INTERNÉ INFORMAČNÉ SYSTÉMY

(SPRACÚVANIE OSOBNÝCH ÚDAJOV V CIRKEVNÝCH AUTOMATIZOVANÝCH INFORMAČNÝCH SYSTÉMOCH)

Tento dokument nadväzuje na záväzné pravidlá Katolíckej cirkvi v oblasti ochrany osobných údajov:

Zabezpečenie ochrany osobných údajov Rímskokatolíckou cirkvou v Slovenskej republike
Zabezpečenie ochrany osobných údajov Gréckokatolíckou cirkvou v Slovenskej republike

Použité skratky:

AIS	automatizovaný informačný systém
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
IdM	Identity management, správa identít
IKT	informačné a komunikačné technológie
IS	informačný systém
OÚ	osobné údaje (osobný údaj)
OOÚ	ochrana osobných údajov
RBAC	Role based access control, riadenie prístupu na základe rolí
Smernica KC	smernica Zabezpečenie ochrany osobných údajov Rímskokatolíckou, resp. Gréckokatolíckou cirkvou v Slovenskej republike
ÚOOÚ	Úradu na ochranu osobných údajov
ZOOÚ	Zákon o ochrane osobných údajov

Obsah:

1. Rámec ochrany osobných údajov v AIS

Jedným z dôležitých aspektov moderných technológií tvoriacich základ virtuálneho sveta je informačná bezpečnosť[1].
Informačná bezpečnosť naberá na dôležitosti nielen vzhľadom na penetráciu informačných technológií vo všetkých oblastiach ľudskej činnosti, ale aj vzhľadom na programové smerovanie krajín moderného sveta k znalostnej ekonomike a elektronizácii štátnej správy (eGovernment). Takto sa informačné a komunikačné technológie (IKT) stávajú strategickou súčasťou dnešnej spoločnosti, čo je podčiarknuté aj rozsahom informačnej kriminality, resp. nárastom zneužívania možností IKT a pretavením tohoto problému do legislatívnych rámcov technologicky vyspelých krajín na zabezpečenie informačnej bezpečnosti a ochrany osobných údajov.

Práve spracovávanie osobných údajov (OÚ) dotknutých osôb je jedným z rizikových faktorov informačnej bezpečnosti, čo sa premietlo aj do Zákona o ochrane osobných údajov[2] (ZOOÚ) a európskeho nariadenia GDPR[3].
Keďže prostredníctom IKT sú realizované prakticky všetky moderné automatizované informačné systémy, splnenie legislatívnych požiadaviek OOÚ sa bezprostredne informačných a komunikačných systémov dotýka[4].
V rámci implementácie ochrany osobných údajov (OOÚ) v automatizovaných informačných systémov (AIS) treba dbať aj na širší kontext ZOOÚ a GDPR, osobitne na nariadenie eIDAS[5], smernicu NIS[6] a jej implementáciu v slovenskom Zákone o kybernetickej bezpečnosti[7] i najnovšie nariadenie ePrivacy[8].

Vymedzenie pojmov a definície, osobitné ustanovenia pre spracúvanie OÚ podľa jednotlivých kategórií dotknutých osôb, kategórie spracúvaných OÚ a identifikácia informačných systémov sú uvedené v smerniciach: *Zabezpečenie ochrany osobných údajov Rímskokatolíckou cirkvou v Slovenskej republike* a *Zabezpečenie ochrany osobných údajov Gréckokatolíckou cirkvou v Slovenskej republike*.

---

1 Hovoríme o informačnej bezpečnosti vo všeobecnosti. Kybernetická bezpečnosť je podmnožinou informačnej bezpečnosti a vzťahuje sa priamo na konkrétne technológie IKT.
2 Zákon č. 18/2018 Z. z. o ochrane osobných údajov.
3 General Data Protection Regulation (GDPR) – Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov). Štruktúrovaný dokument GDPR je k dispozícii na webovej stránke: https://www.lewik.org/dataset/136/
4 GDPR neposkytne žiadne konkrétne návody, za prípravu metodík, návodov a názorov na problematiku je zodpovedná The Article 29 Data Protection Working Party (WP 29), ktorá pripravuje vykonávacie pravidlá a výklady GDPR: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
5 eIDAS – electronic IDentification, Authentication and trust Services. Nariadenie o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu): http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
6 NIS – Network and Information Security. Smernica o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii: http://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52013PC0048&from=EN
7 Zákon o kybernetickej bezpečnosti bol schválený 30.1.2018 a nadobúda účinnosť 1.4.2018: https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2017/407
8 ePrivacy – Nariadenie Európskeho parlamentu a Rady (EÚ) o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách a o zrušení smernice 2002/58/ES (smernica o súkromí a elektronických komunikáciách): http://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

2. Základné povinnosti prevádzkovateľa AIS

Prevádzkovateľ/sprostredkovateľ spracovania OÚ je v rámci automatizovaných informačných systémov povinný zabezpečiť:

- **ochranu** osobných údajov
- **monitorovanie** prístupu a spôsobu spracovávania OÚ
- **detekovanie** bezpečnostných incidentov a ich nahlasovanie
- **školenia a vzdelávanie** v oblasti OOÚ

Ochrana, monitoring, detekovanie incidentov a vzdelávanie sa realizujú v technologickej, procesnej a personálnej oblasti.

2.1. Technologické riešenie kompatibilné s legislatívou

Je treba zvoliť také technologické riešenia, ktoré majú **implementované mechanizmy ochrany OÚ** v legislatívnych rámcoch ZOOÚ, GDPR, Zákona o kybernetickej bezpečnosti a Smernice KC. **Technologické riešenie má mať nielen adekvátny dizajn, ale musí byť aj realizovateľné a udržateľné.**

Technologické riešenia musia zabezpečiť potrebné monitorovanie prístupu a spôsobu spracovávania OÚ, detekovanie bezpečnostných incidentov a reporting pokladov pre ich nahlasovanie.

Technologické riešenia kompatibilné so ZOOÚ/GDPR by mali spĺňať požiadavky uvedené v kapitole 3 (*Technologické princípy a požiadavky ochrany OÚ v AIS*).

2.2. Procesy a postupy adekvátne legislatíve

Je potrebné implementovať procesy a postupy ochrany OÚ podľa ZOOÚ, GDPR, Zákona o kybernetickej bezpečnosti a Smernice KC vo forme záväzných interných nariadení **pri implementácii technológií i vo forme záväzných interných nariadení a postupov.**

Ide o procesy a postupy, pri ktorých je **jasne vymedzené kto a aké má práva pre prístup do AIS a k spracovávaniu konkrétnych OÚ**. Procesy a postupy spracovávania OÚ, ktoré reflektujú ich adekvátnu ochranu, tak nie je možné prakticky zabezpečiť bez riadenia prístupu na základe rolí (RBAC) a s tým súvisiacou správou identít (IdM).

Ide tiež o procesy a postupy, ktoré sú navrhnuté a realizované tak, **aby nedošlo ku kompromitácii OÚ**, ich úniku, či znehodnoteniu.

V procesnej oblasti treba pamätať na:

- upratanie dát, t.j. ich analýza a roztriedenie, minimalizácia, distribúcia, časové obmedzenie a pod.
- zavedené konkrétne postupy spracovávania a uchovávania dát (napr. životný cyklus spracovávania OÚ v matričných záznamoch, v elektronických spisoch tribunálu,...)
- technologické procesy (napr. konfigurácia a správa AIS, šifrovanie a pseudo-anonymizácia dát, monitoring IS a detekcia incidentov, uchovávanie záznamov, archivovanie a zálohovanie dát, realizácia bezpečnostných opatrení, vhodné vykonať, resp. vykonávať v pravidelných intervaloch audit, penetračné testovanie a pod.)
- vypracované plány s postupmi riešenia incidentov a testovanie ich funkcionality, čo je síce čiastočne obsiahnuté i v technologických procesoch, ale ich svojím rozsahom a povinnosťami aj presahuje (kap. 3.5)
- procesy v personálnej oblasti (kap. 2.3)

2.3. Personálne aspekty ochrany OÚ

S OÚ, ktoré sa v AIS nachádzajú, prichádzajú do kontaktu oprávnené osoby, resp. iné fyzické osoby na základe poverenie prevádzkovateľa či sprostredkovateľa. V personálnej oblasti treba zabezpečiť:

- poučenia o ochrane osobných údajov pre oprávnené a fyzické osoby, ktoré majú v rámci AIS prístup k OÚ
- pravidelné školenia informačnej bezpečnosti
- kontrolu dodržiavania záväzných nariadení a zákonov o OOÚ
- právne ošetrený monitoring používateľov, nie ich špehovanie[9]!!!

Povinnosť ochrany OÚ a z nej vyplávajúce požiadavky by mali byť zakomponované do pracovnej zmluvy oprávnených osôb.

AIS sú implementované a spravované nielen zamestnancami IKT prevádzkovateľa, resp. sprostredkovateľa, ale častokrát externými dodávateľmi, u ktorých treba zabezpečiť:

- analýzu, návrh, implementáciu, resp. konfiguráciu AIS na testovacích dátach, ktoré neobsahujú reálne OÚ
- v prípade nutnosti prístupu k OÚ prevádzkovateľa/sprostredkovateľa je treba nielen podpísať dohodu o mlčanlivosti (NDA), ale aj postupovať podľa Smernice KC

9 Napr. vzhľadom na využívanie *home office* (práca z domu/mimo pracoviska), prípadne využívanie *BYOD* (vlastné počítače, smartfóny, tablety v práci) býva u zamestnávateľov kvôli ochrane OÚ a monitorovaniu odpracovanej doby tendencia využívať invazívne monitorovacie prostriedky (screenshoty obrazovky, odchytávanie klávesnice, pohybov myši, či dokonca sledovanie pracovníka pomocou webkamery).
WP29, ktorá pripravuje vykonávacie pravidlá a výklady GDPR, však k tejto problematike vydala doporučenie, v ktorom upozorňuje, že takýto spôsob kontroly a ochrany OÚ je neprimeraný a zamestnávateľ si ho v prípade konfliktu neobháji.

2.4. Detekovanie bezpečnostných incidentov a ich nahlasovanie

ZOOÚ a GDPR ukladá povinnosť nahlasovať bezpečnostné incidenty, pri ktorých bola porušená ochrana OÚ, resp. prišlo k ich kompromitácii Úradu na ochranu osobných údajov (ÚOOÚ), pričom:

- ak pri bezpečnostnom incidente hrozí vysoké riziko pre práva jednotlivcov, je treba informovať aj dotknuté osoby o incidente a prípadných dopadoch úniku ich osobných údajov
- oznamuje sa takmer každé porušenie a bez zbytočného odkladu, najneskôr do 72 hodín (v tomto prípade však s odôvodnením, prečo to nebolo bez odkladu)

Podľa GDPR je vhodnou praxou v organizácii zavedenie **DPO**[10], ktorému je každý incident bezodkladne nahlásený a ktorý na základe svojich kompetencií sprocesuje jeho nahlásenie ÚOOÚ a pomôže určiť, či treba informovať aj dotknuté osoby.
Vzhľadom na organizačnú štruktúru Katolíckej cirkvi v Slovenskej republike a Smernicu KC sa javí ako najefektívnejšie realizovať spoločného DPO v rámci Konferencie biskupov Slovenska pre celú Cirkev i všetky právnické osoby, ktoré si odvodzujú svoju právnu subjektivitu od Katolíckej cirkvi.

10 DPO – Data Protection Officer nahrádza zodpovednú osobu zo staršej legislatívy. DPO musí byť riadne zapojená do všetkého ohľadom ochrany OÚ v organizácii a môže to byť nielen fyzická osoba, ale aj právnická osoba, resp. tím.

3. Technologické princípy a požiadavky ochrany OÚ v AIS

Základnou požiadavkou na automatizované informačné systémy tvorené prostriedkami IKT je **koncepčnosť**:

- koncepčnosť systémov, čo znamená ich **jasný dizajn v oblasti funkčnosti (procesná funkčnosť i robustnosť/spoľahlivosť), informačnej bezpečnosti a ochrany OÚ**
- koncepčnost spracovávaných dát a procesov, čo znamená **jasné vymedzenie spracovávaných dát a vymedzenie spôsobu ich spracovávania i archivovania prostriedkami IKT**
- koncepčnost prístupu k IKT v organizácii, čo znamená j**asný postoj k automatizovaným informačným systémom – potrebe a opodstateniu ich využívania, ich personálnemu, technologickému a finančnému zabezpečeniu**

3.1. Technologický dizajn

Požiadavky na technologický dizajn

- procesná funkčnosť
- robustnosť a spoľahlivosť
- bezpečnosť „by design and by default“
- ochrana OÚ „by design and by default“
- správa identít a rolí (identity management) a riadenie prístupu na základe rolí (role based access control)
- implementácia ďalších mechanizmov zabezpečujúcich požiadavky ZOOÚ/GDPR (monitorovanie, export, šifrovanie, pseudoanonymizácia a pod.)
- konfigurovateľnosť podľa požiadaviek nadefinovaných procesov, spoľahlivosti, systémovej bezpečnosti a ochrany OÚ
- správa AIS – administrácia, systémový monitoring, zálohovanie,...

3.2. Správa identít a rolí, riadenie prístupu na základe rolí

Role based access control (RBAC) – striktný „role based“ prístup k OÚ. Ide o riadenie prístupu k osobným údajom a ich spracovaniu na základe správy identít oprávnených osôb a definovania ich rolí (IdM – **identity management**), t.j. oprávnení v rámci informačných systémov (jasné vymedzenie kto a v akom rozsahu môže v informačnom systéme narábať s osobnými údajmi dotknutých osôb).

AIS musia podporovať správu identít a riadenie prístupu podľa rolí (kto a aký má prístup k OÚ podľa organizačnej štruktúry organizácie).

V prípade, že AIS správu identít a riadenie prístupu podľa rolí nepodporuje, je treba potrebnú funkcionalitu suplovať, napr. na úrovni operačného systému a pod.

3.3. Ochrana súkromia „by design and by default“

Privacy by design and by default (GDPR, čl. 25)

- analogicky „security by design and by default“ – bezpečnosť i ochrana OÚ musia byť súčasťou návrhu a realizácie informačného systému i procesov spracovávania dát. Prvky bezpečnosti a ochrany OÚ musia byť automaticky a štandardne zapnuté pri prevádzke AIS.
- týka sa procesov, t.j. spôsobov, ako sa OÚ spracovávajú
- týka sa informačných systémov, t.j. prostriedkov, pomocou ktorých sa OÚ spracovávajú

3.4. Monitorovanie a dokladovanie

Monitorovanie, t.j. zaznamenávanie/logovanie/ukladanie záznamov o tom, kto a kedy sa prihlásil, prípadne aké operácie s osobnými údajmi vykonával.

- povinnosť monitorovať a zaznamenávať (logovať) prístup k informačným systémom
- podľa povahy informačného systému, resp. spôsobou uloženia a spracovávania OÚ aj prípadná potreba monitorovať a zaznamenávať jednotlivé operácie s OÚ

Monitoring by design and by default

- analogicky „security/privacy by design and by default“ – mechanizmy monitorovania a zaznamenávania prístupu, resp. narábania s OÚ musia byť súčasťou návrhu a realizácie informačného systému i procesov spracovávania dát. Prvky monitorovania a zaznamenávania musia byť automaticky a štandardne zapnuté pri prevádzke AIS.

Dokladovanie prístupu a nakladania s OÚ

- povinnosť vedieť dokladovať na základe monitorovania a logovania spôsob narábania s OÚ
- povinnosť ukladať záznamy v zákonom stanovených lehotách
- pozor! – vlastné logovacie záznamy môžu obsahovať OÚ a treba sa k nim správať ako k AIS, na ktoré sa vzťahuje ZOOÚ/GDPR

3.5. Riešenie incidentov

Je potrebné mať vytvorené plány na riešenie incidentov:

- disaster recovery – obnovenie dát po havárii, úniku a poškodeniu dát
- spôsob oznamovania a riešenia incidentov v oblasti ochrany OÚ
- revokácia/blokovanie používateľov a rolí, zabránenie prístupu k OÚ osobám, ktoré na základe ukončenia svojho pracovného zaradenia, prípadne porušenia pravidiel ochrany OÚ by mali mať zablokovaný prístup do AIS

Je vhodné mať aj prakticky odskúšanú funkčnosť plánov a procesov riešenia incidentov, aby v prípade reálneho problému neprišlo k zbytočným výpadkom, strate, či úniku dát.

Incidenty, pri ktorých prišlo ku kompromitácii OÚ, treba hlásiť poverenému DPO (viď kap. 2.4). Incidenty, pri ktorých je podozrenie, že mohlo prísť ku kompromitácii OÚ, je vhodné minimálne skonzultovať s DPO.

4. Aplikácie a systémy *GDPR ready*

Je vhodné vytvoriť na celoslovenskej úrovni zoznam technológií (od operačných systémov až po aplikácie), ktoré spĺňajú podmienky stanovené ZOOÚ, GDPR a Smernicou KC.

Realizácia zoznamu je riešená interne členmi Pracovnej skupiny IKT pri GS KBS.

5. Príklad funkčnej a technologickej implementácie ochrany OÚ

Príklad funčnej i technologickej ochrany OÚ – implementácia zabezpečených poštových schránok Portálu elektronických služieb Katolíckej cirkvi ***ecclesia.sk*** tak, ako je realizovaná v Bratislavskej arcidiecéze, spolu so zabezpečením interných systémov Bratislavskej arcidiecézy – je na vyžiadanie k dispozícii pracovníkom Cirkvi, ktorí sú poverení správou informačných a komunikačných technológií.