Ochrana osobných údajov
GDPR v cirkevnom prostredí

Peter Šantavý
psantavy@abuba.sk

ecclesia

Ochrana osobných údajov (OOÚ)
GDPR v cirkevnom prostredí

Elektronizáciu procesov v cirkevnom prostredí sme začali seriózne implementovať v roku 2008, pričom jedným z najdôležitejších aspektov vyvíjaných riešení bola bezpečnosť a ochrana osobných údajov.

Prezentovaný stav riešenia ochrany osobných údajov v Bratislavskej arcidiecéze reflektuje nielen naplnenie našich zámerov v kontexte aktuálneho znenia Zákona o ochrane osobných údajov, ale aj kroky potrebné pre zabezpečenie kompatibility s GDPR.

Personal data protection
GDPR in the environment of the Catholic Church

Seriously we have begun to implement the electronization of the Catholic Church processes in 2008. Information security and personal data protection has been one of the most important aspects of the evolved solutions.

The presented state of the privacy solution in the Archdiocese of Bratislava reflects not only the fulfillment of our intentions in the context of the current wording of the personal data protection legislation, but also steps ensuring compatibility with the GDPR.

ecclesia

Ochrana osobných údajov

GDPR v cirkevnom prostredí

Peter Šantavý
psantavy@abuba.sk

ecclesia

Prečo sa zaoberať OOÚ?

- pracujeme s citlivými údajmi
  Od osobných údajov až po forum internum...
- tradícia *Loca credibilia*
  Verejné právnické inštitúcie, uznané bulou Ondreja II. z roku 1231.
  V sídlach biskupstiev, prepošstiev alebo konventoch:
  Bratislava, Nitra, Spišská Kapitula. Nemali obdobu nikde v Európe...
- realita informačnej kriminality
  Dôsledkom je takmer vždy strata, resp. zneužitie OÚ...
- legislatívne požiadavky
  Zákon č. 122/2013 Z. z. o ochrane osobných údajov.
  Zmena a doplnenie niektorých zákonov v znení zákona č. 84/2014 Z. z.

ecclesia

OOÚ je záležitosť

- právna
  – legislatívne požiadavky a ich aplikácia v organizácii
- procesná
  – nastavenie procesov tak, aby spĺňali právne a bezpečnostné požiadavky
- technologická
  – výber a implementácia technológií na realizáciu fungovania nastavených procesov
- personálna
  – vzdelávanie a formácia používateľov aj IT odborníkov v narábaní s OÚ
  – osvojovanie si bezpečnostných návykov
  - Komplexná ochrana OÚ je proces!

ecclesia

OOÚ v Bratislavskej arcidiecéze

- práca s OÚ podľa aktuálnej legislatívy
  Podľa § 21 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 84/2014 Z. z. (ďalej len Zákon o ochrane osobných údajov alebo ZOOÚ).

- príprava na aktualizáciu Zákona o ochrane osobných údajov a GDPR
  – právna a procesná
  – technologická

ecclesia

Osobné údaje (OÚ)

- OÚ identifikujú konkrétnu fyzickú osobu

  Definícia (§4 ods. 1 zákona č. 122/2013 Z. z.): „údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou 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“.

- OÚ je v zásade akákoľvek kombinácia údajov potrebných pre identifikáciu osoby

  – meno, priezvisko, adresa, titul
  – rasový alebo etnický pôvod, politické názory, vierovyznanie, svetonázor, členstvo v politickej strane, zdravotný stav, sexuálna orientácia, register trestov, rodné číslo, biometrické údaje, ...
  – rozsah údajov sa mení a dopĺňa
  – rozsah údajov môže byť dynamický podľa kontextu

ecclesia

Spracovávanie OÚ

- možnosti spracovávania OÚ
  – na základe súhlasu osoby/zákonného zástupcu
  – na základe zákona (upravuje získavanie, nakladanie i spracovávanie OÚ)
- kto pracuje s osobnými údajmi
  – prevádzkovateľ alebo sprostredkovateľ osobných údajov
  – patria k nim aj štátom uznané cirkvi
- čo je spracovávanie osobných údajov
  – vykonávanie operácií s osobnými údajmi
  – zákon základné vymenováva; prakticky akékoľvek narábanie s OÚ

Občan má právo na ochranu osobných údajov!

ecclesia

Povinnosti spracovávateľa OÚ

- vyplývajú zo zákonných noriem
  – aktuálne zákon č. 84/2014 Z. z., ktorým sa mení a dopĺňa zákon č. 122/2013 Z. z. o ochrane osobných údajov
  – ochrana osobných údajov
  – vymedzenie zodpovednosti
  – registrácia a evidencia informačných systémov (IS) spracúvajúcich OÚ
- IS OÚ nepodliehajúce registrácii
  – prevádzkovateľ je povinný viesť evidenciu a splniť ďalšie náležitosti:
    – vypracovanie bezpečnostného projektu/smernice
    – vypracovanie poučenia o povinnosti mlčanlivosti pre fyzické osoby
    – vypracovanie poučení oprávnených osôb
    – vypracovanie zmlúv so sprostredkovateľmi
    – vypracovanie evidenčných listov informačných systémov

ecclesia

Cirkev ako spracovávateľ OÚ

- aplikácia zákonných noriem:
  – identifikácia informačných systémov (IS) diecézy, farností, ...
  – riešenie IS, ktoré spracovávajú OÚ nečlenov Cirkvi, môžu spadať pod registráciu (sobášne matriky): ohlásenie zodpovednej osoby s náležitými skúškami a povereniami
  – vytvorenie bezpečnostného projektu a evidenčných listov IS
  – zabezpečenie poučenia oprávnených osôb pre prácu s IS (zodpovedná osoba, štatutár a ďalšie oprávnené osoby pracujúce s IS)
  – vytvorenie zmlúv so sprostredkovateľmi (externé firmy pre účtovníctvo, personalistiku,...)
  – zabezpečenie poučenia o povinnosti mlčanlivosti pre fyzické osoby
- každá organizácia (IČO) spracúvajúca OÚ
  – diecézy, farnosti, rehole, cirkevné organizácie...

ecclesia

Terminológia ZOOÚ

- zodpovedná osoba – je zodpovedná za ochranu OÚ organizácie
  – musí mať absolvované príslušné skúšky
  – musí byť poverená ako zodpovedná osoba pre danú organizáciu
  – musí byť poučená do úrovne podľa § 27 (nemusí mať plný prístup, musí vedieť zabezpečiť povinnosti vyplývajúce zo ZOOÚ)
- oprávnená osoba je osoba, ktorá prichádza do styku s OÚ v IS organizácie
  – štatutár je oprávnená osoba s plným prístupom ku všetkým IS organizácie
  – ostatné oprávnené osoby (na základe svojho zaradenia v organizácii) majú prístup k OÚ v IS v rámci svojho zaradenia
  – oprávnené osoby musia byť poučené pre prácu s IS
  – poučovať môže zodpovedná osoba a ju štatutár

ecclesia

Čo treba zabezpečiť na úrovni farnosti?

- nahlásenie zodpovednej osoby za farnosť
  – potvrdenie o skúškach, výpis z registra trestov, poverenie za farnosť, oznámenie prevádzkovateľa o poverení
- dokumentácia k IS spracovávajúcim OÚ
  – bezpečnostný projekt, evidenčné listy IS, sprostredkovateľské zmluvy (ak OÚ spracováva externý subjekt)
- poučenie oprávnených osôb
  – poučenie štatutárov a následne štatutármi ďalšie osoby vo farnostiach, evidencia záznamov o poučeniach
- doplnkové úkony
  – označenie priestorov s kamerovým systémom, tlačivá pre FO...

ecclesia

Čo a ako treba evidovať na úrovni farnosti?

- nahlásenie zodpovednej osoby za farnosť
  – kópia dokumentov nahlásených na Úrad pre ochranu osobných dajov
  – podací lístok, resp. doklad o nahlásení na ÚOOÚ
- dokumentácia k IS spracovávajúcim OÚ
  – bezpečnostný projekt, evidenčné listy IS, sprostredkovateľské zmluvy
- dokumentácia poučení oprávnených osôb pre prácu s IS
  – evidencia záznamov o poučeniach štatutárov a ďalších osôb
- voľba spôsobu evidencie
  – každá farnosť má svoju zložku OOÚ na ABÚ
  – možnosť viesť kópiu evidencie aj priamo vo farnosti

ecclesia

Procesy a OOÚ

- definovanie OÚ, úkonov a procesov
  – ako sa získavajú, spracovávajú a archivujú OÚ
- správa identít a definovanie rolí v IS
  – zavedenie správy identín a riadenia prístupu podľa rolí
  – kto a aký má prístup k OÚ podľa organizačnej štruktúry organizácie
  – kompatibilné so ZOOÚ / GDPR, rešpektujúce CIC
- záväzné nariadenia pre prácu s OÚ
  – pre všetkých, ktorí prichádzajú do styku s OÚ
- plány na riešenie incidentov
  – disaster recovery, oznamovanie incidentov,...
  – revokácia/blokovanie používateľov a rolí

ecclesia

Technologické aspekty OOÚ

- technologický dizajn IS
  – procesná funkčnosť
  – robustnosť a bezpečnosť „by design and by default“
  – správa identít a rolí (identity management)
- technologická kompatibilita IS
  – interoperabilita na ekleziálnej úrovni
  – implementácia mechanizmov zabezpečujúcich požiadavky ZOOÚ/GDPR
- konfigurácia IS
  – podľa požiadaviek nadefinovaných procesov, spoľahlivosti a ochrany OÚ
- správa IS
  – administrácia, monitoring, zálohovanie,...

ecclesia

Ľudský faktor a OOÚ

- dôležitosť ľudského faktora
  – z pohľadu informačnej bezpečnosti – je ľudský faktor najslabší?!?
  – z pohľadu procesného
- školenia a vzdelávanie v oblasti OOÚ
  – poučenia oprávnených a fyzických osôb
  – pravidelné školenia informačnej bezpečnosti
  – OOÚ zakomponovaná do pracovnej zmluvy
- kontrola a monitoring
  – kontrola dodržiavania záväzných nariadení a zákonov o OOÚ
  – monitoring činnosti IS, napr.:
    – behaviorálna analýza dátových tokov pomocou NextGen, IPS, IDS,...
    – monitoring používateľov – právne ošetrené, nie špehovanie!!!

ecclesia

Spôsob nasadenia v Bratislavskej arcidiecéze

- právne konzultácie s odborníkmi na OOÚ a vypracovanie základných dokumentov
  – analýza aktuálneho stavu, organizačnej štruktúry a procesov
  – identifikácie informačných systémov
  – príprava potrebnej dokumentácie
- aplikácia na Arcibiskupský úrad
  – pomerne jednoduché nasadenie vzľadom na procesy a IS ABÚ
- nasadenie vo farnostiach
  – vypracovanie dokumentov modelovej farnosti s celým spektrom IS a procesov
  – hierarchické nasadenie cez dekanáty (pozor na zákonné lehoty!)

ecclesia

Ochrana osobných údajov

GDPR v cirkevnom prostredí

Peter Šantavý
psantavy@abuba.sk

ecclesia

Čo je to GDPR?

- General Data Protection Regulation

  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: *https://www.lewik.org/dataset/136/*

- Právna sila nariadenia

  – nariadenie – smernica – rozhodnutia – odporúčania/stanoviská
  – má prednosť pred vnútroštátnym právom
  – všeobecne záväzné (pre všetkých)
  – neimplementuje sa, platí v takej forme, v akej ho prijala ERaP

- Platnosť a účinnosť

  – schválené 27. apríla 2016, platné od 17. mája 2016
  – účinnosť nadobúda 25. mája 2018

ecclesia

Čo GDPR obsahuje?

- Ochrana OÚ v celej šírke problematiky
  – na základe Charty základných práv EÚ (čl. 8, odsek 8): „Každý má právo na ochranu osobných údajov, ktoré sa ho týkajú“
  – povinnosti pre spracovávateľov OÚ: prevádzkovateľov i sprostredkovateľov
  – celá šírka spektra spracovávaných OÚ FO (Preambula – ods. 15): „... by mala byť ochrana technologicky neutrálna a nemala by závisieť od použitých technologických riešení“
- Pracovná skupina 29 (Working Party 29)
  – GDPR neposkytne žiadne konkrétne návody!
  – The Article 29 Data Protection Working Party je zodpovedná za prípravu metodík, návodov a názor na problematiku GDPR:
  http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
  – WP29: vykonávacie pravidlá a výklady GDPR

ecclesia

Širší kontext GDPR

- nariadenie GDPR
  – **G**eneral **D**ata **P**rotection **R**egulation
  – všeobecné nariadenie o ochrane údajov:
  http://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32016R0679&qid=1486657099840
- nariadenie eIDAS
  – **e**lectronic **ID**entification, **A**uthentication and trust **S**ervices
  – 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
- smernica NIS
  – **N**etwork and **I**nformation **S**ecurity
  – 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

ecclesia

Osobné údaje podľa GDPR

- Osobné údaje (čl. 4)
  – OÚ sú prakticky akékoľvek údaje týkajúce sa identifikovanej alebo identifikovateľnej (aj nepriamo) fyzickej osoby („dotknutá osoba“)
- Čo môže byť OÚ?
  – meno a/alebo priezvisko, vierovyznanie, stav, pohlavie,...
  – fotografia i záznam z kamerového systému
  – biometrický údaj (napr. odtlačok prsta, zvukový záznam hlasu,...)
  – telefónne číslo, číslo účtu, identifikátor v systéme
  – IP adresa, lokalizačné údaje (GPS, wifi+login,...)
  – množina OÚ sa výrazne rozširuje o údaje technického charakteru
- OÚ v našom kontexte: ZOOÚ vs. GDPR
  – analýza IS a procesov organizácie, na základe ktorej môžeme identifikovať celú množinu OÚ dotknutých osôb podľa GDPR

ecclesia

Zásady GDPR

- Zásady GDPR (čl. 5)
  - zákonnosť, spravodlivosť a transparentnosť
  - obmedzenie účelu
  - minimalizácia údajov
  - správnosť
  - minimalizácia uchovávania
  - integrita a dôvernosť
  - zodpovednosť prevádzkovateľa
- Prevádzkovateľ
  - je zodpovedný za dodržiavanie zásad GDPR
  - musí viesť záznamy o spracovávaní OÚ
  - musí byť schopný preukázať dodržiavanie legislatívy

ecclesia

Ďalšie povinnosti podľa GDPR

- Nahlasovanie bezpečnostných incidentov
  – povinnosť nahlasovať Úradu na ochranu OÚ
  – dotknutým osobám (ak hrozí vysoké riziko pre práva jednotlivcov)
  – oznamuje sa takmer každé porušenie a bez zbytočného odkladu, najneskôr do 72 hodín, no s odôvodnením, prečo to nebolo bez odkladu
- Implementačná povinnosť
  – povinnosť a zodpovednosť prevádzkovateľa i sprostredkovateľa
  – podľa GDPR ~ metodík, pravidiel a postupov WP29
- Zodpovedná osoba (~ZOOÚ)
  – DPO, Data Protection Officer
  – môže byť niele fyzická, ale aj právnická osoba
  – musí byť riadne zapojená do všetkého ohľadom OOÚ v organizácii
  – nie je zodpovedná za súlad s GDPR, tou je organizácia!

ecclesia

Dotknuté osoby a ich OÚ (1)

- Sprísnenie podmienok súhlasu
  – ak spracovávanie OÚ na základe súhlasu, nie zo zákona
  – súhlas musí byť konkrétny, slobodný, informovaný a jednoznačný
  – v zrozumiteľnej a ľahko dostupnej forme, formulácia jasná a jednoduchá
  – povinnosť prevádzkovateľa vedieť preukázať súhlas dotknutej osoby
  – explicitne, nie implicitne
  – dotknutá osoba má právo kedykoľvek odvolať svoj súhlas
  – spracovávanie OÚ osoby mladšej ako 16 rokov len so súhlasom zákonného zástupcu
- Právo na opravu a doplnenie (čl. 16)
  – právo na opravu OÚ; povinnosť bez zbytočného odkladu OÚ opraviť
  – právo na doplnenie neúplných OÚ, a to aj prostredníctvom poskytnutia doplnkového vyhlásenia

ecclesia

Dotknuté osoby a ich OÚ (2)

- Právo „byť zabudnutý“ (čl. 17)
  – ak sú OÚ spracovávané protizákonne alebo bezdôvodne
  – ak je súhlas odvolaný (netýka sa to OÚ zhromažďovaných na základe zákona)
  – pominul dôvod spracovávania OÚ
  – lehota 1 mesiac
  – technologická, právna i organizačná primeranosť a proporcionalita (napr. sociálne siete, vyhľadávače, technológie AI – deep learning, neural networks, learning machine,...)
  – výnimky, ak je silnejšie iné právo (sloboda slova, verejné zdravie)
- Právo na prenosnosť údajov (čl. 20)
  – právo získať svoje údaje v štruktúrovanom, bežne používanom formáte
  – právo na prenos od jedného prevádzkovateľa k druhému, ak je to technicky možné (telefónny operátor, bankový účet,...)

ecclesia

Dôsledky GDPR pre procesy a informačné systémy

- Koncepčnosť procesov a systémov
- Privacy by design and by default (čl. 25)
  – analogicky „security by design and by default“
  – týka sa procesov, t.j. spôsobov, ako sa OÚ spracovávajú
  – týka sa informačných systémov, t.j. prostriedkov, pomocou ktorých sa OÚ spracovávajú
  – striktný „role based“ prístup k OÚ (*role based access control* - na základe správy identít a definovania rolí)
- Niektoré pravidlá ochrany OÚ
  – pseudoanonymizácia OÚ
  – minimalizácia údajov (v spracovávaní a aj v čase)
  – procesné obmedzenie prístupu k OÚ na základe rolí
  – ochrana OÚ v IS (spôsob uloženia, šifrovanie, bezpečnostné certifikácie)

ecclesia

Praktické rady

- Oboznámenie sa s GDPR a WP29
  – štruktúrovaná verzia nariadenia:
  https://www.lewik.org/dataset/136/
- Implementácia Zákona o ochrane OÚ
  – zjednodušene povedané:
  GDPR rozširuje, aktualizuje a dopĺňa aktuálne znenie Zákona o OOÚ
  – vstúpi do platnosti aj nový Zákon o ochrane OÚ, ktorý
  – harmonizuje OOÚ s GDPR v Slovenskej republike
  – rieši aplikáciu GDPR v praxi, inštitúty a procesné pravidlá v kontexte slovenského právneho systému
- Realizácia OOÚ vo všetkých oblastiach
  – právnej – procesnej – technologickej – personálnej

ecclesia

Procesné rady (1)

- Definovanie OÚ a inventarizácia dát
  – identifikácia OÚ
  – určenie, kde sa nachádzajú
- Definovanie spracovávania dát
  – definovanie procesov
  – vyhodnotenie oprávnenosti spracovávania a potreby uchovávania dát
- Kategorizácia OÚ podľa rizikovosti
  – kategorizácia údajov podľa citlivosti
  – určenie, kto a v akom rozsahu k nim nutne potrebuje prístup
  – zavedenie správy identít a riadenia prístupu podľa rolí (IDM a RBAC)

ecclesia

Procesné rady (2)

- Zavedené konkrétne postupy
  - – záväzné interné nariadenia pre prácu s OÚ
  - – požadovaný monitoring, evidencia a dokladovanie
  - – riešená primeraná forma ochrany OÚ
  - – plány na riešenie incidentov
  - – udržiavanie potrebnej dokumentácie IS a procesov
- Schopnosť spolupracovať s Úradom OOÚ
  - – vedieť zdokladovať spôsob spracovávania OÚ
  - – byť pripravený reagovať na požiadavky ÚOOÚ a ZOOÚ, napr.:
    - – vykonať analýzu vplyvov na ochranu osobných údajov
    - – spolupracovať pri riešení požiadaviek dotknutých osôb
    - – spolupracovať pri riešení bezpečnostných incidentov

ecclesia

Technologické rady (1)

- Základné pravidlá
  – security by design and by default
  – privacy by design and by default
  – prakticky nutná implementácia IDM a RBAC (správy identít a riadenia prístupu podľa rolí)
- Principiálne rozhodnutia
  – výber technológií
    – technologické platformy
    – cloud? (ak áno, aký? + jeho zhoda s GDPR)
    – aplikačné systémy
      (funkcionalita a aktualizovanie v dlhodobej perspektíve, vendor lock-in)
  – principiálny dizajn technologického riešenia
  – výber spoľahlivých dodávateľov IKT a nastavenie zmluvných vzťahov

ecclesia

Technologické rady (2)

- Technologické dôsledky
  - integrovanie prvkov ochrany dát
    - šifrovanie a pseudoanonymizácia dát
    - DLP (data leak prevention) systémy, IPS
  - riadenie prístupu (IDM a RBAC)
  - archivovanie a zálohovanie dát
  - „primerané“ bezpečnostné opatrenia ako výsledok vykonanej analýzy rizík
  - monitoring systémov a detekcia incidentov (IDS)
  - nástroje riešenia incidentov
    - forézna analýza
    - analýza dát z detekčných systémov
    - reporting narušenia/úniku dát
  - uchovávanie záznamov
    - prevádzkové záznamy (logy)
    - záznamy o bezpečnostných incidentoch

ecclesia

Čo po nasadení riešenia?

- Personálne aspekty
  – poučenia oprávnených a fyzických osôb
  – pravidelné školenia informačnej bezpečnosti
  – kontrola dodržiavania záväzných nariadení a zákonov o OOÚ
  – právne ošetrený monitoring používateľov, nie ich špehovanie!!!
- Procesy a technologické aspekty
  – monitoring IS a detekcia incidentov
  – uchovávanie záznamov
  – archivovanie a zálohovanie dát
  – realizácia bezpečnostných opatrení
  – vhodné vykonať (vykonávať v pravidelných intervaloch) audit, penetračné testovanie a pod.
  - Komplexná ochrana OÚ je proces!

ecclesia

ĎAKUJEM ZA POZORNOSŤ

INFO@ECCLESIA.SK


ecclesia