# KOMUNIKÁCIA OSOBNÝCH ÚDAJOV S VEREJNOSŤOU
## (OSOBNÉ ÚDAJE V ELEKTRONICKOM STYKU S DOTKNUTÝMI OSOBAMI)

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 |
| IKT | informačné a komunikačné technológie |
| IS | informačný systém |
| OÚ | osobné údaje (osobný údaj) |
| OOÚ | ochrana osobných údajov |
| 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 |

Osobné údaje sa vo veľkej miere spracúvajú prostredníctvom automatizovaných informačných systémov (informačných a komunikačných technológií) i v prostredí Rímskokatolícke cirkvi, Gréckokatolíckej cirkvi a právnických osôb, ktoré si svoju právnu subjektivitu od nich odvodzujú.

Spracovanie osobných údajov dotknutých osôb v automatizovaných informačných systémoch sa riadi Zákonom 18/2018 Z.z. o ochrane osobných údajov a Nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov.

## 1. Pojem „komunikácia osobných údajov s verejnosťou“

V kontexte ochrany osobných údajov ide o komunikáciu s osobami, ktorej obsahom môžu byť osobné údaje dotknutých osôb. Ide o komunikáciu medzi internými informačnými systémami prevádzkovateľa (napr. poštová schránka podateľne biskupského úradu) a externými informačnými systémami (napr. poštová schránka farníka na gmail.com, centrum.sk, mojafirma.eu a pod.).

Automatizované informačné systémy prevádzkovateľa, ktoré sa na komunikáciu s verejnosťou využívajú, musia okrem náležitostí uvedených v tomto dokumente spĺňať primeranú ochranu dát, resp. technologické požiadavky uvedené v dokumente **Interné informačné systémy**.

## 2. Povinnosti pre prevádzkovateľov IS pre komunikáciu s verejnosťou

Základné pravidlo pre komunikáciu s verejnosťou:

**Osobné údaje nesmú byť súčasťou nezabezpečenej elektronickej komunikácie!**

Zabezpečená elektronická komunikácia by mala zahŕňať:
– **overenú identitu** komunikujúcej strany;
– **ochranu komunikovaných dát** pred kompromitáciou[1].

### 2.1. Zabezpečená emailová komunikácia – šifrovanie emailu s elektronickým podpisom

Zabezpečená emailová komunikácia s verejnosťou (t.j. mimo uzavretých interných informačných systémov) využíva možnosti tzv. elektronického podpisu, pomocou ktorého je možné komunikáciu šifrovať (chrániť komunikované dáta pred prečítaním) a podpísať (uviesť identitu a overiť neporušenosť správy). **Osobné údaje sú v tomto prípade posielané bezpečným spôsobom**.

Technologické riešenia zabezpečenej komunikácie s elektronickým podpisom:
– využitím technológií S/MIME alebo PGP;
– v budúcnosti prepojením interných elektronických systémov Katolíckej cirkvi na systémy štátnej správy (elektronické schránky na portáli Slovensko.Sk).

### 2.2. Zabezpečená emailová komunikácia – zaheslovaná / šifrovaná príloha emailu

Ide o emailovú komunikáciu s verejnosťou (t.j. mimo uzavretých interných informačných systémov) smerom k externým, resp. nezabezpečeným emailovým službám prijímateľa, v rámci ktorých sa **osobné údaje posielajú v zaheslovaných, resp. šifrovaných prílohách**.

Niektoré technologické riešenia pre posielanie zabezpečených príloh:
– posielanie prílohy vo formáte zaheslovaného dokumentu MS Office, LibreOffice a pod.;
– využitie externého zaheslovania a šifrovania, napr. šifrovaný zip súbor, zašifrovanie dokumentu pomocou aescrypt a pod.

Čo treba zabezpečiť pre zabezpečené posielanie šifrovanej prílohy:
– overenie emailovej adresy príjemcu (emailová adresa skutočne patrí osobe, s ktorou komunikujeme);
– zaslanie hesla na odomknutie, resp. dešifrovanie prílohy alternatívnou cestou (sms, telefonicky, osobne a pod.).

### 2.3. Nezabezpečená emailová komunikácia

Ak ide o emailovú komunikáciu s verejnosťou (t.j. mimo uzavretých interných informačných systémov), ktorá nevyužíva šifrovanie na základe elektronického podpisu alebo šifrovanie príloh, teda **ak ide o komunikáciu bežnými emailami, osobné údaje takto nemôžu byť posielané!**[2]

1 Pod kompromitáciou sa rozumie akýkoľvek únik, prezradenie, odpočúvanie, či zneužitie dát.
2 Napr. posielanie bežného emailu na centrum.sk, gmail.com, yahoo.com, post.sk, rôzne firemné emaily osôb a pod.

V prípade, že obsahom nezabezpečenej emailovej komunikácie je odpoveď na podnet osoby, ktorá vo svojom emaili sama uviedla osobné údaje, treba v odpovedi vymazať osobné údaje z tela pôvodného emailu.[3]

### 2.3. Komunikácia technológiou rýchlych správ

Komunikáciu pomocou rýchlych správ (rôzne typy messengerov) **vo všeobecnosti nie je možné považovať za bezpečnú**, primárne vzhľadom na možnosť prevádzkovateľa monitorovať obsah komunikácie a rôzne spôsoby ukladania histórie komunikácie.

**Výnimkou** sú systémy, ktoré umožňujú *end to end* šifrovanie komunikácie[4], pri ktorých však treba pamätať na overenú identitu komunikujúcej protistrany (s kým komunikujem).

### 2.4. Komunikácia cez diskusné fóra a sociálne siete

**Osobné údaje nesmú byť komunikované prostredníctvom sociálnych sietí, či rôznych diskusných fór.** Ide o platformy, ktorých prevádzkovatelia majú prístup k aktuálnemu obsahu i k jeho histórii, obsah môže byť ďalej spracúvaný/profilovaný, resp. v rôznych formách sprístupnený tretím stranám.

### 2.5. Využívanie cloudových služieb

**Využívanie cloudových služieb pre uloženie, resp. posielanie, či sprístupnenie osobných údajov nie je bezpečné**, nakoľko prevádzkovatelia týchto služieb majú prístup k aktuálnemu obsahu i k jeho histórii, pričom obsah môže byť ďalej spracúvaný/profilovaný, resp. v rôznych formách sprístupnený tretím stranám.

**Výnimkou** sú prípady, v ktorých sa protredníctvom cloudových služieb posielajú šifrované osobné údaje, t.j. údaje, ktoré sú lokálne na strane prevádzkovateľa zašifrované, na cloudovom úložisku sa nachádzajú len v tejto podobe, z úložiska sú adresátom stiahnuté a až lokálne u adresáta dešifrované. V tomto prípade treba splniť podmienky uvedené v bode 2.2.[5]

---

3 Napr. osoba žiada informáciu, či sa v matrike farnosti nachádza konkrétny krstný záznam, pričom uvedie osobné údaje ako napr. meno, priezvisko, dátum narodenia, prípadne rodičov a pod. Ak na email odpovedáme (Reply/Odpovedať/...), pričom v odpovedi máme skopírovný obsah pôvodného emailu, je treba vymazať osobné údaje, ktoré tam boli pôvodne uvedené.

4 Ide o komunikáciu prebiehajúcu medzi dvoma stranami (odosielateľ a príjemca) zabezpečujúcu šifrovanie priamo od odosielateľa až po príjemcu. Komunikáciu tak môžu prečítať práve len tieto dve strany a ako samotná komunikácia, tak správy v zariadeniach oboch strán sú chránené proti kompromitácii.

5 Požiadavky uvedené v časti *Niektoré technologické riešenia pre posielanie zabezpečených príloh* a v časti *Čo treba zabezpečiť pre zabezpečené posielanie šifrovanej prílohy.*