JOGSC
Journal of Global Science
ISSN: 2453-756X (Online) Journal homepage: http://www.jogsc.com

Implementácia eGovernmentu v praxi a ľudský faktor

Peter Lošonczi
Vysoká škola bezpečnostného manažérstva v Košiciach
Ústav bezpečnostného manažérstva
Kukučínova 17, 040 01 Košice, Slovakia
peter.losonczi@vsbm.sk

Abstrakt: Cieľom tejto štúdie je posúdenie súčasného stavu využívania e-služieb zamestnancami verejnej správy. Štúdia okrem úvodného teoretického vymedzenia problematiky obsahuje výsledky dotazníkového prieskumu a návrh odporúčaní, ako napomôcť k dodržiavaniu bezpečnostných pravidiel pri využívaní systémov elektronickej komunikácie. Poukazuje na nedostatky, ktoré boli zistene pri prieskume a súvisia zväčša s najchybovejšou časťou systému – človekom.

Kľúčové slová: eGovernment, informatizácia, elektronizácia, bezpečnosť

JEL klasifikácia: K22, G38, H76

1. Úvod

Verejná správa predstavuje správu vecí verejných, je správou vo verejnom záujme a realizuje sa ako prejav výkonnej moci v štáte. Verejná správa na Slovensku funguje ako oddelený model štátnej správy a územnej samosprávy. Funguje na troch stupňoch: štát, kraj a obec.

Informatizácia spoločnosti je chápaná ako koncepčne riadený proces, ktorý predstavuje postupný prechod k maximálnemu využívaniu informačných a komunikačných technológii vo všetkých oblastiach spoločenského, politického aj hospodárskeho života. (Blišťanová, Sedlák, 2012)

2. Základné východiská pre elektronizáciu verejnej správy

eGovernment na Slovensku sa začal rozvíjať už v roku 1995 a to prijatím zákona NR SR č. 261/1995 Z. z. o informačných systémoch verejnej správy. eGovernment alebo informatizácia spoločnosti, či tzv. elektronizácia verejnej správy sú založené na princípe využívania informačno-komunikačných technológií v rámci inštitúcií verejnej správy, vďaka ktorým je možné efektívne a promptne zabezpečiť splnenie prioritných potrieb obyvateľstva súvisiacich s činnosťou a poskytovaním konkrétnych služieb jednotlivých orgánov verejnej správy na všetkých úrovniach. eGovernment teda označuje aktivity verejnej správy sprístupnené elektronickou formou prostredníctvom informačno-komunikačných technológií, ktorými sú počítače, počítačové siete, internetové siete či mobilné telefóny. (http://www.itapa.sk/, 12.10.2017)

V súlade so zákonom NR SR č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o eGovernmente) v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony s účinnosťou od 1. novembra 2016 sú orgány verejnej moci povinné uplatňovať výkon verejnej moci elektronicky. To znamená, že všetky orgány verejnej moci musia po uplynutí prechodného obdobia prijímať elektronické podania predpísaným spôsobom prostredníctvom elektronických schránok. Zároveň musia vytvárať aj elektronické rozhodnutia a doručovať ich dotknutým subjektom elektronicky. V opačnom prípade nebudú splnené podmienky na elektronickú komunikáciu pri výkone verejnej moci podľa citovaného zákona. Výnimka platí pre orgány verejnej moci, ktorým osobitný zákon tento výkon neumožňuje čiže ho explicitne zakazuje. (https://www.slovensko.sk/, 7.2.2018)

Ministerstvo financií Slovenskej republiky ako ústredný orgán štátnej správy pre oblasť informatizácie spoločnosti zriadilo sekciu informatizácie spoločnosti. Do pôsobnosti tejto sekcie patrili úlohy pre tvorbu koncepcií informatizácie, usmerňovania tvorby koncepcií, vydávania informačných štandardov, sledovania stavu informatizácie, riadenia implementácie operačných programov, správa ústredného portálu verejnej správy a pod.. Pod gesciou ministerstva bol vytvorený portál informatizácia.sk, ktorý zastrešuje danú problematiku v oblasti informatizácie spoločnosti na Slovensku. Od 1. júna 2016 sa informatizácia spoločnosti presunula pod gesciu Úradu podpredsedu vlády SR pre investície a informatizáciu, ktorý:

- pripravuje koncepcie informatizácie spoločnosti a legislatívu v oblasti informatizácie verejnej správy a vydávania štandardov pre ISVS,
- sleduje stav a hodnotenia rozvoja informatizácie spoločnosti,
- usmerňuje tvorbu koncepcií rozvoja informačných systémov verejnej správy,
- riadi správu IT zdrojov verejnej správy v oblasti informačných technológií a implementácie prioritnej osi 7 Operačného programu Integrovaná infraštruktúra ako sprostredkovateľský orgán pod riadiacim orgánom.

Operačný program Informatizácia spoločnosti je referenčný dokument, na základe ktorého bola poskytovaná finančná podpora zo štrukturálnych fondov Európskej únie a to na všetky projekty informatizácie spoločnosti v období rokov 2007-2013. Tieto finančné prostriedky boli na Slovensku použité v súlade so stratégiou Európskej únie. Jej cieľom bolo vybudovať konkurencieschopnú európsku ekonomiku založenú na vedomostiach a inováciách. Globálnym cieľom OPIS-u preto bolo vytvorenie inkluzívnej informačnej spoločnosti, ako prostriedku pre rozvoj vysoko výkonnej vedomostnej ekonomiky.

Informačná bezpečnosť je laicky povedané ochrana informačno-komunikačných technológií a ochrana všetkého čo s nimi súvisí. Význam informačnej bezpečnosti úmerne rastie s rozvojom informačno-komunikačných technológií, ktoré ľudia využívajú a sú od nich čoraz viac závislí. V každej organizácii je dôležité technické zabezpečenie pred potenciálnymi útokmi ľudí, ktorí sú schopní využiť každú chybu systému. No na druhej strane nesmieme zabúdať ani na možné zlyhanie ľudského faktora a preto musíme zabezpečiť aj neustále vzdelávanie zamestnancov v tejto oblasti. Základným pilierom informačnej bezpečnosti a ochrany osobných údajov je bezpečnostná politika každej organizácie, ktorá popisuje pravidlá pre eliminovanie bezpečnostných rizík.

Z jednej strany pohľadu je ľahké občanovi tvrdiť, že elektronická komunikácia je naozaj bezpečná. No z druhej strany pohľadu tým zložitejším kritériom je to, ako ľudí o tom presvedčiť a zároveň ako to dokázať, ale aj zabezpečiť. Zavedenie eGovernmentu do verejnej správy na Slovensku prináša hlavne časové a finančné úspory, ale na druhej strane musíme brať do úvahy zložitý proces implementácie a hlavne hrozby a riziká, ktoré súvisia z bezpečnosťou pri napĺňaní a dodržiavaní litery jeho zákona. Významný dôraz je kladený aj na silný vplyv zákona NR SR č. 18/2018 Z. z. o ochrane osobných údajov a nariadeniu Európskeho parlamentu a Rady EÚ č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe týchto údajov - GDPR.

3. Metodológia - prieskum aktuálneho stavu v praxi

Prieskumom realizovaným začiatkom roku 2018 dotazníkovou formou bolo cieľom zistiť aký je súčasný stav bezpečného využívania elektronickej komunikácie zamestnancami v samospráve, poukázať na nízku informovanosť zamestnancov, na chýbajúce znalosti o e-komunikácii, nedodržiavanie bezpečnostnej politiky a bezpečnostných pravidiel zamestnancami, ktorých sa eGovernment bezprostredne dotýka. Miestom skúmania bolo krajské mesto Košice. Prieskumnú vzorku tvorili zamestnanci samosprávy Mesta Košice, Úradu Košického samosprávneho kraja a košických mestských častí. Spôsob výberu vzorky respondentov bol náhodný a veľkosť vzorky bola 100 respondentov (32 % mužov a 68 % žien). Podľa rozdelenia respondentov do piatich vekových skupín, mala prevahu skupina vo veku od 51-60 rokov (36 %), ďalej od 41-50 rokov (29 %), nasledovala skupina od 31-40 rokov (16 %), predposlednou bola skupina najmladších od 18-30 rokov (10 %) a poslednou veková skupina nad 60 rokov (9 %). Čo sa týka prieskumu vzdelanostnej úrovne respondentov, prevahu mali respondenti s vysokoškolským vzdelaním a to až 70 % a so stredoškolským vzdelaním bolo 30 %. Respondenti boli rozdelení do dvoch základných pracovných pozícií na referenta (90 %) a vedúceho zamestnanca (10 %).

3.1 Kľúčové zistenia z prieskumu v skratke

Vstupnou otázkou bola „Viete, čo znamenajú termíny eGovernment, informatizácia alebo elektronizácia verejnej správy?“, kedy sme u respondentov chceli zistiť, či im niečo hovorí pojem eGovernment, informatizácia či elektronizácia verejnej správy. Na túto otázku kladne, odpovedalo 65 % respondentov, ktorí vedia čo znamená eGovernment, informatizácia či elektronizácia verejnej správy. Čiastočne je informovaných 31 % (31) respondentov, neinformovaných o tejto problematike je 3 % (3) respondentov a 1 % respondentov nezaujíma, čo znamená pojem eGovernment.

Pri otázke „Viete, na čo slúži elektronické schránka (eDesk)?“ sme získali zväčša odpoveď že Elektronická schránka (eDesk) slúži na doručovanie elektronických úradných dokumentov, čo predstavuje 87 zo 100 opýtaných. 52 % respondentov odpovedalo, že na zasielanie elektronických podaní, 3 % respondentov si myslia, že elektronická schránka slúži na e-mailovú komunikáciu a 8 %

Siedma otázka dotazníka znela „Viete, čo potrebujete pre vstup do elektronickej schránky?“**.** Respondent mal výber zo siedmych možností. Bola to otázka, pri ktorej mohol respondent zaškrtnúť ľubovoľný počet odpovedí a tak preukázať aj odborné znalosti pre vstup do elektronickej schránky. 87 % (87) respondentov si myslí, že pre vstup do elektronickej schránky je potrebný občiansky preukaz s čipom. 58 % respondentov označilo, že je potrebný aj aktivovaný BOK, 57 % respondentov potrebuje pre vstup do elektronickej schránky aj počítač a 54 % aj pripojenie na internet. Pre vstup do elektronickej schránky potrebuje čítačku kariet aj 58 % respondentov. Za príslušný softvér, ktorý je potrebný pre vstup do elektronickej schránky sa vyjadrilo iba 37 %. 7 % (7) respondentov nevie vôbec, aké komponenty a zariadenia potrebuje pre vstup do elektronickej schránky.

Na ôsmu otázku dotazníka, ktorá znela: „Vlastníte elektronickú identifikačnú kartu?“ iba 22 % (22) respondentov má vo vlastníctve elektronickú identifikačnú kartu a 78 % (78) respondentov ju ešte vôbec nevlastní.

Deviatou otázkou sme sa respondentov opýtali: „Viete, akými kódmi je chránená Vaša elektronická identifikačná karta (eID)?". Na výber boli tri možnosti kódov: BOK, KEP PIN, KEP PUK a štvrtá možnosť výberu bola neviem. 50 % zvolilo možnosť, že eID karta je chránená BOK-om - bezpečnostným osobným kódom. 28 % respondentov si myslí, že ochranu zabezpečuje aj KEP PIN - bezpečnostný kód pre kvalifikovaný elektronický podpis. 23 % respondentov sa pridalo k názoru, že eID karta je chránená aj kódom KEP PUK, ktorý vlastne slúži na odblokovanie súkromného kľúča. Z celkového počtu 100 respondentov sa 46 % respondentov vyjadrilo, že nevie, akými kódmi je chránená elektronická identifikačná karta. Z výsledkov vyplýva, že respondenti nemajú postačujúce informácie a vedomosti o ochrane eID kódmi.

Desiata otázka úzko súvisela s ôsmou otázkou a znela: „Máte aktivovaný BOK (bezpečnostný osobný kód)?“. Respondenti mali na výber tri možnosti: áno, nie a neviem, čo je BOK a na čo sa používa. 16 % respondentov sa vyjadrilo, že má aktivovaný BOK, 74 % respondentov nemá aktivovaný BOK a 10 % respondentov nevie, čo je BOK a načo sa používa. Keď pri ôsmej otázke sa 78 % respondentov vyjadrilo, že nevlastní eID kartu s čipom, tak na porovnanie pri tejto otázke 74 % respondentov nemá ani aktivovaný BOK - bezpečnostný osobný kód.

Jedenásta otázka „Viete, čím sa podpisuje úradné rozhodnutie v elektronickej komunikácii?“ ponúkala respondentovi na výber z piatich možností. Bola to, ktorá umožnila zaškrtnutie viacerých variant:

- zaručeným elektronickým podpisom,
- kvalifikovaným elektronickým podpisom s mandátnym certifikátom,
- kvalifikovanou elektronickou pečaťou,
- naskenovaním podpisu,
- neviem.

39 % respondentov označilo, že na podpísanie úradného rozhodnutia je potrebný zaručený elektronický podpis, 64 % respondentov sa vyjadrilo za kvalifikovaný elektronický podpis s mandátnym certifikátom a 44 % respondentov pridalo aj kvalifikovanú elektronickú pečať. Naskenovaním podpisu by úradné rozhodnutie v elektronickej komunikácii nepodpísal žiaden respondent. 13 % respondentov zatiaľ nevie, čím sa v elektronickej komunikácii podpisuje úradné rozhodnutie. Podľa spracovaných výsledkov a grafického zobrazenia môžeme konštatovať, že asi polovica respondentov nie je si istá respektíve nevie, čím môže podpisovať úradné rozhodnutie v elektronickej komunikácii.

Dvanástou otázkou či „Viete, na čo slúži mandátny certifikát?" sa respondenti vyjadrili k štyrom možnostiam:

- na podpisovanie dokumentov v listinnej podobe,
- na podpisovanie elektronických dokumentov fyzickou osobou oprávnenou konať za inú osobu,
- na podpisovanie elektronických úradných rozhodnutí,
- neviem.

48 % respondentov si myslí, že na podpisovanie dokumentov fyzickou osobou oprávnenou konať za inú osobu. 47 % respondentov sa priklonilo k názoru, že na podpisovanie elektronických úradných rozhodnutí. 19 % respondentov nevie, na čo slúži mandátny certifikát a 5 % respondentov by mandátnym certifikátom podpísalo dokument aj v listinnej podobe - forme. Vyhodnotením tejto otázky môžeme konštatovať aj odbornú neznalosť z radov respondentov, ktorí by sa pokúšali aj o nemožné, podpísať mandátnym certifikátom aj listinný dokument. Podľa spracovanej štatistiky by sa o to pokúsilo 5 % žien starších vekových kategórií.

Predposledná otázka či „Nechávate čipovú kartu zasunutú v čítačke počas celej pracovnej doby?" . Dvaja respondenti čo predstavuje 2 % opýtaných sa vyjadrili, že áno, nechávajú čipovú kartu zasunutú celý deň v čítačke. 31 % respondentov nenecháva čipovú kartu zasunutú v čítačke počas celej pracovnej doby a 67 % respondentov nepoužíva čipovú kartu, čiže ju zasunutú v čítačke ani nemá.

Poslednou otázkou bola otázka v súčasnosti často interpretovaná aj v médiách „ Veríte, Že elektronická komunikácia je bezpečná?"**.** Aj na záverečnú otázku mali možnosť reagovať oslovení respondenti a vyberať z piatich možností, z ktorých mohli označiť iba jednu. Iba 8 % respondentov verí, že elektronická komunikácia je bezpečná. 22 % respondentov sa vyjadrilo, že neverí a 6 % respondentov neverí od čias, kedy boli napadnuté čipy na

občianskych preukazoch. Pochybnosť o bezpečnej elektronickej komunikácii má 37 % respondentov a 27 % respondentov odpovedalo, že nevie posúdiť, či elektronická komunikácia je bezpečná.

4. Výsledky a diskusia

Z výsledkov nášho prieskumu sme dospeli k záveru, že z respondentov, ktorí sa zapojili do ankety, viac ako polovica je informovaná o eGovernmente a vie, čo je informatizácia verejnej správy. Táto znalosť tkvie v tom, že zamestnanci košickej samosprávy už používajú elektronickú komunikáciu. Väčšina respondentov vie, načo slúži elektronická schránka a čo potrebujú pre vstup do schránky. Málo z respondentov vlastní elektronickú identifikačnú kartu s čipom, má aktivovaný bezpečnostný osobný kód a vie, akými kódmi je eID karta chránená. Polovica z respondentov vie, na čo slúži mandátny certifikát a že ním môžu podpísať elektronický úradný dokument. No našli sa medzi respondentmi aj takí, ktorí by mandátnym certifikátom podpísali aj dokument v listinnej podobe. Všetci opýtaní tvrdia, že neposkytli eID kartu a heslo kolegom na podpísanie elektronického dokumentu a väčšina z nich nenecháva zasunutú kartu v čítačke počas celej pracovnej doby. Čo sa týka dôvery v bezpečnosť e-komunikácie, verí jej len 8 % respondentov, čo je pohľadu zamestnancov samosprávy veľmi málo. Veľa z nich stratilo dôveru pre napadnuté čipy na občianskych preukazoch, neveria jej, alebo majú o nej pochybnosť.

Pri vyhodnotení hypotézy „Čím vyšší vek zamestnancov samosprávy, tým väčšia pravdepodobnosť nezáujmu o elektronizáciu verejnej správy.“, sme vychádzali z praxe, že starší zamestnanci samospráv už nejavia záujem o zavádzanie elektronizácie vo verejnej správy. Prikláňajú sa skôr k názoru, že papier a listinná forma komunikácie bola, je a bude tým najjednoduchším a najlepším spôsobom vybavovania úradných záležitostí. Z výsledkov prieskumu sme došli k záveru, že vekové skupiny od 41-50 a od 51-60 rokov majú o elektronizáciu najväčší záujem, čím sme hypotézu vyvrátili.

Pri druhej hypotéze „V oblasti eGovernmentu digitálna gramotnosť populácie s vysokoškolským vzdelaním predstavuje vyššiu úroveň“ sme vychádzali z výsledkov prieskumu 7. otázky a z predpokladu, že vysokoškolsky vzdelaná populácia v samospráve má v oblasti eGovernmentu vyššiu úroveň digitálnej gramotnosti. Z výsledkov prieskumu sme došli k záveru, že v tejto oblasti sú najgramotnejší a najinformovanejší respondenti s vysokoškolským vzdelaním a tým sa nám aj potvrdila naša hypotéza.

Tretiu hypotézu „Mladšie vekové skupiny populácie veria v bezpečnosť elektronickej komunikácie viac ako staršie.“ sme overili na základe výsledkov prieskumu poslednej otázky a vekových skupín respondentov. Tvrdením bolo, že mladšie vekové skupiny veria v bezpečnosť elektronickej komunikácie viac ako tie staršie. Podľa výsledkov prieskumu sme dospeli práve k opačnému tvrdeniu a tým sa hypotéza vyvrátila.

4.1 Odporúčania pre zvýšenie efektívnosti a bezpečnosti

Implementácia procesov eGovernmentu do verejnej správy priniesla so sebou aj novú potrebu vzdelávania jej zamestnancov. Efektívnym vzdelávaním, zvyšovaním kvalifikácie i preškoľovaním môže každý zamestnanec verejnej správy získať určité vedomosti, poznatky, znalosti, zručnosti a schopnosti na výkon svojej práce. V súčasnej dobe moderných informačných technológií, kedy je agenda úradov spracovávaná elektronicky a na vzdelanostnú úroveň zamestnancov sa kladú väčšie nároky a očakávania, je nevyhnutnou podmienkou každého zamestnanca počítačová gramotnosť. (Kováčová, Vacková, 2015)
Ak chceme, aby v inštitúciách a úradoch verejnej správy pracovali vzdelaní, odborní a flexibilní ľudia, navrhujeme:

- zabezpečiť systematické vzdelávanie zamestnancov v odbore IT s koncentráciou na triezve posúdenie bezpečnosti,
- zabezpečiť zamestnancom rôzne formy celoživotného vzdelávania,
- zabezpečiť školenia zamestnancov v oblasti elektronizácie,
- a motivovať ľudí, ktorí moderné technológie odmietajú.

Veľmi veľa závisí aj na ochote zamestnancov vzdelávať sa. Získané nové vedomosti a zručnosti vzdelávaním zamestnancov sa však odrazia nielen na ich práci, vzájomnej komunikácií, ale hlavne na spokojnosti občanov.

Bezpečnosť elektronickej komunikácie z pohľadu eGovernmentu

Môžeme s určitosťou tvrdiť, že bezpečnosť v oblasti eGovernmentu je v súčasnosti jednou z najpreberanejších tém v našej spoločnosti. Bezpečnosť je základnou a zároveň veľmi dôležitou súčasťou každého fungujúceho systému. Potenciálne narušenie bezpečnosti vedie k poklesu dôvery tak občanov ako aj užívateľov elektronizácie. Bez dôvery by sa občania, či už ako klienti verejnej správy alebo užívatelia informačných systémov, ktorí odmietajú moderné technológie, uzavreli a odmietali by tento technologický pokrok ešte vo väčšej miere ako doposiaľ. Problematika bezpečnosti v oblasti eGovernmentu už bola podceňovaná napadnutím ochranných prvkov na čipových občianskych preukazoch. Bezpečnosť eGovernmentu je jedným z kľúčových atribútov, rastie počet narušení a útokov voči jeho systémom, preto navrhujeme niektoré odporúčania.

Z pohľadu občana, či už ako klienta alebo zamestnanca, je základnou požiadavkou bezpečný prístup a bezpečné využívanie elektronickej komunikácie tak, aby nedošlo pri spracovaní osobných údajov v databázach k zneužitiu a nebola ohrozená ich dôvernosť, integrita a dostupnosť. Oblasť informačnej bezpečnosti sa stále mení a každým dňom sa objavujú nové hrozby a riziká. Jedným z rizík môže byť aj nízke bezpečnostné povedomie zamestnancov, zodpovednosť za svoje konanie, podceňovanie rizík či úmyselná počítačová kriminalita. Problematika zabezpečenia počítačových systémov je v súčasnosti veľmi zložitá a organizácie vynakladaj ú na ich ochranu nemalé finančné prostriedky. Preto najlepším spôsobom ochrany je prevencia a eliminácia rizík na prijateľné alebo zostatkové riziko, pretože potenciálne riziko stále existuje. Pre elimináciu rizík odporúčame venovať pozornosť týmto bezpečnostným požiadavkám:

- permanentne školiť zamestnancov VS v oblasti počítačovej bezpečnosti,
- zálohovať elektronické dáta pravidelne,
- zabezpečiť zálohové úložiská na inom mieste,
- zabezpečiť bezpečnosť informačných systémov samospráv,
- zabezpečiť technické prepojenie IS samospráv a ÚPVS na základe dohody o integračnom zámere,
- zabezpečiť systémové riešenia projektov OPIS,
- zabezpečiť legislatívne opatrenia v oblasti informačnej bezpečnosti,
- zabezpečiť dodržiavanie legislatívnych opatrení zamestnancami VS,
- zvýšiť bezpečnostné povedomie a dôslednosť zamestnancov,
- zabezpečiť neustálu bezpečnosť elektronických schránok,
- zabezpečiť neustálu bezpečnosť a archiváciu elektronických dokumentov,
- zabezpečiť bezpečnosť zaručenej konverzie proti potenciálnemu zneužitiu,
- zabezpečiť zadávanie prihlasovacích údajov v IS verejnej správy,
- zabezpečiť zadávanie prihlasovacích údajov do elektronickej schránky na portál ÚPVS prostredníctvom eID karty,
- zabezpečiť kryptológiu, čiže šifrovanie a kódovanie kľúčov, aby nedochádzalo k potenciálnemu dešifrovaniu algoritmov,
- dodržiavať bezpečnostné štandardy,
- aktívne využívať a manažovať bránu firewall,
- nainštalovať a pravidelne aktualizovať antivírusový program,
- zabezpečiť heslom pripojenie do siete,
- zabezpečiť zdieľanie adresárov a súborov,
- zapnúť kontrolu používateľských kont,
- zabezpečiť bezpečnú komunikáciu, uloženie a prenos dát,
- zabezpečiť prístup užívateľov k modulom, agendám, funkciám a údajom prístupovými heslami,
- zabezpečiť pravidelnú obmenu hesiel a ich zložitosť.

Ochrana osobných údajov

Bezpečnosť a ochrana osobných údajov je v súčasnosti pre každú organizáciu jednou z najdôležitejších tém, ktoré rieši súčasná legislatíva a nariadenie Európskeho parlamentu - GDPR. V súvislosti s touto legislatívou, ktorá vstúpi do platnosti v máji tohto roka, je každý prevádzkovateľ aj sprostredkovateľ povinný prijať primerané technické aj organizačné opatrenia vo forme bezpečnostnej smernice. Cieľom týchto opatrení je zaistiť bezpečnosť a ochranu osobných údajov. Najdôležitejšou úlohou zamestnancov verejnej správy je efektívne využívať, poskytovať a zároveň chrániť osobné údaje občanov, ktoré sú uložené v databázach.

Nový zákon rozširuje okruh osobných údajov o údaje technického charakteru, sprísňuje náležitosti súhlasu osoby so spracovaním osobných údajov, sprísňuje vymazanie osobných údajov, zavádza povinnosť nahlasovať bezpečnostné incidenty, povinnosť ustanoviť zodpovednú osobu, ale aj zavádza prísnejšie pokuty za porušenie povinností. V súvislosti s týmito novými legislatívnymi zmenami odporúčame:

- zabezpečiť odborné školenia zamestnancov v oblasti ochrany osobných údajov,
- obmedziť zamestnancom prístup k osobným informáciám,
- zabezpečiť integritu, čiže neporušiteľnosť údajov,
- zabezpečiť dôvernosť údajov, čiže neposkytnúť ich neoprávnenému subjektu,
- zabezpečiť časovú dostupnosť údajov,
- zabezpečiť zadávanie prístupových práv do elektronického IS len so súhlasom nadriadenej osoby,
- zabezpečiť prístup k rodným číslam a URI adresám v IS len so súhlasom nadriadenej osoby,
- zabezpečiť prístup užívateľov do elektronickej schránky len so súhlasom štatutára,
- zabezpečiť obmedzenie prístupových práv k osobným údajom,
- poučiť zamestnancov a vysvetliť význam ochranných kódov na eID karte s čipom (občianskom preukaze a mandátnom certifikáte),
- sledovať udelené oprávnenia jednotlivým zamestnancom,
- odobrať oprávnenia v prípade bezpečnostného incidentu,
- zrušiť oprávnenia v prípade zmeny pracovnej pozície,
- zrušiť oprávnenia v prípade ukončenia pracovného pomeru,
- zabezpečiť zainteresovanosť zamestnancov, aby vedeli čo majú, čo môžu, čo musia a čo nesmú robiť pri spracovávaní informácií.

Vieme o tom, že mnohé z týchto odporúčaní sú už dávno základným štandardom pre prevádzku informačných systémov verejnej správy, avšak im nasadenie a udržiavanie v správnom režime je dosť neisté. Len z tohto dôvodu sme si ich dovolili tu zrekapitulovať.

5. Záver

Implementáciu eGovernmentu do verejnej správy na Slovensku je veľmi zložitým procesom, ktorý ešte stále nie je ukončený. Každé rozvíjanie novej technológie prináša nové úskalia, ktorým musíme čeliť a im odolávať, aby sme ich mohli úspešne zvládnuť, pretože majú svoj význam. Pripravenosť technologická neznamená automatickú pripravenosť ľudskú, schopnosť zvládať zmenu práce, osvojiť si nové postupy, znalosti a trendy prerodu od papierovej agendy k elektronickej. Nastáva obdobie, kedy nevyhnutnou súčasťou fungovania verejnej správy bude aj potreba udržiavať u zamestnancov poznanie a zručnosti v informačnej oblasti vždy na aktuálnej úrovni.

Zoznam bibliografických odkazov

BLIŠŤANOVÁ, M. - SEDLÁK, V. 2012. *Manažérske informačné systémy.* 1. vyd. Košice: Vysoká škola bezpečnostného manažérstva v Košiciach, 2012. 81 s. ISBN 978-80-89282-78-4.

ITAPA. *eGovernment.* [online]. [cit. 2017-10-12]. Dostupné na internete: http://www.itapa.sk/egovernment/

POŽÁR, Jozef. 2005. *Informační bezpečnost.* Plzeň: Vydavatelství a nakladatelství Aleš Čenek, s.r.o., 2005. 311 s. ISBN 80-86898-38-5.

KOVÁČOVÁ, L.; VACKOVÁ, M. 2015. Applying Innovative Trends in the Process of Higher Education Security Personnel in Order to Increase Efficiency, In: *Procedia-Social and Behavioral Sciences*. - Oxford: Elsevier, 2015. - ISSN 1877-0428. - S.120-125.

ÚRAD PODPREDSEDU VLÁDY SR PRE INVESTÍCIE A INFORMATIZÁCIU. 2007. *Stratégia informatizácie verejnej správy.* [online]. [cit. 2018-02-12]. Dostupné na internete: (http://www.informatizacia.sk/strategia-informatizacie-verejnei-spravy/

Nariadenie Európskeho parlamentu a rady EÚ č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

ÚSTREDNÝ PORTÁL VEREJNEJ SPRÁVY. 2016. *Usmernenie k základným povinnostiam orgánov verejnej moci podľa zákona o eGovernmente.* [online]. [cit. 2018-04-05]. Dostupné na internete: https://www.slovensko.sk/sk/agendy/agenda/_usmernenie-k-zakladnym-povinno/

Zákon NR SR č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.Zákon NR SR č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e- Governmente).