Cirkevný zbor Evanjelickej cirkvi augsburského vyznania na Slovensku

Prešov

w w w . p a t m o s . s k

BEZPEČNOSTNÉ OPATRENIA

V Prešove, dňa 01.10.2021

Prevádzkovateľ:	**Cirkevný zbor Evanjelickej cirkvi augsburského vyznania na Slovensku Prešov** (ďalej len prevádzkovateľ)
Sídlo:	Svätoplukova 11, 08001 Prešov
IČO:	31947042
DIČ:	2020544042
IČ DPH:	SK 2020544042
Bankové spojenie:	SLSP a.s.
Číslo účtu:	SK91 0900 0000 0000 9628 9004
Vedúci orgán:	Mgr. Ondrej Koč, Mgr. Martin Chalupka , Mgr. Miroslav Čurlík
Telefón:	+421 51 77 25 925, 0908 987 664
E-mail:	ev.fara@patmos.sk
Web:	www.patmos.sk

Prevádzkovateľ je zapísaný v registri Ministerstva kultúry Slovenskej republiky. Cirkevné oddelenie Ministerstva kultúry Slovenskej republiky vedie evidenciu všetkých právnických osôb, ktoré odvodzujú svoju právnu subjektivitu od cirkví a náboženských spoločností, ak nepodliehajú inej evidencii alebo registrácii. Evidenciu vedie podľa Opatrenia Ministerstva kultúry SR číslo MK-33/2001-1 zo dňa 10. januára 2001 v súlade s § 19 ods. 1 zákona číslo 308/1991 Zb. o slobode náboženskej viery a postavení cirkví a náboženských spoločností v znení neskorších predpisov.

Predmetom tejto dokumentácie sú:

Bezpečnostné opatrenia, určujúce postup pre technické a organizačné zabezpečenie ochrany osobných údajov. Tieto opatrenia sa aktualizujú vždy podľa potreby vzhľadom na najnovšie poznatky. (§ 31)

Bezpečnostná dokumentácia obsahujúca informácie, ktoré slúžia výlučne pre interné potreby prevádzkovateľa a kontrolnej činnosti zo strany Úradu na ochranu osobných údajov.

Bezpečnostné opatrenia platia pre informačné systémy uvedené v Zázname o spracovateľských činnostiach prevádzkovateľa. (§ 37)

Bezpečnostné opatrenia sa týkajú :

1) Personalistiky a miezd
2) Marketingu
3) Evidencie členov cirkevného zboru – Elektronický informačný systém ECAV
4) Elektronického obchodu

Záznam o spracovateľských činnostiach prevádzkovateľa obsahuje najmä: (§ 37) Vzor záznamu https://dataprotection.gov.sk/uoou/node/484

Identifikačné údaje spoločnosti (zodpovednú osobu)
Účel a zákonnosť spracúvania osobných údajov
Kategória dotknutých osôb
Kategória osobných údajov
Kategória príjemcov
Registratúra a archivácia osobných údajov
Posúdenie rizík pri spracúvaní osobných údajov

Prevádzkovateľ neuskutočňuje prenos osobných údajov do tretích krajín. (§ 47)

Rozsah spracovaných osobných údajov:
Prevádzkovateľ spracúva osobné údaje v malom rozsahu.
Počet osôb, ktorým sa spracúvajú osobné údaje v pomere k počtu obyvateľov v Slovenskej republike podľa štatistického úradu Štatistika:

4000 / 5 443 120 = 0,0007

Malý rozsah menej ako 0,1
Veľký rozsah 0,1 a viac

Na účely tejto bezpečnostnej smernice sa rozumie:

- Súhlasom dotknutej osoby akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov.

- Genetickými údajmi osobné údaje týkajúce sa zdedených genetických charakteristických znakov fyzickej osoby alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby

- Biometrickými údajmi osobné údaje, ktoré sú výsledkom osobitného technického spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú jedinečnú identifikáciu alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako najmä vyobrazenie tváre alebo daktyloskopické údaje.

- Údajmi týkajúcimi sa zdravia osobné údaje týkajúce sa fyzického zdravia alebo duševného zdravia fyzickej osoby vrátane údajovo poskytovaní zdravotnej starostlivosti alebo služieb súvisiacich s poskytovaním zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave.

- Spracúvaním osobných údajov spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami.

- Obmedzením spracúvania osobných údajov označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti.

- Profilovaním akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom.

- Pseudonymizáciou spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej fyzickej osobe alebo identifikovateľnej fyzickej osobe.
- Logom záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme.

- Šifrovaním transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo

- Online identifikátorom identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom, najmä IP adresa, cookies, prihlasovacie údaje do online služieb, rádiofrekvenčná identifikácia, ktoré môžu zanechávať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu.

- Informačným systémom akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe.

- Porušením ochrany osobných údajov porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim.

- Dotknutou osobou každá fyzická osoba, ktorej osobné údaje sa spracúvajú.

- Prevádzkovateľom každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov.
- Sprostredkovateľom každý, kto spracúva osobné údaje v mene prevádzkovateľa.

- Príjemcom každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov.

- Treťou stranou každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje.

- Zodpovednou osobou osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa tohto zákona.

- Zástupcom fyzická osoba alebo právnická osoba so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom v členskom štáte, ktorú prevádzkovateľ alebo sprostredkovateľ písomne poveril.
- Podnikom fyzická osoba – podnikateľ alebo právnická osoba vykonávajúca hospodársku činnosť bez ohľadu na jej právnu formu vrátane združení fyzických osôb alebo združení právnických osôb, ktoré pravidelne vykonávajú hospodársku činnosť.

- Skupinou podnikov ovládajúci podnik a ním ovládané podniky.

- Hlavnou prevádzkarňou:
    a) Miesto centrálnej správy prevádzkovateľa v Európskej únii, ak ide o prevádzkovateľa s prevádzkarňami vo viac než jednom členskom štáte, okrem prípadu, keď sa rozhodnutia o účeloch a prostriedkoch spracúvania osobných údajov prijímajú v inej prevádzkarni prevádzkovateľa v Európskej únii a táto iná prevádzkareň má právomoc presadiť

vykonanie takýchto rozhodnutí, pričom v takom prípade sa za hlavnú prevádzkareň považuje prevádzkareň, ktorá takéto rozhodnutia prijala.

b) Miesto centrálnej správy sprostredkovateľa v Európskej únii, ak ide o sprostredkovateľa s prevádzkarňami vo viac než jednom členskom štáte alebo ak sprostredkovateľ nemá centrálnu správu v Európskej únii, prevádzkareň sprostredkovateľa v Európskej únii, v ktorej sa v kontexte činností prevádzkarne sprostredkovateľa uskutočňujú hlavné spracovateľské činnosti, a to v rozsahu, v akom sa na sprostredkovateľa vzťahujú osobitné povinnosti podľa tohto zákona.

- Vnútronými pravidlami postupy ochrany osobných údajov, ktoré dodržiava prevádzkovateľ alebo sprostredkovateľ so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom na území Slovenskej republiky na účely prenosu osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v tretej krajine.

- Kódexom správania súbor pravidiel ochrany osobných údajov dotknutej osoby, ktorý sa prevádzkovateľ alebo sprostredkovateľ zaviazal dodržiavať.

- Medzinárodnou organizáciou organizácia a jej podriadené subjekty, ktoré sa riadia medzinárodným právom verejným, alebo akýkoľvek iný subjekt, ktorý bol zriadený dohodou medzi dvoma alebo viacerými krajinami alebo na základe takejto dohody.

- Členským štátom štát, ktorý je členským štátom Európskej únie alebo zmluvnou stranou Dohody o Európskom hospodárskom priestore. Treťou krajinou krajina, ktorá nie je členským štátom,

- Zamestnancom úradu zamestnanec v pracovnom pomere alebo v obdobnom pracovnom vzťahu podľa osobitného predpisu6) alebo štátny zamestnanec, ktorý vykonáva štátnu službu v štátnozamestnaneckom pomere.

- Oprávnenou osobou je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho, štátnozamestnaneckého, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia, vymenovania a ktorá spracúva osobné údaje po riadnom poučení.

TECHNICKÉ OPATRENIA

Technické opatrenia realizované prostriedkami fyzickej povahy

Informačné systémy sú chránené pred neoprávneným prístupom murovanou budovou s uzamykateľnými dverami na vstupe do budovy a kancelárie farského úradu. Prístup do budovy je chránený vstupnými dverami a elektronickým zámkom s telefónom s kamerou.

Dokumenty neautomatizovaného informačného systému osobných údajov sú chránené v uzamykateľných skriniach a citlivé osobné údaje v nehorľavých uzamykateľných trezoroch. Dokumenty sú umiestnené mimo priameho slnečného žiarenia a pri ich spracúvaní sa použijú žalúzie.

Zobrazovacia technika je umiestnená smerom od dverí, minimálne v pravom uhle ku dverám, pre prípad náhodného vstupu neoprávnenej osoby a možného odpozerania osobných údajov pri ich spracúvaní. Časový úsek počas ktorého je možné prihlásiť sa k pracovnej stanici bez zadania hesla (šetrič obrazovky) je stanovený na päť minút. Počas prítomnosti neoprávnených osôb sa osobné údaje nespracúvajú a ich obsah je uložený na mieste nedostupnom pre neoprávnené osoby.

Tlačiareň je umiestnená a pripojená tak, že k nej majú prístup len oprávnené osoby pri spracovaní miezd a tlači materiálov, kde sú osobné údaje.

Pre fyzickú likvidáciu listinných dokumentov sa používa centrálna skartovačka. CD sa likvidujú rozstrihnutím nožnicami, USB formátovaním a následným fyzickým zničením.

Ochrana pred neoprávneným prístupom

Prenos osobných údajov ako aj uložené dáta nosičov sú chránené šifrovaním podľa aplikačného vybavenia jednotlivých softvérov a dešifrovať ich je možné len použitím zodpovedajúceho kľúča. Prístup tretích strán k informačnému systému nie je povolený, pokiaľ osobitný zákon neurčuje inak, napríklad kontroly, dokazovanie trestných činov.

Riadenie prístupu k osobným údajom oprávnených osôb

Prístup k informačným systémom, ktoré sú predmetom ochrany osobných údajov majú len osoby určené vedúcim orgánom, po riadnom zaškolení a poučení o možných bezpečnostných rizikách, ich predchádzaniu a riešeniu prípadných incidentov . Zoznam používateľov chránených aktív má vedúci orgán a administrátor softvérového vybavenia, s ktorým je uzatvorená riadna zmluva (§ 34).

Práva na prístup do informačného systému osobných údajov prideľuje administrátor na základe pokynov vedúceho orgánu v rozsahu nevyhnutnom na výkon funkcie oprávnenej osoby . Dĺžka identifikačných kódov je minimálne 15 rôznych znakov, ktoré generuje a prideľuje administrátor.

Zmeny identifikačných kódov sa vykonávajú pri prezradení hesla, pri podozrení z prezradenia hesla, dlhodobej neprítomnosti oprávnených osôb, napríklad dlhodobá práceneschopnosť, materská, rodičovská

dovolenka, vyšetrovanie zamestnanca z kriminálnych činov a iných možných hrozbách zneužitia spracúvaných osobných údajov.

Pri ukončení pracovného alebo iného pomeru sa všetky prístupy k informačnému systému zrušia, odovzdá sa kompletná dokumentácia s výpočtovou technikou a komunikačnými prostriedkami.

Ochrana proti škodlivému kódu z verejne dostupnej počítačovej siete a sieťová bezpečnosť.

Na počítačoch je prevedená inštalácia antivírových a antispywarových programov s platnou licenciou, ktoré sú podľa najnovších poznatkov aktualizované. Ochranné programy sú pri zapnutí výpočtových prostriedkov aktuálne a aktívne. Priebežne sú inštalované aktuálne bezpečnostné záplaty operačných systémov a je nastavená ochrana pred nevyžiadanou elektronickou poštou. Pravidelne sa prevádza údržba nainštalovaných skriptov a iných podobných programov. Používa sa aktuálny bezpečnostný skener, penetračný test pre kontrolu a určenie zraniteľnosti informačného systému. Nainštalovaný je systém na detekciu prieniku firewall na rozhraní siete internet a LAN. Obvodový a lokálny firewall je aktualizovaný na najnovšie poznatky. Pravidelne sa odstraňujú, prípadne vypínajú nevyužívané softvéry, porty a služby. Aktualizácie operačného systému a programového aplikačného vybavenia sú vykonávané vždy, pokiaľ sú vydané ich nové verzie zabezpečeným vzdialeným prístupom alebo stiahnutím aktualizácie na disk a ich následnou inštaláciou.

Poučenie o správnom zaobchádzaní je bližšie popísané v časti personálna politika.

Podmienky zálohovania osobných údajov.

Aktualizácia záloh sa robí na najnovšiu verziu softvéru. Zálohovanie sa realizuje na najnovšie kvalitné pamäťové médiá. Kontrola správneho chodu a ochrany zálohových softvérov skenerom administrátorom. Prevádza sa kontrola starších pamäťových médií, či je technicky možné uložené dáta opätovne prečítať. Uložených záloh sa overujú, či boli skutočne a správne prekopírované. Zálohy informačných systémov sú umiestnené v uzamykateľných trezoroch, prípadne kancelárskych skriniach. Prístup k nim majú jedine osoby oprávnené spracúvať osobné údaje a vedúci orgán.

Likvidácia osobných údajov a dátových nosičov

Dokumentácia osobných údajov sa likviduje na základe registratúrneho plánu a poriadku v riadnom vyraďovacom konaní. Osobné údaje, pri ktorých pominul účel a dôvod na ich archiváciu mimo termínu vyraďovacieho konania, sa likvidujú bez omeškania v najbližšom vhodnom termíne. Technické nosiče osobných údajov sa likvidujú podľa ich povahy rozložením, vymazaním, fyzickým zničením tak, aby ich nebolo možné reprodukovať. Papierová dokumentácia sa likviduje prostredníctvom skartovačky upravenej na vysoký stupeň ochrany rozkladu dokumentu.

ORGANIZAČNÉ OPATRENIA

Poučenie oprávnených osôb

Osoby oprávnené spracúvať osobné údaje sú náležite poučené o spôsobe spracúvania týchto údajov vždy pred uskutočnením prvej spracovateľskej operácie. Poučenie pozostáva najmä z informácií o postupoch pri získavaní, zhromažďovaní, šírení, zaznamenávaní, usporadúvaní, zmenách, vyhľadávaní, prehliadaní, kombinovaní, premiestňovaní, uchovávaní, blokovaní, likvidácii, sprístupňovaní, zverejňovaní a inej manipulácie s osobnými údajmi.

Poučenie je pre oprávnenú osobu vykonávané v rozsahu podľa jej pracovnej náplne pracovnej zmluve alebo inej právnej spolupráci na základe zmluvy, kde je vymedzený účel, rozsah a spôsob spracúvania osobných údajov v zmysle platnej legislatívy. Poučenie obsahuje poučenie o mlčanlivosti o osobných údajoch počas vzájomnej spolupráce a aj po ukončení spolupráce. (§ 79)

Oprávnené osoby sú poučené aj o bezpečnostných pravidlách pri spracúvaní osobných údajov najmä o:
Spôsobe zabezpečenia informačného systému
Používaní neautorizovaných systémových programov
Zodpovednosti a dôsledkoch za nezodpovedné nakladanie, zneužitie informácii
Povinnosti nahlasovať každý incident vedúcemu orgánu (strata – krádež informačného systému, rázne spomalenie počítača, iné neštandardné správanie sa počítača, strata- prezradenie hesla, požiaru a iných prírodných katastrof) , ktorý by mohol viesť k zneužitiu osobných údajov.
Postup pri predchádzaní incidentom a spôsob riešenia incidentov.
Povinnosti dodržiavať pokyny vedúcich orgánov a administrátorov
Povinnosti vzdelávať sa a zúčastňovať sa školení.

Poučenie sa vykonáva zamestnancom, externými školeniami, samo vzdelávaním a inými dostupnými možnosťami . Z poučenia je vypracovaný záznam. Zodpovedná osoba nie je stanovená.

Zoznamy aktív (osobných údajov) a ich aktualizácia

Zoznam alebo rozsah aktív je vedený podľa právneho základu a účelu spracovania údajov a je aktualizovaný bez zbytočného omeškania oprávnenými a poučenými osobami podľa ich najnovších dostupných poznatkov.

Riadenie prístupu

Prístup do chránených priestorov objektov majú len oprávnené osoby, ktoré majú pridelené kľúče do objektu aj do kancelárií. Pri vstupe sa zapíšu sa do knihy dochádzky. V prípade straty, prezradenia alebo iného odhalenia kľúčov a prístupových prvkov sa táto skutočnosť nahlasuje vedúcemu orgánu, ktorý urobí príslušné opatrenia, aby zabránil možným škodám.
Prístupová politika hesiel sa zakladá na prideľovaní, odoberaní a obmedzení prístupu aktívam v takom rozsahu, v akom majú oprávnené osoby s osobnými údajmi právo nakladať. Správu hesiel má vo svojej kompetencii administrátor na základe pokynov vedúceho orgánu.

Počas neprítomnosti oprávnených osôb sú pridelené nové prístupové oprávnenia zastupujúcim oprávneným osobám. Po ukončení zastupovania sú zástupcom pridelené prístupy zrušené. Pridelené

heslá, kľúče a iné prístupové prvky sa nesmú nachádzať pri informačnom systéme, pre ktorý boli zabezpečujúce prvky pridelené.

Pravidlá pre spracúvanie osobných údajov v chránených priestoroch a mimo nich.

Prístup k osobným údajom majú len osoby oprávnené a náležite poučené o manipulácii a spôsobe spracúvania osobných údajov. Počas práce s osobnými údajmi sú oprávnené osoby vždy prítomné v chránených priestoroch. Pri vstupe inej ako oprávnenej osoby, napríklad upratovačka, návšteva, zákazník, sú povinné urobiť všetko pre to, aby osobné údaje nemohli byť odpozerané, ukradnuté a ináč zneužité, ako napríklad vypnutie obrazovky na zobrazovacej technike, papierové dokumenty obrátené na rub, prípadne odložené do uzamykateľnej zásuvky, skrine.

V čase pobytu neoprávnenej osoby v chránených priestoroch sa dokumenty s osobnými údajmi netlačia na tlačiarni.

Návštevy a iné cudzie osoby, pri ktorých hrozí riziko zneužitia dát organizácie, sú vždy po celú dobu pobytu v chránených priestoroch sprevádzané oprávnenými osobami.

Osobné údaje, ktoré sa spracúvajú mimo chránených priestorov napríklad pri spoločenských, športových, kultúrnych aktivitách, sa spracúvajú tak, aby nemohli byť zneužité, že sa nikdy nenechávajú bez dozoru oprávnenej a poučenej osoby. Počítače, smartfóny a iná technika musí byť pred opustením chránených priestorov zabezpečená heslom a údaje z nej musia by riadne zálohované. Po ukončení aktivity sa dokumentácia aj technické vybavenie bezodkladne odnesie do chránených priestorov.
Zodpovednosť za zverené alebo získané osobné údaje má oprávnená osoba. Nedodržanie bezpečnostných opatrení sa môže považovať za porušenie disciplíny alebo za porušenie zmluvných podmienok, pri osobe v inom ako pracovnom pomere spolupracujúcej na základe zmluvy.

Likvidácia osobných údajov

Za likvidáciu databáz osobných údajov sú zodpovedné oprávnené osoby, ktorým to vyplýva z náplne ich práce. Dokumentácia osobných údajov sa likviduje na základe registratúrneho plánu a poriadku v riadnom vyraďovacom konaní. Osobné údaje, pri ktorých pominul účel a dôvod na ich archiváciu mimo termínu vyraďovacieho konania, sa likvidujú bez omeškania v najbližšom vhodnom termíne.

Technické nosiče osobných údajov sa likvidujú podľa ich povahy rozložením, vymazaním, fyzickým zničením tak, aby ich nebolo možné reprodukovať. Kontrolu nad tým, či sú databázy úspešne zlikvidované má administratívny pracovník.

Papierová dokumentácia sa likviduje prostredníctvom skartovačky upravenej na vysoký stupeň ochrany rozkladom dokumentu. Likvidáciu uskutočňujú oprávnené osoby, ktoré sa riadia podľa registratúrneho plánu, prípadne podľa inštrukcií vedúceho orgánu.

Bezpečnostné incidenty

Akýkoľvek bezpečnostný incident ako napríklad neoprávnený lokálny prístup k informačným systémom, neoprávnený prienik k údajom do technických nosičov, zneužitie osobných údajov, výpadok elektriny, havária, narušiteľ a pod., ohlasuje poverený zamestnanec incident vedúcemu orgánu a postupuje táto oprávnená osoba v zmysle poučenia. Pri jeho nedostupnosti sa bezpečnostné incidenty ohlasujú

najbližšiemu nižšiemu zodpovednému orgánu. V prípade technického zlyhania informačného systému aj administrátorovi.
Po každom bezpečnostnom incidente sa urobí zápisnica, kde je popísaný celý priebeh incidentu s vyvodenými dôsledkami pre zodpovedné osoby za spôsobený incident a riešenia na budúce predchádzanie rovnakým a podobným zlyhaniam. Návrhy riešení, postupy pri riešení incidentov sú spracované v týchto Bezpečnostných opatreniach.

Prevádzkovateľ oznámi úradu na ochranu osobných údajov porušenie ochrany osobných údajov ak je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby.
Porušenie ochrany osobných údajov sa oznamuje prostredníctvom webovej stránky úradu:
https://dataprotection.gov.sk/uoou/sk/dp/dp-breach

Opravy a údržbu automatizovaných prostriedkov vykonáva autorizovaný servis, s ktorým má organizácia uzatvorenú riadnu zmluvu (§ 34).

Kontrolná činnosť

Kontrolná činnosť organizácie je zabezpečená poverenou osobou, ktorá vykonáva dohľad nad dodržiavaním zákonných povinností v súvislosti s ochranou osobných údajov.

Kontrolná činnosť zameraná na dodržiavanie bezpečnostných opatrení je vykonávaná podľa potreby, minimálne raz za štvrťrok.

Opätovné poučenie oprávnených osôb sa vykonáva pri technických, legislatívnych, personálnych zmenách a opakovanie jeden krát za rok, na pracovnej porade prevádzkovateľa.

Bezpečnostné opatrenia ochrany osobných údajov sválené dňa 27.9.2021, uznesením Zborového presbyterstva Cirkevného zboru Evanjelickej cirkvi a.v. na Slovensku Prešov č. 9/2021.

Mgr. Ondrej Koč v.r. predsedajúci zborový farár	Mgr. Martin Chalupka v.r. zborový farár, senior ŠZS	Mgr. Miroslav Čurlík v.r. zborový dozorca