za komoru vedie evidenciu všetkej korešpondencie komory s Úradom.

Čl. 34 Záverečné ustanovenia

1. Táto smernica podlieha aktualizácii podľa potrieb komory a na základe prípadných zmien Zákona a znenia štatútu komory.
2. Ustanoveniami tejto smernice sú povinní sa riadiť všetci členovia a zamestnanci komory, ktorí sa v rámci pracovného zaradenia alebo svojej funkcie zoznamujú s osobnými údajmi spracúvanými v IS, na túto prácu boli náležite určení, boli poučení o právach a povinnostiach ustanovených Zákonom a o zodpovednosti za ich porušenie.
3. Táto smernica je v nevyhnutom rozsahu záväzná pre zmluvných dodávateľov a tretie strany.
4. Výnimky z povinností vyplývajúcich z tejto Smernice môže udeľovať štatutárny zástupca komory alebo ním písomne poverená osoba. Výnimka musí byť v súlade so Zákonom, udelená písomne a musí byť daná na vedomie poverenej zodpovednej osobe za komoru.
5. Dopĺňanie a prípadné zmeny uvedených ustanovení smernice vykonáva predstavenstvo komory.
6. Všetci zamestnanci a členovia komory sú povinní sa s touto smernicou oboznámiť do 10 dní po jej schválení predstavenstvom komory. Za preukázateľné oboznámenie zamestnancov a členov komory so smernicou zodpovedá tajomník komory.
7. Táto interná smernica nadobúda účinnosť dňom jej schválenia predstavenstvom komory, po jej podpise predsedom komory.

V Bratislave, dňa 6.9.2016

Mgr. Peter Kulifaj
Predseda Slovenskej komory SP a ASP

Špecifikácia príloh

Príloha č. 1 Evidencia informačného systému osobných údajov
Príloha č. 2 Poverenie zodpovednej osoby
Príloha č. 3 Poverenie na získavanie osobných údajov
Príloha č. 4 Záznam o poučení oprávnenej osoby
Príloha č. 5 Určenie oprávnených osôb s prístupom k osobným údajom
Príloha č. 6 Záznam o poučení inej fyzickej osoby
Príloha č. 7 Súhlas dotknutej osoby so spracúvaním osobných údajov
Príloha č. 8 Informácia dotknutej osobe o účele a podmienkach spracúvania osobných údajov
Príloha č. 9 Záznam o vykonanej kontrole v informačnom systéme
Príloha č. 10 Záznam o bezpečnostnom incidente v informačnom systéme

Príloha č. 1

EVIDENCIA INFORMAČNÉHO SYSTÉMU OSOBNÝCH ÚDAJOV

podľa § 43 ods. 1 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

I. NÁZOV INFORMAČNÉHO SYSTÉMU OSOBNÝCH ÚDAJOV

II. ÚDAJE O PREVÁDZKOVATEĽOVI

Názov prevádzkovateľa	
Identifikačné číslo organizácie (IČO)	
Adresa prevádzkovateľa (ulica a číslo, obec, PSČ, štát)	
Právna forma	
Štatutárny orgán prevádzkovateľa (príp. osoba oprávnená konať v jeho mene)	
Zástupca prevádzkovateľa	
Počet oprávnených osôb	

III. ÚDAJE O INFORMAČNOM SYSTÉME OSOBNÝCH ÚDAJOV

Účel spracúvania osobných údajov	
Právny základ spracúvania osobných údajov	
Okruh dotknutých osôb	
Zoznam osobných údajov (alebo rozsah)	
Označenie bezpečnostných opatrení	

IV. SPRACOVATEĽSKÉ OPERÁCIE S OSOBNÝMI ÚDAJMI

Poskytovanie osobných údajov	
Tretie strany (prípadne okruh tretích strán) / Právny základ	
Sprístupňovanie osobných údajov	
Okruh príjemcov / Právny základ	
Zverejňovanie osobných údajov	
Spôsob zverejnenia / Právny základ	
Cezhraničný prenos osobných údajov	
Tretia krajina / Právny základ	

V. ZAČIATOK SPRACÚVANIA OSOBNÝCH ÚDAJOV

Mesto, dátum .....

Meno a podpis štatutárneho orgánu prevádzkovateľa

Príloha č. 2

POVERENIE ZODPOVEDNEJ OSOBY

Organizácia ***názov organizácie,*** so sídlom ***adresa sídla organizácie/ ulica číslo, PSČ, mesto***, IČO: ***IČO organizácie***, ako prevádzkovateľ informačných systémov, v ktorých sa spracúvajú osobné údaje dotknutých osôb, zastúpená štatutárnym zástupcom organizácie ***titul, meno, priezvisko štatutárneho zástupcu,*** narodeným ***dátum narodenia štatutárneho zástupcu***, týmto poveruje:

Meno a priezvisko: ***titul, meno, priezvisko poverenej osoby***
Pracovné zaradenie: ***pracovné zaradenie poverenej osoby***
(ďalej len „zodpovedná osoba“)

výkonom dohľadu nad dodržiavaním zákonných ustanovení pri spracúvaní osobných údajov v informačných systémoch ***názov organizácie***.
Poverenie sa vydáva na základe § 23 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „Zákon“).

Zodpovedná osoba spĺňa predpoklady na výkon funkcie stanovených v § 23 ods. 5 až 9 Zákona:
- odovzdala výpis z registra trestov
- absolvovala skúšku na výkon funkcie zodpovednej osoby podľa § 24 Zákona (potvrdenie o absolvovaní skúšky č. ***xxxx/20xx zo dňa DD.MM.RRRR***)
- pre plnenie úloh má v informačných systémoch postavenie oprávnenej osoby.

Súčasťou tohto poverenia je aj záznam o poučení oprávnenej osoby podľa § 21 ods. 3 Zákona.

Zodpovedná osoba je pri výkone poverenia povinná postupovať najmä v zmysle § 27 Zákona.
Pri výkone tohto poverenia zodpovedná osoba spolupracuje s vedúcimi zamestnancami prevádzkovateľa.

Poverenie sa vydáva s účinnosťou odo dňa jeho vydania na neurčitý čas a môže byť ukončené v súlade s § 26 Zákona.

V ***Meste***, dňa ***DD. mesiac RRRR***

Podpis predsedu a odtlačok pečiatky organizácie
_____
Titul, Meno PRIEZVISKO
Predseda Slovenskej komory SP a ASP

S poverením vyjadrujem súhlas a poverenie prijímam v plnom rozsahu.

V ***Meste***, dňa ***DD. mesiac RRRR***

Podpis poverenej osoby
_____
Titul, Meno PRIEZVISKO poverenej osoby

Príloha č. 3

POVERENIE NA ZÍSKAVANIE OSOBNÝCH ÚDAJOV

Organizácia ***názov organizácie,*** so sídlom ***adresa sídla organizácie/ ulica číslo, PSČ, mesto***, IČO: ***IČO organizácie***, ako prevádzkovateľ informačných systémov, v ktorých sa spracúvajú osobné údaje dotknutých osôb, zastúpená štatutárnym zástupcom organizácie ***titul, meno, priezvisko štatutárneho zástupcu,*** narodeným ***dátum narodenia štatutárneho zástupcu***, týmto poveruje:

Meno a priezvisko: ***titul, meno, priezvisko poverenej osoby***
Pracovné zaradenie: ***pracovné zaradenie / výkon funkcie poverenej osoby***
(ďalej len „oprávnená osoba“)

na činnosti súvisiace so získavaním osobných údajov podľa § 15 zákona č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len Zákon) od ***špecifikácia cieľovej skupiny*** pri výkone práce ***špecifikácia činnosti spojenej so spracúvaním osobných údajov oprávnenou osobou***.

Toto oprávnenie sa vydáva na získavanie osobných údajov pre informačný systém ***Názov informačného systému*** s podmienkami uvedenými v Informácii pre dotknutú osobu.
Oprávnená osoba je povinná pri získavaní osobných údajov postupovať v zmysle § 5 až § 18 Zákona. Povinnosti a kompetencie oprávnenej osoby sú taktiež konkretizované v internej smernici č. OCK / 6-2016 Ochrana osobných údajov v pôsobnosti Slovenskej komory SP a ASP.

Poverenie sa vydáva na dobu určitú t.j. na dobu trvania uvedeného pracovného zaradenia / výkonu funkcie. Vo veci ukončenia dôvodov na získavanie a spracúvanie osobných údajov je povinný bezodkladne rozhodnúť štatutárny orgán prevádzkovateľa informačného systému.

V ***Meste***, dňa ***DD. mesiac RRRR***

Podpis predsedu a Odtlačok pečiatky organizácie
_____
Titul, Meno PRIEZVISKO
Predseda Slovenskej komory SP a ASP

POTVRDENIE O PREVZATÍ POVERENIA

V ***Meste***, dňa ***DD. mesiac RRRR***

Podpis poverenej osoby
_____
Titul, meno, priezvisko poverenej oprávnenej osoby

Príloha č. 4

ZÁZNAM O POUČENÍ OPRÁVNENEJ OSOBY

Podpísaný/á
Meno a priezvisko: ***titul, meno, priezvisko poverenej osoby***
Pracovné zaradenie: ***pracovné zaradenie poverenej osoby***
(ďalej len „oprávnená osoba“)

potvrdzuje, že bol(a) v zmysle §§ 21 a 22 zákona č. 122/2013 Z.z o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „Zákon“) poučený(á) o právach a povinnostiach ustanovených Zákonom a o zodpovednosti za ich porušenie, vrátane zodpovednosti podľa Zákona ako aj o pracovnoprávnej, občianskoprávnej a trestnoprávnej zodpovednosti podľa príslušných predpisov.

Prevádzkovateľ informačných systémov, v ktorých sa spracúvajú osobné údaje dotknutých osôb – ***názov organizácie,*** so sídlom ***adresa sídla organizácie/ ulica číslo, PSČ, mesto***, IČO: ***IČO organizácie***,

ma zároveň informoval o:

- rozsahu oprávnení, popise povolených činností, podmienkach spracúvania osobných údajov a obsahu spracovateľských operácií pri spracúvaní osobných údajov, ktoré vyplývajú z môjho pracovného zaradenia a určených pracovných povinností a ktoré sú konkretizované ďalej v Bezpečnostnej smernici, popise pracovnej pozície a riadiacich aktoch organizácie, s ktorými som bol(a) oboznámený(á) pred týmto poučením,
- povinnosti zachovávať mlčanlivosť o osobných údajoch, s ktorými prídem do styku; tie nesmiem využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmiem zverejniť a nikomu poskytnúť ani sprístupniť,
- tom, že povinnosť mlčanlivosti trvá aj po zmene pracovného zaradenia, skončení pracovného pomeru alebo zmluvného vzťahu,
- povinnostiach vyplývajúcich z Bezpečnostnej smernice na ochranu osobných údajov.

V ***Meste***, dňa ***DD. mesiac RRRR***

Podpis poverenej osoby

_____

Titul, meno, priezvisko poverenej oprávnenej osoby

VYPLNÍ OSOBA, KTORÁ VYKONALA POUČENIE

Meno, priezvisko, titul osoby, ktorá vykonala poučenie: ***titul, meno, priezvisko***
Pracovné zaradenie: ***názov pracovné zaradenie***

Dátum vykonania poučenia: ***DD.MM.RRRR***

Podpis osoby, ktorá vykonala poučenie

_____

Titul, meno, priezvisko osoby ktorá vykonala poučenie

Dátum, kedy poučená osoba prestala byť oprávnenou osobou: .....

Príloha č. 5

URČENIE OPRÁVNENÝCH OSÔB S PRÍSTUPOM K OSOBNÝM ÚDAJOM

Prevádzkovateľ informačných systémov (IS), v ktorých sa spracúvajú osobné údaje (OÚ) dotknutých osôb: ***Názov organizácie***
Názov informačného systému: ***názov informačného systému***
Zodpovedná osoba za IS: ***titul, meno, priezvisko poverenej zodpovednej osoby***

Titul	Meno	Priezvisko	Útvar / volený orgán	Funkcia	Rozsah oprávnení / povolené činnosti							Získavanie OÚ

Mesto, dátum

.....
Meno a podpis štatutárneho orgánu prevádzkovateľa

Legenda povolených činností: A - úplný prístup / čítanie, zápis, zmena; B - len čítanie (v prípade, že pre daný IS je povolené len čítanie, tak sa za označenie prístupu pridá /B, napr. VZ/B);
P - čiastočný prístup v rozsahu oddelenia, VK - výberové konania; D – dochádzka; SH - služobné hodnotenia; VZ - vzdelávanie
Legenda získavanie OÚ: Z - uveďte ak oprávnená osoba získava osobné údaje priamo od dotknutej osoby

Príloha č. 6

ZÁZNAM O POUČENÍ INEJ FYZICKEJ OSOBY

Podpísaný/á
Meno a priezvisko: ***titul, meno, priezvisko poučenej osoby***
Názov a číslo dokladu totožnosti: ***názov a číslo dokladu totožnosti poučenej osoby***
Zamestnávateľ*: ***v odôvodnených prípadoch uviesť názov zamestnávateľa poučenej osoby***
Adresa zamestnávateľa*: ***v odôvodnených prípadoch uviesť adresu zamestnávateľa pouč. osoby***
(ďalej len „poučená osoba“)

potvrdzujem, že som bol(a) v zmysle § 22 zákona č. 122/2013 Z.z o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „Zákon“) poučený(á) o právach a povinnostiach ustanovených Zákonom a o zodpovednosti za ich porušenie, vrátane zodpovednosti podľa Zákona ako aj o pracovnoprávnej, občianskoprávnej a trestnoprávnej zodpovednosti podľa príslušných predpisov.

Prevádzkovateľ informačných systémov, v ktorých sa spracúvajú osobné údaje dotknutých osôb – ***názov organizácie,*** so sídlom ***adresa sídla organizácie/ ulica číslo, PSČ, mesto***, IČO: ***IČO organizácie***,

ma zároveň informoval o:

- rozsahu oprávnení, popise povolených činností, podmienkach spracúvania osobných údajov a obsahu spracovateľských operácií pri spracúvaní osobných údajov,
- povinnosti zachovávať mlčanlivosť o osobných údajoch, s ktorými prídem do styku; tie nesmiem využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmiem zverejniť a nikomu poskytnúť ani sprístupniť, - aj po ukončení dôvodov na oboznamovanie sa s osobnými údajmi, skončení zmluvnej služby alebo iného zmluvného vzťahu,
- povinnostiach vyplývajúcich z Bezpečnostnej smernice na ochranu osobných údajov Prevádzkovateľa

V odôvodnených prípadoch sa uvedie dôvod a rozsah oboznamovania sa s osobnými údajmi:

V ***Meste***, dňa ***DD. mesiac RRRR***

Podpis poučenej osoby

_____

Titul, meno, priezvisko poučenej osoby

VYPLNÍ OSOBA, KTORÁ VYKONALA POUČENIE

Meno, priezvisko, titul osoby, ktorá vykonala poučenie: ***titul, meno, priezvisko***
Pracovné zaradenie: ***názov pracovné zaradenie***

Dátum vykonania poučenia: ***DD.MM.RRRR***

Podpis osoby, ktorá vykonala poučenie

_____

Titul, meno, priezvisko osoby ktorá vykonala poučenie

Príloha č. 7

SÚHLAS DOTKNUTEJ OSOBY SO SPRACÚVANÍM OSOBNÝCH ÚDAJOV

Podpísaný/á
Meno a priezvisko: ***titul, meno, priezvisko dotknutej osoby (DO)***
Pracovné zaradenie: ***pracovné zaradenie DO / vzťah DO k prevádzkovateľovi***
(ďalej len „dotknutá osoba“)

potvrdzuje, že bol/a v zmysle § 15 zákona č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov poučený/á prevádzkovateľom o právach a povinnostiach dotknutej osoby uvedených v § 28 zákona a

s ú h l a s í

s ich spracúvaním v informačnom systéme ***názov informačného systému*** prevádzkovateľa – ***názov organizácie,*** so sídlom ***adresa sídla organizácie/ ulica číslo, PSČ, mesto***, IČO: ***IČO organizácie***, v rozsahu podľa zoznamu osobných údajov a podmienok spracúvania uvedených v Informácii na druhej strane tohto súhlasu.

Osobné údaje sú spracúvané za účelom ***popis účelu spracovanie osobných údajov***, v rozsahu a za podmienok stanovených osobitnými zákonmi*. Osobitné zákony boli prevádzkovateľom aplikované do procedúr a pracovných postupov na ich vykonanie (interné smernice).

Osobné údaje k uvedenému účelu sú získavané od zamestnancov v rámci pracovnoprávnych vzťahov a v súvislosti s vedením agendy uchádzačov o zamestnanie a realizácie výberových konaní, **....**

Súhlas na spracúvanie osobných údajov sa dáva na dobu trvania pracovnoprávneho vzťahu. Po skončení pracovnoprávneho vzťahu zabezpečí prevádzkovateľ likvidáciu osobných údajov alebo ich archiváciu v zmysle osobitných zákonov.

Zaväzujem sa bez zbytočného odkladu oznámiť zamestnávateľovi každú zmenu mojich osobných údajov do 7 dní po ich zmene. Dotknutá osoba potvrdzuje, že poskytnuté osobné údaje sú správne, pravdivé a boli poskytnuté dobrovoľne, bez nátlaku a súhlasí s ich využitím k vymedzenému účelu.

V ***Meste***, dňa ***DD. mesiac RRRR***

Podpis dotknutej osoby

_____

Titul, meno, priezvisko dotknutej osoby

* Zákon č. 219/2014 Z.z. o sociálnej práci a o podmienkach na výkon niektorých odborných činností v oblasti sociálnych vecí a rodiny a o zmene a doplnení niektorých zákonov, zákon č. 311/2001 Z. z. Zákonník práce, zákon č. 580/2004 Z. z. o zdravotnom poistení, zákon č. 461/2003 Z. z. o sociálnom poistení, zákon č. 595/2003 Z. z. o dani z príjmov, zákon č. 650/2004 Z. z. o doplnkovom dôchodkovom sporení, zákon č. 5/2004 Z. z. o službách zamestnanosti, zákon č. 462/2003 Z. z. o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca, zákon č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia, zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci, zákon č. 563/2009 Z.z. o správe daní (daňový poriadok) a ďalšie zákony upravujúce povinnosti zamestnávateľa.

Zoznam osobných údajov

Rodné číslo, priezvisko, meno, titul, dátum a miesto narodenia, adresa trvalého a prechodného pobytu, štátna príslušnosť, osobné číslo, pohlavie, rodinný stav. rodinní príslušníci, počet vyživovaných detí, absolvované školy a vzdelanie, výnimky zo vzdelania, doby v zamestnaní, dátum uzatvorenia pracovného pomeru, dôvod vzniku pracovného pomeru, spôsob získania zamestnanca, skúšobná doba, dátum skončenia pracovného pomeru (PP), dôvod skončenia PP, spôsob skončenia PP, pracovná kategória, druh pracovného pomeru, pracovné zaradenie, organizačný útvar, fond pracovnej doby, mzdové náležitosti, dovolenka, porušenie pracovnej disciplíny, nárok na starobný dôchodok, zmenená pracovná schopnosť, služobné hodnotenie, školenia a kurzy, číslo telefónu, predchádzajúci zamestnávatelia, doba základnej vojenskej služby, údaje o priznaní invalidného, čiastočne invalidného dôchodku, údaje o zmenenej pracovnej schopnosti, zdravotná poisťovňa zamestnanca, meno a priezvisko manželky/manžela, druha/družky, rodné číslo manželky/manžela, druha/družky, dátum narodenia, rodné meno; meno a priezvisko dieťaťa, rodné číslo dieťaťa, názov a adresa školy, ktorú dieťa navštevuje, údaje o dôchodkovom poistení zamestnanca, údaje o zákonných zrážkach zamestnanca (výživné), údaje o sporení, pôžičkách a zrážkach na poistenie zamestnanca, údaje o osobnom účte zamestnanca, údaje o dočasnej práceneschopnosti zamestnanca, materských dávkach a o ošetrovaní chorého člena rodiny, daňové vyhlásenie k dani z príjmu, daňový bonus, vyhlásenie zamestnanca na uplatnenie zníženia sadzby poistného na starobné poistenie, doklad o návšteve školy (16-25 r.), ostatné údaje vyžadované zákonmi SR, podobizeň na účely vyhotovenia zamestnaneckej karty.

Informácia dotknutej osobe v zmysle § 15, ods. 1 až 3, zákona č. 122/2013 Z.z.

V zmysle § 15 zákona č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov vám v súvislosti so spracúvaním vašich osobných údajov oznamujeme nasledovné informácie:

a) ***Názov organizácie***, so sídlom ***adresa sídla organizácie/ ulica číslo, PSČ, mesto***, IČO: ***IČO organizácie*** (ďalej len „**...**“) je prevádzkovateľom informačného systému ***názov informačného systému*** (ďalej len „**...**“), v ktorom budú Vaše osobné údaje spracúvané v rozsahu podľa vyššie spísaného zoznamu.

b) Účelom spracúvania osobných údajov je ***plánovanie, zabezpečovanie, rozvoj ľudských zdrojov a realizácia miezd, prípadne realizácia zmluvných vzťahov s fyzickými osobami, ktoré vykonávajú činnosť, vytvárajú dielo podľa autorského zákona, alebo za finančnú odmenu poskytujú Prevádzkovateľovi služby v rámci akvizičnej činnosti.*** Účel spracúvania je stanovený osobitnými zákonmi pre oblasť pracovno-právnych vzťahov, daní, sociálneho, zdravotného a dôchodkového poistenia.

c) Pre splnenie uvedeného účelu spracúvania osobných údajov prevádzkovateľ využíva systém POHODA od spoločnosti STORMWARE s.r.o.

d) Ďalšie podmienky spracúvania osobných údajov:
   - Osobné údaje môžu byť spracúvané prostredníctvom automatizovaných, čiastočne automatizovaných, alebo neautomatizovaných prostriedkov spracúvania, pričom sa uplatňujú primerané technické, organizačné a personálne bezpečnostné opatrenia zodpovedajúce spôsobu spracúvania, ktoré sú deklarované Bezpečnostným projektom na ochranu osobných údajov.
   - Osobné údaje spracúvajú len oprávnené osoby, ktoré boli náležitým spôsobom určené a poučené.

e) Dobrovoľnosť poskytnutia osobných údajov:
   - Poskytnutie uvedených osobných údajov nie je dobrovoľné; je potrebné na splnenie účelu spracúvania osobných údajov, ktorý určili osobitné zákony SR, vzťahujúce sa na zamestnanosť, sociálne a zdravotné poistenie, daňové a iné povinnosti zamestnávateľa. Z uvedeného dôvodu sa písomný súhlas na spracúvanie osobných údajov nezískava.
   - ***Dobrovoľné je len poskytnutie vašej podobizne, ktorá je však potrebná na korektné zabezpečenie služieb, zamestnaneckých výhod a činností Organizácie a slúži výhradne pre vnútornú potrebu.***

f) Príjemcovia:
   - Osobné údaje môžu byť sprístupnené len príjemcom, ktorý splnili požadované podmienky na bezpečnosť osobných údajov a ktorých výkon priamo súvisí so splnením účelu spracúvania (Zdravotná poisťovňa, Sociálna poisťovňa, Daňový úrad, Úrad práce, Ústredie práce, sociálnych vecí a rodiny).

g) Zverejňovanie:
   - Osobné údaje nebudú zverejnené.

h) Tretie krajiny:
   - Osobné údaje nebudú sprístupnené príjemcom v tretej krajine.

Zároveň vás poučujeme o existencii vašich práv ako dotknutej osoby uvedených v §28 Zákona č. 122/2013 Z.z.

Príloha č. 8

INFORMÁCIA DOTKNUTEJ OSOBE O ÚČELE A PODMIENKACH SPRACÚVANIA OSOBNÝCH ÚDAJOV

(vykonaná v zmysle §15, ods. 1 až 3, zákona č. 122/2013 Z.z.)

Podpísaný/á
Meno a priezvisko: ***titul, meno, priezvisko dotknutej osoby (DO)***
Pracovné zaradenie: ***pracovné zaradenie DO / vzťah DO k prevádzkovateľovi***
(ďalej len „dotknutá osoba“)

potvrdzuje, že bol/a v zmysle § 15 zákona č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov poučený/á prevádzkovateľom o právach a povinnostiach dotknutej osoby uvedených v § 28 zákona a o nasledovných podmienkach a účele spracúvania osobných údajov:

a) ***Názov organizácie***, so sídlom ***adresa sídla organizácie/ ulica číslo, PSČ, mesto***, IČO: ***IČO organizácie*** (ďalej len „**...**“) je prevádzkovateľom informačného systému ***názov informačného systému*** (ďalej len „**...**“), v ktorom budú Vaše osobné údaje spracúvané v rozsahu podľa zoznamu, ktorý je uvedený na druhej strane tohto tlačiva.
b) Účelom spracúvania osobných údajov je ***plánovanie, zabezpečovanie, rozvoj ľudských zdrojov a realizácia miezd, prípadne realizácia zmluvných vzťahov s fyzickými osobami, ktoré vykonávajú činnosť, vytvárajú dielo podľa autorského zákona, alebo za finančnú odmenu poskytujú Prevádzkovateľovi služby v rámci akvizičnej činnosti.*** Účel spracúvania je stanovený osobitnými zákonmi pre oblasť pracovno-právnych vzťahov, dane, sociálne, zdravotné a dôchodkové poistenie.
c) Pre splnenie uvedeného účelu spracúvania osobných údajov prevádzkovateľ využíva systém POHODA od spoločnosti STORMWARE s.r.o..
d) Ďalšie podmienky spracúvania osobných údajov:
   - Osobné údaje môžu byť spracúvané prostredníctvom automatizovaných, čiastočne automatizovaných, alebo neautomatizovaných prostriedkov spracúvania, pričom sa uplatňujú primerané technické, organizačné a personálne bezpečnostné opatrenia zodpovedajúce spôsobu spracúvania, ktoré sú deklarované Bezpečnostným projektom na ochranu osobných údajov.
   - Osobné údaje spracúvajú len oprávnené osoby, ktoré boli náležitým spôsobom určené a poučené.
e) Dobrovoľnosť poskytnutia osobných údajov:
   - Poskytnutie uvedených osobných údajov nie je dobrovoľné; je potrebné na splnenie účelu spracúvania osobných údajov, ktorý určili osobitné zákony SR, vzťahujúce sa na zamestnanosť, sociálne a zdravotné poistenie, daňové a iné povinnosti zamestnávateľa. Z uvedeného dôvodu sa písomný súhlas na spracúvanie osobných údajov nezískava.
   - ***Dobrovoľné je len poskytnutie vašej podobizne, ktorá je však potrebná na korektné zabezpečenie služieb, zamestnaneckých výhod a činností Organizácie a slúži výhradne pre vnútornú potrebu.***
f) Príjemcovia:
   - Osobné údaje môžu byť sprístupnené len príjemcom, ktorý splnili požadované podmienky na bezpečnosť osobných údajov a ktorých výkon priamo súvisí so splnením účelu spracúvania (Zdravotná poisťovňa, Sociálna poisťovňa, Daňový úrad, Úrad práce, Ústredie práce, sociálnych vecí a rodiny).
g) Zverejňovanie:
   - Osobné údaje nebudú zverejnené.
h) Tretie krajiny:
   - Osobné údaje nebudú sprístupnené príjemcom v tretej krajine.

Zároveň vás poučujeme o existencii vašich práv ako dotknutej osoby uvedených v §28 Zákona č. 122/2013 Z.z.

Príloha č. 9

ZÁZNAM O VYKONANEJ KONTROLE V INFORMAČNOM SYSTÉME

názov IS

I. Dátum čas a miesto kontroly	
Dátum kontroly IS:	***DD.MM.RRRR***
Čas kontroly IS:	***hh:mm***
Miesto kontroly IS:	***názov miestnosti, v ktorej sa vykonávala kontrola IS***

II. Údaje o spracovateľovi záznamu	
Titul, Meno, Priezvisko:	
Funkcia v organizácii:	
Funkcia v informačnom systéme:	
Titul, meno, priezvisko kompetentného nadriadeného, ktorý vykonanie kontroly nariadil:	

III. Predmet kontroly	
Personálna bezpečnosť:	*Poverenie ZO a jej nahlásenie na Úrad*
Administratívna bezpečnosť:	*Ukladanie a práca s dokumentmi obsahujúcimi osobné údaje*
Režimové a organizačné opatrenia:	*Určenie oprávnených osôb a ich poučenie*
Objektová bezpečnosť	
Technická bezpečnosť v neautomatizovanom IS	
Systémová bezpečnosť v automatizovanom IS	
Komunikačné prostriedky	
Iná (napríklad zlúčenie viacerých oblastí)	

IV. Výsledok kontroly

Zodpovedná osoba – p. ***Titul, meno, priezvisko*** *pozná zásady práce s osobnými údajmi a povinnosti zodpovednej a oprávnenej osoby.*
Osobné údaje sú ukladané predpísaným spôsobom a práca s nimi prebieha v súlade s Internou smernicou č. OCK / 6-2016 Ochrana osobných údajov v pôsobnosti Slovenskej komory SP a ASP.
Dokumenty požadované zákonom – určenie oprávnených osôb a ich poučenie je vykonané.
Komplexná dokumentácie Bezpečnostného projektu ja uložená a obsahuje požadované dokumenty.
Nebolo zistené žiadne porušovanie zákona č. 122/2013 Z. z. o ochrane osobných údajov.
Bez závad.

_____
podpis spracovateľa

V. Návrh opatrení k náprave zistených nedostatkov

...

_____
osoba zodpovedná za výkon dohľadu

VI. Výsledok a termíny ich realizácie

...

_____
osoba zodpovedná za výkon dohľadu

VII. Stanovisko štatutárneho zástupcu prevádzkovateľa IS

Neboli zistené žiadne nedostatky.

_____
štatutárny zástupca prevádzkovateľa IS

Príloha č. 10

ZÁZNAM O BEZPEČNOSTNOM INCIDENTE V INFORMAČNOM SYSTÉME

názov IS

I. Špecifikácia incidentu	
Dátum a čas vzniku incidentu	***DD.MM.RRRR, hh:mm***
Dátum a čas zistenia incidentu	***DD.MM.RRRR, hh:mm***
Dátum a čas vypracovania záznamu	***DD.MM.RRRR, hh:mm***

II. Údaje o spracovateľovi záznamu	
Titul, Meno, Priezvisko:	
Funkcia v organizácii:	
Funkcia v informačnom systéme:	
Titul, meno, priezvisko kompetentného nadriadeného:	

III. Oblasť vzniku incidentu	
Personálna bezpečnosť:	
Administratívna bezpečnosť:	
Režimové a organizačné opatrenia:	
Objektová bezpečnosť	
Technická bezpečnosť v neautomatizovanom IS	
Systémová bezpečnosť v automatizovanom IS	
Komunikačné prostriedky	
Iná (napríklad zlúčenie viacerých oblastí)	

IV. Špecifikácia incidentu	
Popis miesta incidentu	
Popis obsahu incidentu	
Popis zaistených dôkazov	

V. Riešenie incidentu	
Titul, meno, priezvisko osoby, ktorej bol incident postúpený k vybaveniu:	
Funkcia v organizácii:	
Funkcia v informačnom systéme:	

VI. Návrh opatrení využitých k náprave incidentu
...
_____
osoba zodpovedná za výkon dohľadu

VII. Výsledok a termíny ich realizácie
...
_____
osoba zodpovedná za výkon dohľadu

VIII. Stanovisko štatutárneho zástupcu prevádzkovateľa IS
Neboli zistené žiadne nedostatky.
_____
štatutárny zástupca prevádzkovateľa IS