Směrnice o ochraně osobních údajů – průvodní dopis

Vážené sestry a vážení bratři,
v souvislosti s novým nařízením EU o ochraně osobních údajů (GDPR) přijala Ústřední rada CČSH Směrnici o ochraně osobních údajů v CČSH, kterou Vám tímto zasíláme. Je závazná pro všechny organizační složky CČSH. Účinnost směrnice je stanovena od 1. září 2018, aby bylo možné se s jejím obsahem seznámit a uvést současnou praxi zpracovávání osobních údajů v naší církvi do souladu s evropským nařízením.
Směrnice je poměrně komplikovaná, nicméně zásadních je těchto několik informací, kterým, prosím, věnujte pozornost:

Zásady zpracování osobních údajů

Stručně lze tyto zásady shrnout do několika bodů:
- osobní údaje zpracováváme pouze na základě daných právních titulů (viz dále) a v takové míře, v jaké je potřebujeme pro naši činnost; nezískáváme zbytečně údaje, které nepotřebujeme; údaje nezpracováváme déle, než je třeba
- osobní údaje by měly být zabezpečeny proti zneužití – to znamená například uloženy v uzamčené skříni nebo kanceláři, kam nemají přístup neoprávněné osoby; nebo uloženy v zaheslovaném počítači.

Záznamy o činnosti zpracování

Dle nového nařízení je povinností vypracovat ke každé činnosti zpracování tabulku – „Záznam o činnosti zpracování“ (viz Směrnice článek X.). Vzorová tabulka spolu s legendou je **přílohou č. 1** tohoto dopisu. Tyto záznamy se vyplňují pouze jednou za každý případ zpracování (například vedení kartotéky členů NO). V případě, že vznikne nový případ zpracování, je nutné o něm též vyplnit záznam. Každá diecéze bude na základě Směrnice jmenovat koordinátora pro ochranu OÚ. U těchto koordinátorů by měly být všechny záznamy shromážděny.

Souhlas se zpracováním osobních údajů

Zpracování osobních údajů (OÚ) je možné na základě několika právních titulů, mezi něž patří plnění zákonné povinnosti, plnění smlouvy, ochrana oprávněných zájmů správce, ochrana zájmů člověka (např. zdraví), výkon úkolů veřejné moci a udělení souhlasu se zpracováním osobních údajů. Ve většině případů zpracování osobních údajů v rámci CČSH k němu dochází buď na základě zákonné povinnosti, závazku ze smlouvy nebo oprávněného zájmu správce – tedy církve (např. vedení kartotéky členů církve). **V těchto případech není nutné získávat souhlas se zpracováním OÚ**. Případy, kdy tento souhlas je třeba, jsou v naší situaci poměrně ojedinělé - například zasílání newsletterů a pozvánek nebo zveřejňování údajů o narozeninách členů NO v církevním tisku.
Náležitosti souhlasu: Identifikace správce (například náboženská obec); žádost o zpracování údajů (vypsat, o které se jedná); uvést účel zpracování; poučení, že souhlas je zcela dobrovolný a lze jej kdykoliv odvolat (uvést způsob, jakým to lze učinit). Podpis osoby, která souhlas uděluje (měl by být vždy písemný) – viz **příloha č. 2**, kde jsou uvedeny i případy, ve kterých je souhlas potřeba.

Informace o zpracování osobních údajů

Na rozdíl od souhlasu je nutné ve všech případech informovat o tom, že zpracováváte osobní údaje, jaké to jsou, na základě jakého právního titulu (viz bod výše) a na koho je možné se v případě dotazu obrátit. Tuto informaci je třeba poskytovat ve chvíli, kdy OÚ získáváme – zahrnout ji tedy např. do smluv (pozor – ve smlouvě nesmí být souhlas se zpracováním OÚ, protože by nebyl svobodný) nebo vyvěsit na internetových stránkách, při osobním kontaktu jej předat písemně. Informaci lze podat formou otázek a odpovědí – viz **příloha č. 3**.

Na koho je možné se obrátit

Do doby, než budou jmenováni diecézní koordinátoři, je možné se s jakýmikoliv dotazy a nejasnostmi v této oblasti obracet na tajemnici ÚR Mgr. Janu Krajčiříkovou a vedoucího ÚÚR Ing. Jana Švábenického.

Jana Krajčiříková, tajemnice ÚR

Záznam o činnosti zpracování

Případ zpracování		
Stručný popis		
Správce	Náboženská obec	
	IČ	
	sídlo	
	kontakt	
Pověřenec	firma/jméno	
	IČ/dat. nar.	
	sídlo/kontaktní adresa	
	kontakt	
Účel zpracování		
Kategorie subjektů údajů		
Kategorie osobních údajů	podle GDPR	
	typově	
Kategorie příjemců		
Plánovaná lhůta pro výmaz a způsob jejího určení		
Opatření k ochraně OÚ	organizační opatření	
	bezpečnostní opatření	

Legenda:
Případ zpracování – vyberte pojmenování, které bude dané zpracování charakterizovat, např. vedení matrik, personalistika, uzavírání smluv
Stručný popis – v čem daný případ zpracování spočívá (např. „NO vede v souladu s řády CČSH knihu pokřtěných. Je vedena ve fyzické podobě a elektronicky na počítači na faře. Údaje jsou shromažďovány podle pokynu diecézní rady. “)
Správce – subjekt, který provádí zpracování osobních údajů, typicky např. náboženská obec
Pověřenec – pověřence bude na základě Směrnice jmenovat ÚR, kontakt na něj Vám bude sdělen
Účel zpracování – z jakého důvodu jsou osobní údaje v daném případě zpracovávány
Kategorie subjektů údajů – charakteristika skupin subjektů údajů, o kterých se osobní údaje shromažďují, např. členové náboženské obce, zaměstnanci
Kategorie osobních údajů podle GDPR – podle GDPR **-** základní, zvláštní kategorie (do zvláštní kategorie patří tzv. citlivé údaje podle čl. III. Směrnice – např. údaj o náboženském vyznání; osobní údaje jako jméno, datum narození, adresa, jsou základními os. údaji); typově – vyjmenovat konkrétní kategorie údajů – jméno, adresa, datum narození…
Kategorie příjemců – komu jsou osobní údaje případně předávány, např. státní orgány, církevní právnické osoby, obchodní partneři, …
Plánovaná lhůta pro výmaz a způsob jejího určení – podle čeho bude stanoveno, že mají být údaje vymazány (omezená doba souhlasu, vyprší potřeba je zpracovávat kvůli promlčecím dobám, údaje budou prokazatelně potřeba jen po omezenou dobu, …)
Opatření k ochraně OÚ: organizační opatření: např. omezení přístupu zaměstnanců, snížení oběhu údajů v rámci struktury správce, …
Opatření k ochraně OÚ: bezpečnostní opatření: např. použití zaheslovaných účtů, pravidelné zálohování, uchovávání odděleně od jiných dokumentů, …

Souhlas se zpracováním osobních údajů
(upravený vzor pro newslettery zasílané členům NO)

Vážená/ý ……..,

vážíme si toho, že s Náboženskou obcí CČSH …….. se sídlem …….. (dále jen „správce“) vstupujete do kontaktu a doufáme, že tak budete činit i nadále. Vzhledem k tomu, že si správce přeje zpracovávat Vaše osobní údaje také pro účely, které mu neukládá zákon, které nevyplývají z žádné smlouvy uzavřené s Vámi a které nejsou nezbytné pro ochranu oprávněných zájmů správce (například pro ochranu jeho majetku atd.), dovoluje si správce požádat Vás tímto o souhlas se zpracováním Vašich osobních údajů. Udělení souhlasu je čistě dobrovolné. Z jeho neudělení pro Vás neplynou žádné negativní důsledky a nic se pro Vás ve vztahu ke správci nemění. Správce pouze nebude moci využívat Vaše osobní údaje pro účely uvedené v tomto formuláři, ke kterým svůj souhlas neudělíte.

Správce si přeje využívat Vaše osobní údaje k následujícím účelům, ke kterým je nutný souhlas se zpracováním osobních údajů z Vaší strany:

☐ zasílání aktualit z NO a zvaní na akce pořádané NO a spřízněnými osobami
☐ zasílání přehledu nově vydaných publikací s křesťanskou tématikou
☐ zasílání aktualit s duchovní tématikou
☐ zasílání přání k svátku, narozeninám, Vánocům a Velikonocům
☐ zveřejňování blahopřání k svátku a k narozeninám na vývěsní desce NO
☐ zasílání nabídky volnočasových aktivit, kurzů a seznamu křesťanských spolků působících v NO
☐ zasílání rozpisu bohoslužeb v okolních NO
☐ zmínění svátků a narozenin při bohoslužbě
☐ zasílání informací o veřejných dobročinných sbírkách

Souhlas můžete udělit se všemi výše uvedenými účely zpracování Vašich osobních údajů, s některými z nich nebo s žádným. Svůj souhlas můžete kdykoli odvolat pomocí odkazu v každé zasílané e-mailové zprávě nebo přímo kontaktováním správce na tel. čísle …….. nebo e-mailem na adrese ……..

Pokud si přejete souhlas udělit, zaškrtněte příslušné políčko u konkrétního účely zpracování osobních údajů a vyplňte následující informace, které budou využity k Vaší identifikaci a pro daný účel zpracování osobních údajů:

Jméno a příjmení: ……..
Telefon: ……
E-mail: ……..

Já, níže podepsaná/ý …….. , dat. nar. ……., trvale bytem …….. tímto uděluji souhlas se zpracováním osobních údajů pro účely, které jsem výše vyznačil/a. Správce je oprávněn mne kontaktovat prostřednictvím ☐ pošty, ☐ telefonu, ☐ e-mailu.

V …… dne ……..

_____
podpis

Informace o zpracování osobních údajů

Vážený/á _____,

v souladu s článkem 13 nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“) si Vás dovolujeme informovat, že o Vaší osobě zpracováváme osobní údaje, které jste nám poskytl/a.

Kdo je správcem Vašich osobních údajů a jak jej můžete kontaktovat?

Správcem Vašich osobních údajů, tedy osobou, která rozhoduje o způsobu a účelu zpracování Vašich osobních údajů, je _____, IČ: _____ se sídlem _____ (dále jen „správce“). Správce můžete kontaktovat poštou na adrese sídla, osobě, prostřednictvím telefonu na čísle _____ nebo prostřednictvím e-mailu na adrese _____.

Jmenoval správce pověřence pro ochranu osobních údajů?

Ano, správce jmenoval v souladu se svými povinnostmi podle GDPR pověřence pro ochranu osobních údajů. Naším pověřencem je pan/í _____. Kontaktovat jej/ji můžete poštou na adrese _____, telefonicky na čísle _____ nebo prostřednictvím e-mailu na adrese _____.

Za jakým účelem Vaše osobní údaje zpracováváme?

Na základě čeho je správce oprávněn Vaše osobní údaje zpracovávat?

Je poskytnutí osobních údajů k těmto účelům zpracování zákonným nebo smluvním požadavkem?

Budou Vaše osobní údaje předávány jiným osobám?

Jak dlouho budou Vaše osobní údaje zpracovávány?

Jaká práva máte v souvislosti se zpracováním osobních údajů?

Kdykoli můžete požádat o sdělení, zda Vaše osobní údaje zpracováváme, a poskytnutí kopie všech osobních údajů, které o Vás zpracováváme. Pokud zjistíte, že Vaše osobní údaje, které zpracováváme, nejsou správné, můžete požadovat jejich opravu. Pokud máte za to, že bychom Vaše osobní údaje zpracovávat nadále neměli, můžete požadovat výmaz Vašich osobních údajů. Pokud nebudete s vyřešením Vaší žádosti spokojeni, můžete se obrátit se stížností na Úřad pro ochranu osobní údajů. V případech, kdy Vaše osobní údaje zpracováváme na základě Vašeho souhlasu, můžete souhlas kdykoli odvolat.

Dovolujeme si zdůraznit, že na základě uplatnění těchto práv Vám nehrozí žádné riziko. Je naším zájmem zpracovávat osobní údaje zákonně a řádně a nepoškozovat Vaše práva. Pokud máte pochybnosti, že se nám to daří, budeme rádi, když nás na to upozorníte.

Já, níže podepsaný/á _____, narozen/a dne _____, trvale bytem _____ svým podpisem stvrzuji, že mi byla poskytnuta informace o zpracování osobních údajů v souvislosti s _____.

Dne _____ _____

(podpis)

Směrnice upravující zpracování a ochranu osobních údajů v Církvi československé husitské

Úvodní ustanovení

Článek I.
Důvody úpravy

1. V souvislosti s nabytím účinnosti nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“) přijímá Ústřední rada Církve československé husitské (ÚR CČSH) tuto Směrnici upravující zpracování a ochranu osobních údajů v rámci CČSH (dále jen „Směrnice“).

Článek II.
Předmět úpravy a rozsah působnosti

1. Směrnice upravuje postupy zpracování a ochrany osobních údajů zpracovávaných jednotlivými organizačními složkami CČSH v rámci jejich činnosti jako správců a zpracovatelů a povinnosti zaměstnanců a dalších osob, podílejících se na zpracování osobních údajů, které jsou k nim v obdobném právním vztahu jako zaměstnanci.
2. Organizačními složkami CČSH se rozumí zejména Úřad ústřední rady CČSH, úřady jednotlivých diecézí CČSH, farní úřady CČSH, všechny církevní právnické osoby zřízené CČSH a všechny orgány CČSH, ustavené na základě příslušných řádů CČSH, které zpracovávají osobní údaje (například rada starších, diecézní rada, ústřední rada, právní rada, kárné a revizní výbory).
3. Směrnice se vztahuje na veškeré činnosti zpracování osobních údajů prováděné v rámci CČSH v postavení správce i zpracovatele a na všechny zaměstnance a osoby v obdobném právním vztahu k CČSH jako zaměstnanci.

Článek III.
Definice pojmů

1. Není-li dále stanoveno jinak, mají následující pojmy pro účely směrnice tento význam:
   a) **osobním údajem** se rozumí jakákoli informace o identifikované nebo identifikovatelné osobě; identifikovatelnou osobou je každá osoba, kterou lze identifikovat na základě konkrétního osobního údaje buď přímo, nebo ve spojení s jiným osobním údajem;
   b) **citlivými osobními údaji** se rozumí osobní údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické údaje, biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu či sexuálním životě nebo sexuální orientaci fyzické osoby a údaje o trestných činech a rozsudcích v trestních věcech;
   c) **důvěrnými osobními údaji** se rozumí takové osobní údaje, které fyzické osoby, kterých se týkají, považují za zvlášť významné pro svá práva a svobody;
   d) **subjektem údajů** se rozumí fyzická osoba, které se osobní údaje týkají; subjektem údajů není zesnulá fyzická osoba;

e) **zaměstnanci** se rozumí osoby ve služebním nebo pracovním poměru k CČSH, osoby vykonávající pro CČSH závislou práci na základě dohody o provedení práce nebo dohody o pracovní činnosti a jiné osoby v obdobném právním vztahu k CČSH jako osoby ve služebním nebo pracovním poměru.
f) **externí osobou** se rozumí osoba odlišná od pracovníka, zpracovatele a správce;
g) **zpracováním osobních údajů** se rozumí jakákoli operace nebo soubor operací prováděných s osobními údaji nebo jejich souborem, zejména jejich shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;
h) **činností zpracování** se rozumí soubor operací zpracování osobních údajů prováděných za jedním účelem;
i) **správcem osobních údajů** se rozumí osoba určující způsob a účel zpracování osobních údajů; zpracování osobních údajů prováděné zaměstnanci správce podle jeho pokynů se počítá jako zpracování osobních údajů prováděné správcem;
j) **zpracovatelem osobních údajů** se rozumí osoba odlišná od zaměstnance, která pro správce provádí zpracování osobních údajů;
k) **odpovědným zaměstnancem** se rozumí zaměstnanec dohlížející na dodržování právních předpisů a vnitřních předpisů CČSH u konkrétní činnosti zpracování a zodpovídající za jejich dodržování.
l) **počítačem** se rozumí stolní počítač, notebook, tablet, chytrý telefon a jakékoli obdobné zařízení umožňující pracovat s osobními údaji v elektronické formě.
m) pokud je ve Směrnici použit výraz **farář**, rozumí se tím také administrátor; co je dále stanoveno o faráři platí v případě jiných právnických osob o členu statuárního orgánu;
n) **spolupracujícím laikem** se rozumí člen CČSH, který není ve služebním ani obdobném poměru k CČSH, ale ze své vlastní svobodné vůle pro ni vykonává činnosti.

Základní povinnosti

Článek IV.
Zásady zpracování

1. Všechny organizační složky CČSH provádějí zpracování osobních údajů pouze na základě zákonného titulu pro zpracování ve smyslu čl. 6 GDPR a pouze pro účely, pro které byly osobní údaje shromážděny. Pro jiný účel mohou být osobní údaje zpracovávány pouze na základě souhlasu subjektu údajů, zákonné povinnosti stanovené právem České republiky nebo Evropské unie, nebo pokud jsou naplněny podmínky podle čl. 6 odst. 4 GDPR.
2. Zpracování osobních údajů je přípustné pouze za dodržení zásad zákonného zpracování ve smyslu čl. 5 GDPR. CČSH dbá o spravedlivé a transparentní zacházení se subjekty údajů a jejich osobními údaji a o dodržování práv subjektů údajů.
3. Osobní údaje mohou být shromažďovány a zpracovávány pouze pro konkrétně stanovený účel a pouze v rozsahu a způsobem, který je nezbytný pro dosažení stanoveného účelu.
4. Osobní údaje nejsou zpracovávány po dobu delší, než je nezbytně nutné. Doba uchování jednotlivých druhů dokumentů obsahujících osobní údaje se řídí platnými právními předpisy České republiky a Evropské unie a zvláštní vnitřní směrnicí CČSH a dalšími předpisy církve.

5. Pokud jsou osobní údaje zpracovávány na základě souhlasu subjektu údajů, dbají zaměstnanci o to, aby byl udělený souhlas svobodný a informovaný. Zakazuje se uvádět souhlasy se zpracováním osobních údajů do smluv, obchodních podmínek a jiných dokumentů, v jejichž rámci by neudělení souhlasu mělo negativní následky pro subjekt údajů.
6. V případě zjištění, že zpracování osobních údajů v rámci CČSH nesplňuje v některém případě některou ze zásad, bude zpracování osobních údajů až do vyřešení nedostatku omezeno. Nelze-li nedostatek odstranit, bude zpracování ukončeno.
7. CČSH dbá při zpracování osobních údajů na dodržování svých povinností v oblasti zabezpečení osobních údajů ve smyslu čl. 24, 25 a 32 GDPR a dalších ustanovení ukládajících CČSH povinnosti jako správci nebo zpracovateli osobních údajů.
8. Při zavádění opatření k ochraně osobních údajů je dbáno na to, aby byla opatření přiměřená povaze zpracování osobních údajů, kategorii a množství zpracovávaných osobních údajů a míře rizika, které při zpracování osobních údajů hrozí, a to jak z pohledu pravděpodobnosti vzniku újmy pro subjekty údajů, tak její potenciální výši.

Článek V.
Pověření zaměstnanců

1. Ústřední rada CČSH a jednotlivé diecézní rady CČSH jmenují koordinátory GDPR. Úkoly koordinátora GDPR jsou:
   a) zajišťovat jednotnost procesů zpracování osobních údajů v rámci celé organizační struktury ústředí církve a jejích diecézí,
   b) sjednocovat postupy odpovědných zaměstnanců,
   c) přijímat a vyhodnocovat podněty a informace zaměstnanců a pověřence pro ochranu osobních údajů ve věci ochrany osobních údajů, hrozících rizik a zkvalitnění procesů zpracování,
   d) předkládat vyhodnocené podněty a informace podle písm. c) s doporučeními ústřední, resp. diecézní radě,
   e) koordinovat zavádění nových procesů a opatření týkajících se zpracování osobních údajů do praxe,
   f) vyhodnocovat připomínky k analýze rizik v rámci zavádění záměrné a standardní ochrany osobních údajů,
   g) vést evidenci záznamů o činnostech zpracování, seznamů zaměstnanců, vnitřních předpisů týkajících se ochrany osobních údajů, analýz rizik a dalších dokumentů vypracovávaných podle Směrnice nebo GDPR v souvislosti s ochranou osobních údajů,
   h) sloužit jako kontaktní místo pro subjekty údajů ve věcech souvisejících se zpracováním jejich osobních údajů,
   i) koordinovat vyřizování žádostí subjektů údajů o uplatnění jejich práv,
   j) vést evidenci žádostí subjektů údajů o uplatnění práv a reakcí na ně.
2. Funkci koordinátora GDPR vždy vykonává vedoucí zaměstnanec. Diecézní koordinátor GDPR vykonává svoji funkci také ve vztahu k náboženským obcím a dalším církevním právnickým osobám v rámci diecéze.
3. Pro každou činnost zpracování je určen odpovědný zaměstnanec. Úkoly odpovědného zaměstnance jsou:
   a) dohlížet na dodržování GDPR a tohoto předpisu v rámci jim svěřených činností zpracování,
   b) ukládat zaměstnancům úkoly související s jim svěřenou činností zpracování,
   c) vypracovávat posouzení vlivu činnosti na ochranu osobních údajů,

d) vypracovávat analýzu rizik v rámci zavádění záměrné a standardní ochrany osobních údajů,
e) spolupracovat s pověřencem pro ochranu osobních údajů a koordinátorem GDPR na řešení incidentů porušení zabezpečení, zlepšování úrovně ochrany osobních údajů a zavádění nových procesů a na vyřizování žádostí subjektů údajů o uplatnění práv.

Článek VI.
Povinnosti zaměstnanců

1. Zaměstnancům je zakázáno provádět jménem CČSH jakékoli zpracování osobních údajů, které jim nebylo přímo uloženo v rámci jejich pracovního nebo obdobného poměru. Zaměstnanci zpracovávají osobní údaje výhradně jen stanoveným způsobem a ve stanoveném rozsahu.
2. Zaměstnancům je zakázáno předávat osobní údaje zpracovávané v rámci CČSH třetím osobám, pokud jim to neukládá právní předpis České republiky nebo Evropské unie nebo jim to nevyplývá z jejich pracovní náplně nebo jim to není přímo uloženo v rámci jejich pracovního nebo obdobného poměru.
3. Zaměstnanci jsou povinni zachovávat mlčenlivost o všech skutečnostech, o kterých se v rámci zpracování osobních údajů dozvědí, a to i po skončení služebního nebo pracovního poměru. Tím nejsou dotčeny jejich povinnosti vyplývající z jiných právních předpisů.
4. V rámci zpracování osobních údajů dbají zaměstnanci na to, aby k dokumentům obsahujícím osobní údaje neměly přístup neoprávněné osoby, ať již zaměstnanci CČSH nebo jiné osoby.
5. Zaměstnanci jsou povinni seznámit se s příslušnými ustanoveními GDPR, dodržovat vnitřní předpisy CČSH dotýkající se ochrany osobních údajů, zejména tuto Směrnici, spisový a skartační řád a předpisy o využívání informačních systémů.
6. V rámci uloženého zpracování osobních údajů zaměstnanci průběžně kontrolují, zda jsou zpracovávané osobní údaje přesné, zda jsou pro daný účel potřebné a zda pro dosažení účelu zpracování není potřeba zpracovávat další osobní údaje. V případě zjištění nepřesnosti osobních údajů jsou zaměstnanci povinni vyvinout úsilí k nápravě tohoto stavu. V případě, že jsou zpracovávané osobní údaje nadbytečné nebo jsou potřebné další osobní údaje, vyrozumí o tom zaměstnanci odpovědného zaměstnance.
7. Osobní údaje uvedené v knihách pokřtěných, oddaných a zesnulých jsou zapisovány na formulářích stanovených ústřední radou. Pracovníci jsou povinni používat aktuální verzi formulářů.

Článek VII.
Pověřenec pro ochranu osobních údajů

1. Ústřední rada CČSH jmenuje pověřence pro ochranu osobních údajů.
2. Pověřenec pro ochranu osobních údajů může být zaměstnanec CČSH nebo osoba plnící funkci pověřence na základě jiného právního vztahu („externí osoba“).
3. Koordinátoři GDPR slouží jako prostředníci mezi pověřencem pro ochranu osobních údajů a diecézemi.
4. Pověřenec pro ochranu osobních údajů plní následující úkoly:
   a) prostřednictvím koordinátorů GDPR poskytuje poradenství zaměstnancům CČSH v otázkách souvisejících se zpracováním osobních údajů,
   b) dohlíží na dodržování právních předpisů České republiky a Evropské unie, týkajících se zpracování osobních údajů, a této Směrnice,

c) vypracovává stanovisko k posouzení vlivu činnosti na ochranu osobních údajů,
d) spolupracuje s Úřadem pro ochranu osobních údajů a slouží jako jeho kontaktní místo,
e) spolupracuje při vyřizování žádostí subjektů údajů o uplatnění jejich práv,
f) jednou ročně vypracovává soubornou zprávu o stavu ochrany osobních údajů pro potřeby CČSH

5. Pověřenec pro ochranu osobních údajů je oprávněn při zjištění závažného pochybení při zpracování osobních údajů spočívajícího v chybném nastavení procesů nebo bezpečnostních opatření přikázat zaměstnancům pozastavit zpracování osobních údajů. V takovém případě okamžitě informuje vedoucího zaměstnance oddělení, v jehož rámci ke zpracování osobních údajů dochází, a statutární orgán. Do vyřešení zjištěného problému nemůže být rozhodnuto o obnovení zpracování osobních údajů.
6. Zaměstnanci jsou povinni poskytnout pověřenci pro ochranu osobních údajů maximální součinnost při plnění jeho úkolů a řídí se jeho pokyny při vyřizování žádostí subjektů údajů a při omezení zpracování podle bodu 7.5 Směrnice.

Článek VIII.
Externí zpracovatelé

1. Je-li nezbytné využít při zpracování osobních údajů služeb externího zpracovatele, bude uzavřena s externím zpracovatelem smlouva o zpracování osobních údajů. Smlouva specifikuje činnost zpracovatele a obsahuje náležitosti podle čl. 28 GDPR.
2. CČSH dbá při výběru zpracovatele na jeho důvěryhodnost a požaduje záruky, že bude dodržovat všechna ustanovení GDPR, zejména že bude dbát o ochranu osobních údajů a vyvine vůči CČSH veškerou potřebnou součinnost při řešení žádostí subjektů údajů a při řešení incidentů porušení zabezpečení.
3. Zpracovatel se ve smlouvě o zpracování osobních údajů zaváže k zajištění srovnatelného nebo vyššího standardu ochrany osobních údajů, jaký požaduje tato Směrnice.
4. V případě využívání služeb spolupracujících laiků, jsou tito povinni zavázat se k dodržování pravidel ochrany osobních údajů – formou smlouvy nebo jednostranným prohlášením o ochraně osobních údajů – jinak nelze jejich služeb při činnosti vyžadující přístup k osobním údajům využít.

Článek IX.
Posouzení vlivu činnosti zpracování na ochranu osobních údajů

1. V případě, že CČSH rozhodne o zahájení činnosti, k níž je nutné provádět zpracování osobních údajů, určí osoba, která o zahájení činnosti a způsobu jejího provádění rozhodla, odpovědného zaměstnance.
2. Odpovědný zaměstnanec vypracuje posouzení vlivu činnosti zpracování na ochranu osobních údajů ve smyslu čl. 35 GDPR nebo na základě výjimek stanovených v GDPR určí, že posouzení není třeba vypracovávat.
3. Ustanovení bodu 9.1 a 9.2 platí obdobně, pokud CČSH rozhodne o zavedení nové technologie v rámci stávajících činností zpracování osobních údajů.
4. Posouzení vlivu činnosti zpracování na ochranu osobních údajů je předáno k přezkoumání pověřenci pro ochranu osobních údajů, který k němu zaujme ve lhůtě 3 týdnů stanovisko a předá posouzení a stanovisko osobě, která o zahájení činnosti rozhodla, a koordinátorovi GDPR.

5. Osoba, která rozhodla o zahájení činnosti, dbá na doporučení pověřence pro ochranu osobních údajů obsažená ve stanovisku podle tohoto bodu a přijme patřičná opatření. Pokud se od doporučení odchýlí, je povinna toto odchýlení podrobně zdůvodnit. O přijatých opatřeních a odůvodnění odchýlení informuje koordinátora GDPR.
6. Je-li na základě posouzení pravděpodobné, že činnost zpracování osobních údajů nese rizika pro práva a svobody subjektů údajů, pověří osoba, která o zahájení činnosti rozhodla, ve spolupráci s příslušným statutárním orgánem CČSH a koordinátorem GDPR zaměstnance příslušných organizačních útvarů, aby navrhli opatření k odstranění nebo zmírnění rizik.
7. Není-li možné snížit rizika na přiměřenou úroveň, přehodnotí osoba, která o zahájení činnosti rozhodla, své rozhodnutí a navrhne úpravu zahajované činnosti tak, aby bylo zpracování osobních údajů omezeno.
8. Není-li možné postupovat podle bodu 9.7, požádá příslušná organizační složka CČSH ve spolupráci s pověřencem pro ochranu osobních údajů o předchozí konzultaci Úřad pro ochranu osobních údajů.

Článek X.
Záznamy o činnosti zpracování

1. O každé činnosti zpracování je vypracován záznam o činnosti zpracování.
2. Záznam o činnosti zpracování obsahuje:
   a) jméno zaměstnance, který záznam vypracoval,
   b) roli zaměstnance, který záznam vypracoval,
   c) datum vypracování záznamu,
   d) jméno a kontaktní údaje správce,
   e) jméno a kontaktní údaje pověřence pro ochranu osobních údajů,
   f) účely zpracování,
   g) kategorie subjektů údajů,
   h) kategorie osobních údajů,
   i) kategorie příjemců osobních údajů,
   j) plánované lhůty pro uchování osobních údajů,
   k) obecný popis technických a organizačních opatření na ochranu osobních údajů,
   l) informaci o případném předání osobních údajů do třetí země.
3. Záznamy vypracovává odpovědný zaměstnanec a předává je koordinátorovi GDPR.
4. V případě změny v činnosti zpracování vypracuje odpovědný zaměstnanec aktualizovaný záznam o činnosti zpracování, který předá koordinátorovi GDPR. Původní záznam o činnosti zpracování je nadále uchováván. Aktualizované záznamy o činnosti zpracování jsou číslovány vzestupnou řadou.
5. Záznamy dle tohoto článku se uchovávají po dobu 10 let po ukončení činnosti zpracování.

Článek XI.
Seznamy zaměstnanců

1. Odpovědný zaměstnanec sestavuje seznam zaměstnanců, kteří se podílejí na činnosti zpracování.
2. Seznam obsahuje:
   a) označení činnosti zpracování,
   b) jméno zaměstnance,
   c) zařazení zaměstnance,

d) roli zaměstnance ve smyslu článku XIII.,
e) úkoly zaměstnance v rámci činnosti zpracování.

3. Kopii seznamů předá odpovědný zaměstnanec koordinátorovi GDPR.

Organizační a bezpečnostní opatření

Článek XII.
Záměrná a standardní ochrana osobních údajů

1. Součástí zavádění nové činnosti zpracování osobních údajů nebo nové technologie zpracování je zavedení přiměřených opatření k zajištění ochrany osobních údajů v rámci jednotlivých úkonů zpracování osobních údajů pro účely této činnosti.
2. Opatření podle bodu 1 zahrnují určení zaměstnanců, kteří se budou na činnosti zpracování podílet, podrobení zpracování opatřením zavedeným jako základní úroveň zabezpečení pro všechny činnosti zpracování prováděné CČSH a zavedení nových opatření pro zamezení rizikům souvisejícím s konkrétní zaváděnou činností zpracování.
3. Pro stanovení rizik podle bodu 2 vypracuje odpovědný zaměstnanec analýzu rizik. Analýza rizik se provádí v případě, že nebylo provedeno posouzení vlivu činnosti na ochranu osobních údajů podle čl. IX.
4. Analýza rizik obsahuje přinejmenším:
   a) popis jednotlivých úkonů zpracování v rámci činnosti zpracování,
   b) hrozby pro ochranu osobních údajů při jednotlivých úkonech zpracování,
   c) posouzení pravděpodobnosti nastání jednotlivých hrozeb,
   d) posouzení míry újmy plynoucí z jednotlivých hrozeb,
   e) stanovení míry rizika plynoucího z jednotlivých hrozeb,
   f) návrh opatření k odstranění nebo snížení hrozeb.
5. Pravděpodobnost nastání hrozby a míra újmy z hrozby plynoucí se hodnotí na stupnici 1-5. Stupeň pět představuje nejvyšší stupeň pravděpodobnosti nastání hrozby a míry újmy. Míra rizika se stanoví jako součin těchto dvou hodnot.
6. Odpovědný zaměstnanec předává analýzu rizik k vyjádření pověřenci pro ochranu osobních údajů a koordinátorovi GDPR.
7. Do okamžiku provedení analýzy rizik a zavedení všech potřebných opatření není možné započít s činností zpracování.

Článek XIII.
Přiřazení rolí

1. Každému zaměstnanci je na základě jeho pracovní pozice a zařazení v organizačním řádu přiřazena role.
2. Role definuje okruh dokumentů, ke kterým je zaměstnanci poskytnut přístup, a to jak v elektronické, tak ve fyzické podobě.
3. Role spravuje a přiřazuje vedoucí pracovník IT oddělení na základě informací poskytnutých mu personálním oddělením a jednotlivými odpovědnými zaměstnanci.
4. Role jsou pravidelně aktualizovány s ohledem na změny v činnostech zpracování.

Článek XIV.
Obecná pravidla přístupu k osobním údajům

1. Přístup k dokumentům obsahujícím osobní údaje je omezen pouze na zaměstnance, kteří s nimi musejí nezbytně pracovat pro plnění svých pracovních úkolů.
2. Přístup k dokumentům obsahujícím osobní údaje v elektronické podobě je řízen na základě přiřazení rolí jednotlivým zaměstnancům podle článku XIII. Základní úroveň přístupu k dokumentům je nulová. Na základě přiřazení rolí jsou zaměstnancům zpřístupňovány jednotlivé druhy dokumentů.
3. Zaměstnanci přistupují k dokumentům v elektronické podobě na základě přihlášení se k uživatelskému účtu. Každý zaměstnanec má přiřazenou jednu identitu spojenou s uživatelským účtem, která je totožná pro všechny informační systémy používané v příslušné organizační složce CČSH.
4. Není-li možné zajistit jednotnou identitu pro všechny informační systémy a aplikace ve smyslu bodu 3, jsou přijata technická opatření k tomu, aby bylo uživatelské jméno každého zaměstnance v jednotlivých informačních systémech a aplikacích vždy jednoznačně přiřaditelné ke konkrétnímu zaměstnanci.
5. Pro přihlášení se k uživatelskému účtu je zaměstnanec povinen využívat silné heslo. Silné heslo je tvořeno alespoň osmi znaky a obsahuje alespoň tři ze čtyř následujících typů znaků: velká a malá písmena, čísla, nealfabetické znaky.
6. Zakazuje se zapisovat přístupová hesla ve fyzické i elektronické podobě a sdělovat je jiným zaměstnancům a externím osobám.
7. Veškeré případy přístupu k dokumentům obsahujícím osobní údaje v elektronické podobě jsou zaznamenávány pomocí logování. Logy obsahují mimo jiné informaci, ze kterého uživatelského účtu došlo k přístupu k dokumentu, kdy k přístupu došlo a v čem přístup spočíval.
8. Přístup k dokumentům obsahujícím osobní údaje ve fyzické podobě je řízen na základě rolí ve smyslu článku XIII.
9. V případě, že k dokumentům ve fyzické podobě chce přistoupit zaměstnanec, jehož role to neumožňuje, je zaměstnanec, který je za dokumenty zodpovědný, povinen zjistit, zda byl zaměstnanec, byť přechodně přístupem k dokumentům pověřen. V případě, že pověřen nebyl, nebude zaměstnanci přístup umožněn.
10. O veškerých úkonech s dokumenty, které provádí zaměstnanec, jehož role to neumožňuje, se pořizují záznamy, které tvoří součást příslušného spisu.

Článek XV.
Zóny fyzického přístupu

1. Každý objekt využívaný v rámci jednotlivých organizačních složek zcela nebo z části k administrativním účelům bude rozdělen na přístupové zóny s odstupňovaným zabezpečením a omezením přístupu.
2. Do veřejné zóny spadají prostory přístupné pro externí osoby bez omezení. V této zóně je zakázáno uchovávat osobní údaje s výjimkou nezbytných případů a v nutném rozsahu a za předpokladu, že jsou zavedena dostatečná bezpečnostní opatření.

3. Vnitřní zóna zahrnuje prostory ve vnitřním objektu, ve kterých se samostatně pohybují pouze zaměstnanci. Vstup do této zóny je umožněn pouze za použití klíče nebo identifikační čipové karty. Pohyb externích osob včetně dodavatelů služeb je ve vnitřní zóně umožněn pouze v doprovodu zaměstnance.
4. Ochranná bezpečnostní zóna zahrnuje prostory sloužící k uchovávání citlivých osobních údajů a důvěrných osobních údajů a informací a dokumentů, jejichž neoprávněné zveřejnění by mohlo příslušné organizační složce CČSH nebo jiným osobám způsobit závažnou újmu. Do ochranné bezpečnostní zóny je povolen vstup pouze zaměstnancům, jejichž náplň práce souvisí s dokumenty a informacemi zde uchovávanými.
5. Vstup do ochranné bezpečnostní zóny je vždy opatřen mechanickým nebo elektronickým zámkem. Zaměstnanci jsou povinni tento vstup uzamykat.
6. Serverovna a další prostory, ve kterých se nacházejí úložiště velkého množství osobních údajů v elektronické podobě, vždy spadají do ochranné bezpečnostní zóny.
7. Rozsah a rozložení jednotlivých zón a podrobná pravidla pro přístup do nich stanoví koordinátor GDPR ve spolupráci s vedoucími pracovníky a po konzultaci se správcem budovy.
8. Koordinátor GDPR zajistí distribuci informací o rozložení zón a pravidlech přístupu do nich mezi zaměstnanci.
9. Neoprávněné šíření informací podle tohoto článku představuje bezpečnostní riziko pro CČSH a může být posouzeno jako porušení povinnosti zaměstnance.

Článek XVI.
Fyzická bezpečnost osobních údajů

1. Prostory, ve kterých dochází ke zpracování osobních údajů, se až na výjimky stanovené touto Směrnicí nalézají vždy ve vnitřní zóně nebo v ochranné bezpečnostní zóně.
2. Zaměstnanci dbají na základní pravidla bezpečnosti, zejména při odchodu z prostor pečlivě zamykají dveře a kontrolují zavření oken.
3. Externí osoby nesmějí být ponechány v prostorách podle bodu 1 bez dozoru zaměstnance.
4. Při odchodu z prostor podle bodu 1 je zaměstnanec povinen zajistit, aby k jeho uživatelskému účtu nemohla přistoupit třetí osoba, například spuštěním spořiče obrazovky, který pro obnovení vyžaduje zadání uživatelského hesla.
5. Na všech počítačích, noteboocích a tabletech je nastaveno automatické uzamykání obrazovky s nutností opětovného zadání uživatelského hesla při nečinnosti delší než 10 minut.
6. V okamžiku skončení pracovní doby je zaměstnanec povinen odhlásit se ze všech informačních systémů, které využívá, a odhlásit uživatelský účet na pracovním počítači.

Článek XVII.
Uchovávání fyzických dokumentů obsahujících osobní údaje

1. Fyzické dokumenty obsahující osobní údaje jsou uchovávány v kancelářích, které jsou využívány zaměstnanci provádějícími danou činnost zpracování, nebo v jiných k tomu určených prostorách.
2. Veškeré fyzické dokumenty obsahující osobní údaje jsou v době, kdy nejsou přímo využívány, uloženy v uzamykatelných skříních nebo uzamčených kancelářích.
3. Dokumenty jsou seskupovány podle činnosti zpracování, ke které slouží. Dokumenty sloužící různým činnostem zpracování se nemísí.

4. Složky dokumentů jsou viditelně označeny štítkem, na kterém je uveden název činnosti zpracování.
5. Složky dokumentů obsahují záznam o nahlížení do dokumentů, ve kterém se uvádí označení dokumentu, do kterého bylo nahlíženo, nahlížející osoba, osoba, která nahlížení umožnila, účel nahlížení a datum nahlížení.
6. Složky dokumentů dále obsahují seznam kopií dokumentů s datem pořízení a místem jejich uložení.

Článek XVIII.
Bezpečnost informačních systémů a zálohování

1. IT oddělení vypracovává pro jednotlivé informační systémy a datová úložiště dokumentaci popisující bezpečnostní opatření zavedená pro daný systém nebo úložiště.
2. Bezpečnostní opatření zahrnují mimo jiné řízení přístupu, šifrování, pseudonymizaci nebo používání antivirových programů.
3. Dokumentace obsahuje rovněž popis postupu obnovení dat při incidentu porušení zabezpečení spolu se lhůtami pro toto obnovení. Lhůty se stanovují podle úrovně důležitosti dat zpracovávaných v daném informačním systému nebo na daném úložišti.
4. IT oddělení stanoví způsob zálohování jednotlivých informačních systémů a datových úložišť a dobu uchování záloh.
5. Pokud to možnosti CČSH dovolují, stanovují pracovníci IT bezpečnostní opatření v souladu s mezinárodními standardy ISO 27001, 27002 a 200001.

Článek XIX.
Používání notebooků, tabletů, chytrých telefonů a přenos osobních údajů

1. Vnitřní úložiště tabletů a chytrých telefonů, které je využíváno k uchovávání osobních údajů, musí být zašifrováno.
2. Pokud pracovníci využívají ke zpracování osobních údajů přístroj v jejich soukromém vlastnictví, jsou povinni zajistit na těchto zařízeních stejnou míru ochrany osobních údajů, jaká je aplikována na pracovních počítačích.
3. V případě, že jsou pro uchovávání nebo přenos osobních údajů využívány datové nosiče (cd, flash disky atd.) jsou dokumenty obsahující osobní údaje na tyto nosiče nahrávány v podobě archivu formátu .rar nebo .zip opatřeného heslem.
4. Pokud jsou k přenosu osobních údajů využívány e-mailové zprávy, jsou dokumenty obsahující osobní údaje přenášeny ve formě archivu formátu .rar nebo .zip opatřeného heslem. Heslo k příslušnému archivu je adresátovi e-mailové zprávy zasíláno prostřednictvím sms.
5. Pro služební účely je zakázáno využívat soukromé e-mailové adresy.

Článek XX.
Nakládání s dokumenty po skončení jejich užívání

1. Je-li ukončena činnost zpracování, pro kterou byly osobní údaje zpracovávány, a nejsou-li osobní údaje zpracovávány pro jiný účel ve smyslu čl. 6 odst. 4 GDPR, uchovávají se dokumenty obsahující osobní údaje po dobu trvání lhůt k archivaci stanovených zvláštní vnitřní směrnicí CČSH.

2. Po uplynutí lhůty k archivaci se dokumenty roztřídí na dokumenty určené k archivaci a dokumenty určené ke skartaci.
3. Fyzické dokumenty určené ke skartaci jsou zlikvidovány za využití skartovacího zařízení nebo odborné externí společnosti. S odbornou externí společností bude uzavřena smlouva o zpracování osobních údajů.
4. Dokumenty s osobními údaji, jejichž skartační lhůta uplynula, uchovávané v elektronické podobě, jsou vymazávány tak, aby nebylo možné jejich obnovení.

Práva subjektů údajů

Článek XXI.
Obecná ustanovení

1. V souvislosti se zpracováním osobních údajů svědčí subjektům údajů práva upravená v čl. 12 až 22 GDPR, a to:
   a) právo na informace o zpracování osobních údajů,
   b) právo na přístup k osobním údajům,
   c) právo na opravu,
   d) práva na výmaz,
   e) právo vznést námitku,
   f) právo na přenositelnost osobních údajů.
2. Při vyřizování žádostí subjektů údajů o uplatnění jejich práv postupují zaměstnanci vstřícně a se snahou v maximální možné míře vyhovět subjektům údajů při respektování příslušných ustanovení GDPR a zájmů CČSH, které nejsou v rozporu s GDPR.
3. *Zaměstnanci jsou* povinni postupovat při vyřizování žádostí subjektů údajů nebo jednotlivých úkonů vedoucích k vyřízení žádosti pečlivě a bez zbytečných průtahů.

Článek XXII.
Informační povinnost

1. Pokud jsou osobní údaje získány pro stanovený účel přímo od subjektu údajů, jsou poskytnuty subjektu údajů informace o zpracování osobních údajů v rozsahu podle čl. 13 GDPR, a to v okamžiku získání těchto osobních údajů.
2. Pokud jsou osobní údaje získány z jiného zdroje než od subjektu údajů, jsou poskytnuty subjektu údajů informace o zpracování osobních údajů v rozsahu podle čl. 14 GDPR, a to při prvním kontaktu se subjektem údajů, nejpozději však do jednoho měsíce od jejich získání.
3. Informace o zpracování osobních údajů podle bodu 2 nejsou nutné, pokud je zřejmé, že subjekt údajů už příslušné informace má.
4. Informace podle bodů 1 a 2 jsou poskytovány v maximálním možném rozsahu.
5. Informace podle bodů 1 a 2 se poskytují prokazatelnou formou, a to písemně při získání jedné kopie informace podepsané subjektem údajů, doručením informace na e-mail subjektu údajů nebo zobrazením informace jako povinného kroku v rámci webového rozhraní. Forma poskytnutí informace závisí na formě komunikace se subjektem údajů.
6. V rámci činnosti zpracování může být zvolen odlišný postup poskytnutí informace podle bodu 1 a 2, pokud je zajištěna doložitelnost poskytnutí informace.

Článek XXIII.
Vyřizování žádostí subjektů údajů

1. K přijímání žádostí subjektů údajů je příslušný koordinátor GDPR. Pokud je žádost subjektu údajů doručena jinému zaměstnanci nebo do spisovny, je povinností příslušného zaměstnance předat bez zbytečného odkladu žádost koordinátorovi GDPR.
2. Po přijetí žádosti subjektu údajů prověří koordinátor GDPR, zda je subjekt údajů bezpečně identifikovatelný. Pokud tomu tak není, vyzve subjekt údajů k prokázání identity s poučením, že při neprokázání identity nebude možné žádost vyřídit.
3. Předmět žádosti se posuzuje podle jejího obsahu, nikoli podle označení.
4. V závislosti na tom, jaké právo subjekt údajů uplatní, vyzve koordinátor GDPR odpovědné zaměstnance a pracovníky IT oddělení, aby provedli lustraci úložišť osobních údajů a sdělili mu podrobnosti o zpracování osobních údajů týkajících se žádajícího subjektu údajů. K poskytnutí těchto informací jim stanoví přiměřenou lhůtu ne delší než dva týdny.
5. Koordinátor GDPR vytvoří o přijaté žádosti záznam a předá ji pověřenci pro ochranu osobních údajů.
6. Reakce na žádost subjektu údajů se zasílá písemně s výjimkou případů, kdy subjekt údajů požádá o jiný způsob doručení.
7. Datum a způsob vyřízení žádosti subjektu údajů pověřenec pro ochranu osobních údajů vyznačí do záznamu o přijetí žádosti subjektu údajů.

Incidenty porušení zabezpečení

Článek XXIV.
Hlášení porušení zabezpečení

1. Zjistí-li zaměstnanec porušení zabezpečení osobních údajů, informuje o tom okamžitě prokazatelným způsobem odpovědného zaměstnance, koordinátora GDPR, pověřence pro ochranu osobních údajů a vedoucího pracovníka IT oddělení, pokud se porušení zabezpečení týká osobních údajů uchovávaných v elektronické podobě.
2. Zaměstnanec současně provede všechna opatření k zamezení pokračování porušení zabezpečení nebo jeho opakování, která mu jeho role umožňuje nebo která může fyzicky provést. O těchto opatřeních informuje osoby podle bodu 1.
3. Odpovědný zaměstnanec ve spolupráci se zaměstnancem, který porušení zabezpečení odhalil, vyplní do 24 hodin záznam o incidentu porušení zabezpečení a předá jej osobám podle bodu 1.
4. Pověřenec pro ochranu osobních údajů posoudí, zda je porušení zabezpečení takového charakteru, že vyžaduje hlášení Úřadu pro ochranu osobních údajů, případně subjektům údajů, jejichž osobních údajů se porušení zabezpečení týká.
5. Pokud je nutné provést hlášení podle bodu 4, provede jej pověřenec pro ochranu osobních údajů do 72 hodin od okamžiku, kdy bylo porušení zabezpečení ohlášeno, a uvede v něm všechny informace požadované podle čl. 33 GDPR.

Článek XXV.
Řešení incidentů porušení zabezpečení

1. Řešení incidentu porušení zabezpečení je prioritním úkolem všech zaměstnanců podílejících se na činnosti zpracování a v případě, že se týká osobních údajů zpracovávaných v elektronické podobě, také pracovníků IT oddělení.
2. Zaměstnanci a další osoby vyvíjejí maximální úsilí o odvrácení negativních následků porušení zabezpečení pro subjekty údajů.
3. Byl-li incident porušení zabezpečení ohlášen Úřadu pro ochranu osobních údajů a stanovil-li Úřad pro ochranu osobních údajů nutné kroky nebo dal-li CČSH jakákoli doporučení, jsou zaměstnanci povinni se těmito doporučeními řídit a stanovené kroky provést.
4. Na základě prošetření incidentu porušení zabezpečení provede odpovědný zaměstnanec opětovné posouzení vlivu činnosti na ochranu osobních údajů a stanoví opatření k zamezení opakování incidentu.

Článek XXVI.
Odpovědnost zaměstnanců

1. Způsobí-li zaměstnanec incident porušení zabezpečení úmyslně nebo z hrubé nedbalosti, představuje toto jednání nebo opomenutí porušení právní povinnosti vyplývající z právních předpisů vztahujících se k jím vykonávané práci zvlášť hrubým způsobem. Totéž platí pro případ, kdy se zaměstnanec o takové jednání nebo opomenutí pokusil, ale bez jeho přičinění k incidentu porušení zabezpečení nedošlo.
2. Způsobí-li zaměstnanec incident porušení zabezpečení z nedbalosti, představuje toto jednání nebo opomenutí neuspokojivý pracovní výsledek, na základě kterého bude zaměstnanec vyzván k jeho odstranění. Dojde-li v období 12 měsíců následujících po vyzvání ze strany zaměstnance k opětovnému pochybení, bude případ řešen v souladu s řády CČSH a dalšími právními předpisy.

Kontrola ochrany osobních údajů

Článek XXVII.
Průběžná kontrola

1. V rámci provádění činnosti zpracování zkoumají zaměstnanci průběžně, zda zavedené procesy odpovídají GDPR, zda jsou dodržovány, zda jsou dostatečné pro ochranu osobních údajů a zda představují nejlepší dostupné řešení ochrany osobních údajů.
2. Pověřenec pro ochranu osobních údajů sleduje vývoj rozhodovací praxe dozorového úřadu a soudů, jakož i doporučení dozorového úřadu a Evropského sboru pro ochranu osobních údajů. Své poznatky předává koordinátorům GDPR a odpovědným zaměstnancům a vypracovává doporučení ke zlepšení praxe ochrany osobních údajů.
3. Zaměstnanci IT oddělení sledují vývoj informačních technologií a informují o otázkách relevantních pro ochranu osobních údajů koordinátory GDPR. Na základě svých zjištění vypracovávají doporučení ke zlepšení praxe ochrany osobních údajů.
4. Odpovědní zaměstnanci předávají zaměstnancům provádějícím činnosti zpracování relevantní informace a dohlíží nad začleňováním nové praxe do činnosti zpracování.

5. Pověřenec a koordinátoři GDPR jsou oprávněni provádět dle svého uvážení namátkové kontroly dodržování GDPR a Směrnice v rámci jakékoli činnosti zpracování.

Článek XXVIII.
Incidenční kontrola

1. Dojde-li k incidentu porušení zabezpečení, sestaví koordinátor GDPR ve spolupráci s pověřencem pro ochranu osobních údajů a odpovědným zaměstnancem zprávu shrnující příčiny a podobu incidentu. Zároveň vypracuje doporučení pro provádění ostatních činností zabezpečení pro předejití obdobnému incidentu.
2. Odpovědní zaměstnanci jsou povinni seznámit se se zprávou a s doporučením a podniknout příslušné kroky. Zejména zkontrolují, zda není v rámci jejich činnosti zpracování využíván tentýž proces, který zapříčinil incident porušení zabezpečení.

Závěrečná ustanovení

Článek XXIX.
Přechodná ustanovení

1. Ústřední rada a diecézní rady jmenují koordinátory GDPR do jednoho měsíce ode dne účinnosti Směrnice.
2. Koordinátor GDPR určí odpovědné zaměstnance pro jednotlivé činnosti zpracování, které probíhají k okamžiku účinnosti Směrnice, do dvou týdnů od svého jmenování.
3. Odpovědní zaměstnanci vypracují záznamy o činnosti zpracování do jednoho měsíce ode dne svého jmenování.

Článek XXX.
Platnost a účinnost

1. Směrnice nabývá platnosti dnem schválení ústřední radou a účinnosti dne 1. září 2018.

Směrnice byla schválena usnesením Ústřední rady Církve československé husitské č. 4.1.1.194 dne 15. června 2018.

ThDr. Tomáš Butta
patriarcha