Mária Hudáková, Ag. Rosa,

IČO 37 163 256,

miesto podnikania 93021 Dunajský Klátov 41,

vedená v registri Okresné úradu Dunajská Streda, číslo živnostenského registra 201-13735

Smernica

o technických, organizačných a

bezpečnostných opatreniach spracovania osobných údajov

2025

OBSAH

1. Predmet úpravy

Táto smernica upravuje technické, organizačné a bezpečnostné postupy (ďalej len „opatrenia“) spracovania osobných údajov, povinnosti oprávnených osôb prevádzkovateľa s cieľom zabezpečiť ochranu osobných údajov pri manuálnom a automatizovanom spracúvaní osobných údajov v zmysle nariadenia 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, ktorým sa zrušuje smernica 95/46/ES (ďalej len „GDPR“) a zákonom č. 18/2018 Z. z. o ochrane osobných údajov (ďalej len „ZoOOÚ“)

Prevádzkovateľom na účely zákona je: Mária Hudáková, Ag. Rosa, IČO 37 163 256, miesto podnikania 93021 Dunajský Klátov 41, vedená v registri Okresné úradu Dunajská Streda, číslo živnostenského registra 201-13735.

2. Definície základných pojmov

Na účely definície pojmov tejto smernice v súlade s GDPR a ZoOOÚ sa rozumie:

osobnými údajmi	sú údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu,
oprávnenou osobou	fyzická osoba, ktorá spracováva osobné údaje podľa pokynov prevádzkovateľa, je viazaná povinnosťou mlčanlivosti o skutočnostiach, o ktorých sa dozvedela pri výkone svojej činnosti a bola poučená prevádzkovateľom o zásadách ochrany osobných údajov a o povinnostiach vyplývajúcich z predpisov o ochrane osobných údajov,
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 údajov o 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,
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,
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,
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,
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 podľa § 35 ZoOOÚ,
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,
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 Dohody o Európskom hospodárskom priestore,	štát, ktorý je členským štátom Európskej únie alebo zmluvnou stranou,
treťou krajinou	krajina, ktorá nie je členským štátom,
integritou údajov	neporušenosť a celistvosť (úplnosť) údajov,
likvidáciou osobných údajov	postup zrušenia osobných údajov najmä ich vymazaním, fyzickým zničením hmotných nosičov, spoľahlivo zabezpečujúce neobnoviteľnosť, nereprodukovateľnosť osobných údajov.

3. Zásady spracovávania osobných údajov

Zákonnosť spracúvania osobných údajov- spracúvanie osobných údajov sa vykonáva na základe aspoň jedného z týchto právnych základov:

a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel,
b) spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby,
c) spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
d) spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby,
e) spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, alebo
f) spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh.

Obmedzenie účelu spracúvania osobných údajov - Osobné údaje sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom; ďalšie spracúvanie osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, je možné, ak sú dodržané primerané záruky ochrany práv dotknutej osoby.

Minimalizácia osobných údajov - spracúvanie len takých osobných údajov, ktoré sú nevyhnutné na konkrétny účel; nespracúvajú sa údaje „do zásoby" ani nadbytočné informácie.

Zásada správnosti - osobné údaje musia byť presné, aktuálne a v prípade potreby priebežne aktualizované. Nesprávne alebo neúplné osobné údaje prevádzkovateľ v súčinnosti s dotknutou osobou bezodkladne opraví alebo vymaže.

Zásada minimalizácie uchovávania (obmedzenia uchovávania) - osobné údaje sa uchovávajú len po dobu nevyhnutnú na účel, na ktorý sa spracúvajú; po splnení účelu musia byť osobné údaje vymazané,

anonymizované alebo zlikvidované, napr. životopisy neúspešných uchádzačov o zamestnanie sa po ukončení výberového konania vymažú, ak neexistuje iný zákonný dôvod na ich ďalšie uchovávanie.

Zásada integrity a dôvernosti - osobné údaje musia byť spracúvané spôsobom, ktorý zabezpečuje ich primeranú bezpečnosť, najmä ochranu pred neoprávneným alebo nezákonným spracúvaním a pred náhodnou stratou, zničením alebo pozmeňovaním. Prevádzkovateľ riadi a kontroluje prístup k osobným údajom, osobné údaje spracovávajú len oprávnené a poučené osoby.

Zásada zodpovednosti – prevádzkovateľ dbá na dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a je povinný tento súlad so zásadami spracúvania osobných údajov na požiadanie preukázať.

4. Poučenie oprávnenej osoby

Prevádzkovateľ spracováva osobné údaje vo vlastnom mene oprávnenými osobami najmä zamestnancami prevádzkovateľa. Poverené fyzické osoby, ktoré budú spracovávať osobné údaje musia byť pred spracovaním osobných údajov poučené o:

- politike ochrany osobných údajov,
- rozsahu spracovávania osobných údajov prevádzkovateľom (sprostredkovateľom),
- účele spracovávania osobných údajov,
- právanom základe spracovávania osobných údajov,
- spracovateľských operáciách prevádzkovateľa,
- technických organizačných a bezpečnostných opatreniach a povinnostiach uvedených v tejto smernici, najmä o povinnosti zachovávať mlčanlivosť o osobných údajoch o ktorých sa dozvedeli,
- povinnostiach vyplývajúcich zo ZoOOÚ a GDPR a o
- zodpovednosti za ich porušenie.

Poučenie vykonáva prevádzkovateľom poverená osoba. O poučení osôb spracovávajúcich osobné údaje sa vyhotoví písomný záznam, ktorý obsahuje:

a) identifikačné údaje prevádzkovateľa,
b) vymedzenie rozsahu poučenia,
c) titul, meno, priezvisko, pracovné zaradenie a podpis poučenej osoby,
d) miesto a dátum poučenia,
e) titul, meno, priezvisko, pracovné zaradenie podpis toho, kto vykonal poučenie a
f) dátum, odkedy fyzická osoba prestala byť oprávnenou osobou; tento údaj doplní prevádzkovateľ po ukončení jej činnosti ako oprávnenej osoby.

Záznam o poučení oprávnenej osoby je uvedený v prílohe č 1.

Poučená osoba sa považuje za oprávnenú osobu, ktorá je oprávnená spracovávať osobné údaje prevádzkovateľa podľa pokynov prevádzkovateľa.

Prevádzkovateľ opätovne poučí oprávnenú osobu, ak:

a) došlo k podstatnej zmene v politike ochrany osobných údajov, zmene pracovného, služobného alebo funkčného zaradenia oprávnenej osoby, ak sa tým významne zmenil obsah náplne jej pracovných činností, alebo sa podstatne zmenili podmienky spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov v rámci jej pracovného zaradenia,

b) v pravidelných intervaloch, spravidla po skončení dovolenkovej sezóny v roku.

Po ukončení spracovávania osobných údajov, najmä z dôvodu skončenia pracovnoprávneho vzťahu oprávnenej osoby, prevádzkovateľ zabezpečí vykonanie opatrení, najmä zrušenie prístupových práv k informačnému systému a prístupu do priestorov a poučí zodpovednú osobu o povinnosti zachovávať mlčanlivosť aj po skončení spracovávania osobných údajov a o následkoch porušenia zákonných povinností.

5. Povinnosti oprávnených osôb

5.1 Povinnosť dodržiavať opatrenia na spracovanie osobných údajov

Oprávnené osoby sú povinné najmä:

- oboznámiť sa s politikou ochrany osobných údajov prevádzkovateľa,
- dodržiavať povinnosti a opatrenia pri spracúvaní osobných údajov podľa GDPR, ZoOOÚ a tejto smernice,
- spracovávať osobné údaje podľa pokynov prevádzkovateľa,
- zachovávať primeranú ostražitosť a každé čo i len podozrenie alebo porušenie ochrany osobných údajov oznámiť prevádzkovateľovi alebo zodpovednému zástupcovi.
- zachovávať mlčanlivosť o osobných údajoch a to aj po skončení činností pre prevádzkovateľa,
- osobne sa zúčastniť na školeniach, poučeniach oprávnených osôb o povinnostiach podľa smernice o technických, organizačných a bezpečnostných opatreniach spracovania osobných údajov.

5.2 Povinnosť zachovávať mlčanlivosť

Oprávnené osoby sú povinné chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, odcudzením, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania; v takomto prípade sú povinné bez zbytočného dokladu informovať prevádzkovateľa, ak majú za to, že sa porušuje ZoOOÚ a GDPR, alebo ustanovenia tejto smernice.

Oprávnené osoby sú povinné zachovávať mlčanlivosť o osobných údajoch, s ktorými prichádzajú do styku a nesmú ich využiť ani pre osobnú potrebu.

Je zakázané akékoľvek zverejňovanie, poskytovanie alebo sprístupňovanie osobných údajov prostredníctvom elektronických komunikačných prostriedkov alebo prostredníctvom sociálnych sietí vrátane telefonátov (cez telefón). Osobné údaje je možné poskytnúť len oprávneným príjemcom.

V prípade požiadavky na odovzdanie kamerového záznamu, musí byť tento záznam pred odovzdaním technicky upravený, tak, aby neobsahoval osobné údaje iných osôb. Technickou úpravou sa rozumie rozostretie zobrazenia iných osôb, okrem dotknutej, spôsobom znemožňujúcom ich identifikáciu.

Povinnosť zachovávať mlčanlivosti trvá aj po ukončení spracúvania osobných údajov alebo po ukončení pracovnoprávneho vzťahu oprávnenej osoby alebo iného vzťahu k oprávnenej osobe.

Pred zahájením vykonávania servisnej činnosti prevádzkovateľ uzatvorí s poskytovateľom služby (sprostredkovateľom) zmluvu o spracovaní osobných údajov so všetkými náležitosťami podľa GDPR a ZoOOÚ. Povinnosť zachovávať mlčanlivosť platí aj pre iné osoby, ktoré v rámci svojej činnosti (údržba, oprava, servis) prídu do styku s osobnými údajmi vrátane kamerového systému. O povinnosti zachovávať mlčanlivosť aj po skončení servisnej činnosti prevádzkovateľ vykoná poučenie, o ktorom vyhotoví záznam – v prílohe č. 4.

5.3 Povinnosti pri získavaní osobných údajov

Pri získavaní a spracúvaní osobných údajov sú oprávnené osoby povinné dodržiavať nasledovné pravidlá:

- pred získavaním osobných údajov od dotknutej osoby ju treba oboznámiť s účelom spracúvania osobných údajov, rozsahom spracúvania osobných údajov, predpokladanom okruhu tretích strán pri poskytovaní osobných údajov alebo príjemcov pri sprístupňovaní osobných údajov, forme zverejnenia, ak sa osobné údaje zverejňujú a tretie krajiny, ak sa predpokladá alebo je zrejmé, že sa do týchto krajín uskutoční cezhraničný prenos osobných údajov,
- pri získavaní osobných údajov vyžadovať od dotknutej osoby len nevyhnutný rozsah osobných údajov potrebný pre účel ich spracúvania,
- pri osobnom získavaní a spracúvaní osobných údajov zabezpečiť diskrétnosť, aby prítomné tretie osoby nemohli nahliadať do písomností obsahujúcich osobné údaj alebo sa inak oboznamovať so získavanými osobnými údajmi,
- oprávnená osoba kontroluje a overuje správnosť a aktuálnosť osobných údajov pri ich získaní,
- zakazuje sa, aby sa získavali osobné údaje fyzických osôb pod zámienkou iného účelu, než na účel, na ktorý sú spracovávané; ak osoba uviedla iniciatívne nepožadované osobné údaje, tieto budú ihneď diskrétne zlikvidované,
- vykonávať spracovateľské operácie podľa pokynov prevádzkovateľa,
- nesprávne alebo neúplné osobné údaje je potrebné opraviť alebo doplniť; ak to nie je možné, prevádzkovateľ je povinný ich blokovať do času ich likvidácie,
- zabezpečiť preukázateľný súhlas na spracúvanie osobných údajov dotknutej osoby v informačnom systéme, ak sa osobné údaje spracúvajú na základe súhlasu dotknutej osoby. Súhlas musí byť poskytnutý slobodne, vyjadrený jasne prostredníctvom aktívnej účasti dotknutej osoby (vopred označené políčko alebo nečinnosť a mlčanie sa nepokladajú za súhlas). Súhlas musí byť poskytnutý pred začatím spracúvania osobných údajov, na konkrétny účel, o ktorej je dotknutá osoba vopred informovaná v zrozumiteľnej forme. Udelenie súhlasu musí byť urobený vo forme, aby prevádzkovateľ súhlas vedel kedykoľvek preukázať (napr. písomne) a v prípade prenosu osobných údajov do tretích krajín, ktoré nezaručujú primeranú úroveň ochrany osobných údajov alebo ak ide o automatizované individuálne rozhodovanie vrátane profilovania, musí byť súhlas výslovný.

- v prípade osôb mladších ako 18 rokov, musí byť súhlas poskytnutý alebo schválený zákonným zástupcom dotknutej osoby a prevádzkovateľ overuje túto skutočnosť primeraným spôsobom.

6. Povinnosti a opatrenia pri spracúvaní osobných údajov

6.1 Povinnosti pri používaní informačných systémov

Automatizovaný informačný systém prevádzkovateľa vrátane jeho súčastí (počítače, software, sieťová infraštruktúra) nesmú byť používané na súkromné, alebo iné účely, ktoré nesúvisia s činnosťou prevádzkovateľa.

Každý používateľ sa prihlasuje do informačného systému prevádzkovateľa svojím používateľským menom a heslom. Používateľ je povinný utajiť svoje heslo. Prevádzkovateľ určuje zoznam osôb s administrátorským prístupom a prístup poverených osôb do informačných systémov a kontroluje zaznamenávanie prístupov do informačných systémov (logovanie).

Pri odchode od monitoru počítača je používateľ povinný uzamknúť pracovnú plochu počítača (použitím kombinácie kláves „Ctrl-Alt-Del“ a následne kliknutím na tlačidlo „Lock“, alebo použitím klávesy „Windows logo“ súčasne v kombinácii s klávesou „L“). Pri dlhodobom opustení miesta je používateľ povinný počítač vypnúť, alebo sa z počítača odhlásiť.

Všetky zmeny v konfigurácii počítača a ostatného technického vybavenia môžu byť vykonávané len administrátorom informačného systému.

Používateľ sa nesmie žiadnymi prostriedkami pokúšať sa získať prístupové práva administrátora, alebo privilegovaný stav, ktorý mu nebol nastavený administrátorom informačného systému. Pokiaľ používateľ v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený, alebo prístupové práva, ktoré mu neboli pridelené a nastavené alebo pri podozrení na prezradenie, stratu, odcudzenie alebo odtajnenie autentizačných informácií je povinný túto skutočnosť bezprostredne oznámiť štatutárovi prevádzkovateľa.

Používateľ nesmie vykonávať takú činnosť, ktorá by ostatným používateľom bránila v riadnom používaní informačného systému.

Používateľ je povinný byť ostražitý a vyhodnocovať nedôveryhodnosť prijatej elektronickej pošty, a to vzhľadom na odosielateľa správy, na samotný obsah správy najmä prítomnosť väčšieho množstva gramatických chýb, zvláštny slovosled, inak štruktúrovaná ako bežná podpisová doložka, predmet žiadosti odosielateľa, požiadavka spočívajúca vo vykonaní platby alebo zadaní prístupových a prihlasovacích údajov k nejakej službe, opis okolností vyvolávajúcich časový stres a pod.). Takýto incident je každý používateľ povinný nahlásiť a zdržať sa konania požadovaného v správe.

Je zakázané:

- sťahovať a inštalovať software, používať a šíriť nelegálne software, kopírovať a distribuovať nainštalované software ani súvisiacu dokumentáciu a príručky,
- otváranie príloh elektronickej pošty pochybného pôvodu, ktoré môžu ohroziť bezpečnosť spracovania osobných údajov,
- meniť nastavenia, konfigurácie, robiť zásahy do technických zariadení infraštruktúry, deaktivovať antivírusový sw,
- pripájať alebo odpájať technické zariadenia vrátane USB zariadení.

Prevádzkovateľ pridelené prístupové práva odoberie používateľovi informačného systému ak:

- dôjde k skončeniu, k zmene pracovného zaradenia, pracovného pomeru alebo iného vzťahu k prevádzkovateľovi, k závažnému porušenie pracovnej disciplíny, okamžitému skončeniu pracovného pomeru, ktorých charakter vyvolá potrebu odobratia prístupových práv,
- si to budú vyžadovať okolnosti zisteného bezpečnostného incidentu.

6.1.1 Aplikácia bezpečnostných záplat

Prevádzkovateľ zabezpečuje pravidelnú a včasnú aktualizáciu inštalovaného software. Aktualizácia operačného systému a programového aplikačného vybavenia sa zabezpečuje nastavením automatickej inštalácie bezpečnostných záplat poskytovaných dodávateľom operačného systému. Nastavenie automatickej inštalácie bezpečnostných záplat operačného systému s minimálnou periódou jeden deň.

6.1.2 Antivírové opatrenia a aktualizácia software

Prevádzkovateľ zabezpečuje odolnosť počítačových systémov proti škodlivým kódom antivírusovým softwarom, ktorý kontroluje prítomnosť škodlivého kódu v počítačoch, v prílohách a prichádzajúcej elektronickej pošty a na dátových nosičov. Prevádzkovateľ dbá na používanie výlučne legálneho softwaru vo svojich informačných systémoch.

Antivírusový software musí byť automaticky aktualizovaný. V prípade varovania o hrozbe infikácie, že sa v elektronickej pošte, na disku alebo prenosnom médiu nachádza škodlivý kód, je oprávnená osoba povinná hlásiť túto skutočnosť štatutárovi prevádzkovateľa alebo zodpovednej osobe je povinná zdržať sa manipulácie s týmto súborom alebo prílohou (nepreposielať elektronickú poštu inému adresátovi).

Prevádzkovateľ zabezpečuje aktualizácie používaného software, najmä na základe zverejnených informácií o technických zraniteľnostiach informačných systémov a priebežného vyhodnocovania rizík.

6.1.3 Používanie a tvorba bezpečného hesla

Pre prístup do informačného systému sa pre oprávnených používateľov zriaďuje prístupový kód (používateľské meno), pokiaľ sa nepoužíva iný bezpečnejší typ autorizácie (ID karta s PKI certifikátom, atď.).

Používateľ si zvolí heslo pre prístup do informačného systému minimálnej dĺžky 12 znakov, ktoré obsahuje aspoň jedno veľké písmeno, aspoň jednu číslicu alebo špeciálny znak napr. (!,#,$,%,&*,-,+,:,…atď.).

Pre prístup k zašifrovaným archívom sa volí heslo minimálnej dĺžky 15 znakov, ktoré obsahuje aspoň jedno veľké písmeno, aspoň jednu číslicu alebo špeciálny znak.

Používateľ je povinný chrániť heslá pred vyzradením iným osobám a nesmie uchovávať heslo na miestach dostupných iným osobám (napr. na papieri v kancelárii alebo uchovávať svoje prístupové heslo vo webových prehliadačoch).

Bezpečné heslo nesmie byť ako celok všeobecne známe (tzv. slovníkové slovo).

Používateľ je povinný zmeniť si heslo aspoň raz štvrťročne alebo okamžite v prípade, ak má podozrenie o prístupe k heslu inou osobou.

Nové heslo má byť odlišné od hesla, ktoré už v minulosti použil.

Používateľ nesmie v informačných systémoch prevádzkovateľa používať rovnaké heslo aké používa v iných systémoch.

6.1.4 Zálohovanie dát

Pre zabezpečenie minimalizácie rizika náhodnej straty, výmazu, alebo poškodenia osobných údajov sa pravidelne realizuje zálohovanie dát.

Zálohovanie sa vykonáva najmenej raz týždenne alebo aj skôr, ak dôjde k spracovaniu väčšieho objemu údajov.

Pred vykonaním zálohovania sa vykoná test záložného média zápisom a čítaním zapísaných údajov.

Záložné kópie osobných údajov, prípadne súvisiace metadáta a konfiguračné údaje potrebné pre obnovu, musia byť uložené v dátových kontajneroch umožňujúce ich zašifrovanie technologickými prostriedkami s heslom minimálnej dĺžky 12 znakov (napr. Bitlocker, atď.), ktoré obsahuje aspoň jedno veľké písmeno, aspoň jednu číslicu alebo špeciálny znak.

Záložné nosiče dát (USB disk, CD, DVD nosiče) musia byť uskladnené v inom priestore, kde sa nachádza HW vybavenie zálohovaného informačného systému.

Zálohované údaje musia byť uchovávané minimálne po dobu trojnásobnej periódy zálohovania.

Údaje uchované po dobu dlhšiu, ako je doba životnosti média, na ktorom sú uložené, musia byť zálohované aj na inom nosiči. Tieto údaje musia byť periodicky ukladané na nové nosiče ešte pred uplynutím životnosti pôvodného nosiča, tak aby sa tak predišlo strate spôsobenej nečitateľnosťou média.

Prevádzkovateľ raz ročne vyskúša postup obnovovania dát zo záložných úložísk.

Opatrenia v bodoch 6.1.1 až 6.1.4 vykonáva poverený sprostredkovateľ prevádzkujúci elektronickú platformu služieb dostupných na portáli https://zoznamtesa.sk/ .

6.1.5 Servisné činnosti na informačnom systéme

Pred začatím vykonávania servisnej činnosti prevádzkovateľ uzatvorí s poskytovateľom služby (sprostredkovateľom) zmluvu o spracovaní osobných údajov so všetkými náležitosťami podľa GDPR a ZoOOÚ.

Prevádzkovateľ pred vykonaním servisnej činnosti v informačnom systéme poučí osoby vykonávajúce údržbu alebo servisnú činnosť o povinnosti zachovávať mlčanlivosť o osobných údajoch o ktorých sa servisný technik dozvie pri výkone servisnej činnosti, o zákaze oboznamovať sa s osobnými údajmi, s ktorými príde do styku, o povinnostiach vyplývajúcich zo zákona 18/2018 Z. z., nariadenia GDPR, smernice o technických, organizačných a bezpečnostných opatreniach spracovania osobných údajov a o zodpovednosti za porušenie povinností.

Prevádzkovateľ vyhotoví zápis o poučení osôb – príloha č. 4, kde osoby stojace mimo prevádzkovateľa zaviaže dodržiavať mlčanlivosť o osobných údajoch, s ktorými prídu do styku pri činnostiach pre prevádzkovateľa a to aj po skončení vzťahu k prevádzkovateľovi a o povinnosti neoboznamovať sa s osobnými údajmi, s ktorými prídu do styku.

Prevádzkovateľ prostredníctvom poverenej osoby dohliada na vykonávanie servisnej činnosť a vyhotoví protokol o vykonaných operáciách s osobnými údajmi a o prípadnom prístupe k osobným údajom. Protokol podpíše prevádzkovateľ a osoba vykonávajúca servisnú činnosť.

6.2 Opatrenia sieťovej bezpečnosti

Opatrenia sieťovej bezpečnosti sú určené na prevenciu a monitorovanie pred neoprávneným prístupom, zneužitím, narušením sieťovej infraštruktúry prevádzkovateľa. Ak sa počítače, notebooky a iné zariadenia

pripájajú k sieti Internet prostredníctvom lokálnej počítačovej siete (LAN, Wifi) musí byť aktívne nastavený firewall. Nie je prípustné zapájať iné sieťové prvky umožňujúce prepojenie lokálnej počítačovej siete so sieťou Internet.

Odporúčané nastavenia:

- prednastavené heslo administrátora Wifi routra, firewallu sa zmení pri prvom prístupe k modemu podľa pravidiel tvorby hesiel uvedenej v kapitole 6.1.3 Používanie a tvorba bezpečného hesla,
- podľa konkrétneho modemu zariadenia nastaví sa heslo pre prístup k bezdrôtovej sieti napr. v záložke Maintenance v záložke Údržba -> Interface Setup -> Wireless v časti WPA2-PSK pole "Pre-Shared Key", podľa pravidiel tvorby hesiel uvedenej v kapitole 5.1.3 Používanie a tvorba bezpečného hesla,
- pre vyššiu úroveň bezpečnosti sa na Wifi routri aktivuje filtrácia MAC adries pripájaných zariadení prevádzkovateľa, ktorým sa umožňuje pripojenie sa do lokálnej siete. Administrácia vybraných počítačov / zariadení s MAC adresami, ktoré sú povolené sa zadajú v menu, napr. podľa modelu zariadenia v záložke Interface Setup -> Wireless v tabuľke s názvom Wireless MAC Address Filter. V nej sa zapíše fyzická adresa/MAC adresu zariadení (notebookov, mobilov, tabletov), ktorým sa povolí pripojiť sa do siete,
- pre ochranu proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok) sa aktivujú v ponuke firewallu ochrany proti rôznym druhom DDoS útokov,
- blokujú sa vstupné porty so zamedzením prístupu k sieťovým komponentom z vonkajšej siete (zakázaný vzdialený prístup).

Je zakázané používať nešifrované služby, ako je napr. telnet, ftp, http a nezabezpečené komunikačné systémy na prenos osobných alebo dôverných údajov.

Opatrenia sieťovej bezpečnosti elektronickej platformu služieb dostupných na portáli https://zoznamtesa.sk/ vykonáva poverený sprostredkovateľ.

6.3 Opatrenia fyzickej bezpečnosti

Každý zamestnanec je zodpovedný za fyzickú bezpečnosť svojho pracoviska a zverených pracovných prostriedkov.

Miestnosti, v ktorých sa skladujú listiny s osobnými údajmi musia byť v neprítomnosti oprávnenej osoby uzamknuté, vrátane okien.

Pri osobnej návšteve tretej osoby v priestoroch, kde sa spracúvajú osobné údaje prevádzkovateľa sa tretia osoba vždy sprevádza oprávnenou osobou od vstupu až do jeho odchodu.

V rokovacej miestnosti za prítomnosti tretej osoby sa nesmú na pracovných stoloch nachádzať otvorené spisy s osobnými údajmi, rozložené dokumenty, listiny, do ktorých by mohla tretia osoba hoci aj náhodne nahliadnuť.

Pri dočasnom opustení informačného systému sú oprávnené osoby povinné zabrániť prístupu tretej osoby k osobným údajom, odhlasovať sa z programov na spracovanie osobných údajov, zamknúť počítač alebo aktivovať šetrič obrazovky s povinne nastaveným heslom, odložiť do uzamykateľných skríň listiny s osobnými údajmi alebo uzamknúť miestnosť.

Pri odchode z pracoviska je oprávnená osoba povinná uzamknúť pracovisko, uzavrieť okná a prekontrolovať zariadenia, či nemôžu spôsobiť požiar alebo inú haváriu a aktivovať elektrický zabezpečovací systém objektu. Ak zamestnanec nemôže túto povinnosť splniť, oznámi to ihneď štatutárovi prevádzkovateľa.

Listiny, pamäťové médiá (USB disky, CD, DVD nosiče) s osobnými údajmi musia byť ukladané v uzamykateľnej kovovej skrini s bezpečnostným zámkom, ktorá je umiestnená v uzamykateľnej miestnosti. O vydaných kľúčoch vedie prevádzkovateľ evidenciu.

Strata kľúčov sa nahlasuje u štatutára prevádzkovateľa, ktorý zabezpečí výmenu zámkov.

V čase upratovania v priestoroch, kde sa spracúvajú osobné údaje sa zabezpečuje nepretržitá prítomnosť oprávnenej osoby.

Zakazuje sa zanechávanie dokumentov s osobnými údajmi v tlačových zariadeniach napr. kopírkach, tlačiarňach alebo faxoch bez dozoru.

Opatrenia fyzickej bezpečnosti elektronickej platformy služieb dostupných na portáli https://zoznamtesa.sk/ vykonáva poverený sprostredkovateľ.

6.4 Opatrenia pri prenose osobných údajov mimo priestorov prevádzkovateľa

Osobné údaje okrem prevádzkovateľa a oprávnených subjektov na základe zákona (napr. Sociálna poisťovňa, zdravotné poisťovne, Finančná správa SR, atď.) môže spracovávať len sprostredkovateľ, s ktorým prevádzkovateľ uzatvoril zmluvu o spracovaní osobných upravujúca rozsah a účel spracovania osobných údajov, práva a povinnosti strán pri ochrane spracovávaní osobných údajov (napr. spracovanie účtovníctva). Prenos osobných údajom iným subjektom je prísne zakázaný.

Listiny a nosiče s osobnými údajmi môžu byť fyzicky prenášané mimo priestory prevádzkovateľa len z oprávnených dôvodov a to zabezpečeným spôsobom. Prenášanie listín s osobnými údajmi je povolený len v uzatvorených obaloch alebo uzatvorených balíkoch.

Prenášanie osobných údajov na dátových nosičoch mimo priestory prevádzkovateľa je povolené len v zašifrovaných dátových kontajneroch, do ktorých sa uložia osobné údaje. Na prenášaných dátových nosičoch môžu byť uložené len tieto zašifrované dátové kontajnery a nesmú sa na nich nachádzať nezašifrované osobné údaje.

Tvorba dátových kontajnerov umožňujúce zašifrovanie ich obsahu technologickými prostriedkami s heslom minimálnej dĺžky 12 znakov sa riadi postupom podľa kapitoly 5.1.3 o zálohovaní dát.

Oprávnená osoba je povinná skontrolovať obsah dátového nosiča pred prenosom či neobsahuje nezašifrované osobné údaje.

Prenášanie osobných údajov prostredníctvom elektronických komunikačných sietí (napr. email) je povolené len oprávnenému príjemcovi (napr. na spracovanie účtovníctva) len v zašifrovanej forme napr. uložením dátových súborov do heslom chráneného .zip archívu, alebo zašifrovaného kontajnera a zaslanie tohto chránenej prílohy emailom. Zasielanie osobných údajov týkajúce sa konkrétneho zamestnanca emailom je povolené zasielať:

a) len na emailovú adresu tohto zamestnanca, ktorú tento zamestnanec poskytol,

b) len ako prílohu elektronickej pošty vo forme zašifrovaného súboru s heslom (napr. zip súbor výplatnej pásky chránený heslom).

c) heslo k prílohe nesmie byť zasielané súčasne e-mailom, ale napr. môže byť vopred dohodnuté, alebo zaslané iným kanálom (napr. sms-kou na mobil dotknutej osoby).

Prenos osobných údajov cez portály napr. medzi prevádzkovateľom alebo sprostredkovateľom a oprávneným subjektom (napr. Sociálna poisťovňa, zdravotné poisťovne, Finančná správa SR, atď.), je povolený vyplnením údajových formulárov na zabezpečenej stránke oprávneného subjektu. Pred prihlásením sa na portál je používateľ povinný overiť dôveryhodnosť stránky prostredníctvom platnosti certifikátu stránky (kliknutím na zelený zámok pred „https://...“ -> pripojenie -> informácie o certifikáte -> porovnanie názvu subjektu komu bol certifikát vydaný s názvom stránky/s názvom inštitúcie kam sa prihlasujeme).

V prípade potreby verbálnej komunikácie o informáciách napr. osobná návšteva pobočky Sociálnej poisťovne sa dodržiava zvýšená diskrétnosť a opatrnosť (napr. z hľadiska udržiavania intenzity hlasu, toto miesto verejne prístupné verejnosti).

6.5 Informovanie a vybavovanie žiadostí dotknutých osôb

Pri získavaní osobných údajov od dotknutej osoby je prevádzkovateľ informuje dotknutú osobu o politike ochrany súkromia a prípadne poskytne aj podrobnejšie písomné oboznámenie o spracovaní osobných údajov a na požiadanie zodpovie prípadné otázky. Dokument politika ochrany súkromia obsahuje informácie:

- identifikačné údaje a kontaktné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený,
- kontaktné údaje zodpovednej osoby, ak je určená,
- účel spracúvania osobných údajov, na ktorý sú osobné údaje určené, ako aj právny základ spracúvania osobných údajov,
- oprávnené záujmy prevádzkovateľa alebo tretej strany, ak sa osobné údaje spracúvajú podľa § 13 ods. 1 písm. f),
- identifikáciu príjemcu alebo kategóriu príjemcu, ak existuje,
- informáciu o tom, že prevádzkovateľ zamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii, identifikáciu tretej krajiny alebo medzinárodnej organizácie, informáciu o existencii alebo neexistencii rozhodnutia Európskej komisie (ďalej len „Komisia“) o primeranosti alebo odkaz na primerané záruky alebo vhodné záruky a prostriedky na získanie ich kópie alebo informáciu o tom, kde boli sprístupnené, ak prevádzkovateľ zamýšľa prenos podľa § 48 ods. 2, § 49 alebo § 51 ods. 1 a 2. ZoOOU,
- o dobe uchovávania osobných údajov; ak to nie je možné, informácie o kritériách jej určenia,
- o práve požadovať od prevádzkovateľa prístup k osobným údajom týkajúcich sa dotknutej osoby,
- o práve na opravu osobných údajov,
- o práve na vymazanie osobných údajov alebo o práve na obmedzenie spracúvania osobných údajov,
- o práve namietať spracúvanie osobných údajov,
- o práve na prenosnosť osobných údajov,
- práve kedykoľvek svoj súhlas odvolať,
- práve podať návrh na začatie konania podľa § 100 ZoOOU,
- o tom, či je poskytovanie osobných údajov zákonnou požiadavkou alebo zmluvnou požiadavkou alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, a o tom, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj o možných následkoch neposkytnutia osobných údajov,

- o existencii automatizovaného individuálneho rozhodovania vrátane profilovania podľa § 28 ods. 1 a 4 ZoOOU; v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie o použitom postupe, ako aj o význame a predpokladaných dôsledkoch takého spracúvania osobných údajov pre dotknutú osobu.
- o inom účele a ďalšie relevantné informácie, ak má prevádzkovateľ v úmysle ďalej spracúvať osobné údaje na iný účel ako ten, na ktorý boli získané.

Prevádzkovateľ je povinný vybaviť a odpovedať na uplatnené právo dotknutej osoby bez zbytočného odkladu, najneskôr však do jedného mesiaca, odkedy si dotknutá osoby právo uplatnila.

V prípade požiadavky dotknutej osoby odovzdať jej osobné údaje, prevádzkovateľ zabezpečí vhodným opatrením, aby s odovzdanými údajmi neboli sprístupnené, odovzdané osobné údaje iných osôb.

V prípade požiadavky na odovzdanie kamerového záznamu, musí byť tento záznam pred odovzdaním technicky upravený, tak, aby neobsahoval osobné údaje iných osôb. Technickou úpravou sa rozumie rozostretie zobrazenia iných osôb, okrem dotknutej, spôsobom znemožňujúcom ich identifikáciu.

V prípade namietania dotknutej osoby voči spracúvaniu osobných údajov, prevádzkovateľ posúdi rozsah, účel, právny základ spracúvania osobných údajov a v prípadoch, ak ide o vyhodnotenie legitímnych oprávnených záujmov prevádzkovateľa, tak prevádzkovateľ vykoná test proporcionality. V prípade, ak sa nepreukáže presvedčivý legitímny oprávnený dôvod na spracúvanie, prevádzkovateľ nebudeme osobné údaje namietajúcej osoby ďalej spracúvať.

7. Bezpečnostné incidenty

7.1 Oznámenie porušenia ochrany osobných údajov

Všetci zamestnanci, oprávnené osoby, sprostredkovateľ sú povinné zachovávať primeranú ostražitosť a každé čo i len podozrenie alebo porušenie ochrany osobných údajov oznámiť štatutárovi prevádzkovateľa.

Každý je povinný nahlásiť prevádzkovateľovi informácie o porušení ochrany osobných údajov. Prevádzkovateľ je povinný zdokumentovať každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu.

O incidente sa vyhotoví záznam, ktorý obsahuje:

- miesto, dátum a čas zistenia incidentu,
- opis spôsobu, ako bol incident zistený – uvedie sa najmä meno osoby, ktorá incident ohlásila,
- opis priebehu incidentu, jeho začiatku a skončenia, hrozby, ktoré incident vyvolal,
- opis prijatých opatrení,
- návrh na prijatie opatrení pre zabránenie opakovania incidentu,
- opis porušených opatrení, ktoré zapríčinili, že incident nastal,
- meno a priezvisko, podpis, kto záznam zapísal.

7.2 Postup odstraňovania následkov porušení ochrany osobných údajov

Prevádzkovateľ je povinný oznámiť úradu porušenie ochrany osobných údajov do 72 hodín po tom, ako sa o ňom dozvedel; to neplatí, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby.

Oznámenie o porušení ochrany osobných údajov bude obsahovať aspoň:

- opis povahy porušenia ochrany osobných údajov vrátane, podľa možnosti, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka a kategórií a približného počtu dotknutých záznamov o osobných údajoch;
- kontaktné údaje zodpovednej osoby v našej spoločnosti, kde možno získať viac informácií o porušení ochrany osobných údajov;
- opis pravdepodobných následkov porušenia ochrany osobných údajov;
- opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

Prevádzkovateľ po vyhodnotení rozsahu porušenia ochrany osobných údajov a jeho dopadov na osobné údaje zabezpečí odstránenie príčin porušenia ochrany osobných údajov a prijme potrebné opatrenia na vyriešenie incidentu.

7.3 Opatrenia pri bezpečnostných incidentoch

bezpečnostný incident	ohrozenie	opatrenia
vyzradenie alebo zverejnenie hesla pre vstup do informačného systému	narušenie integrity, strata, alebo zneužitie osobných údajov	• zmeniť všetky prihlasovacie heslá do informačného systému, • vykonať poučenie osôb o ochrane a utajení hesiel, • vykonať disciplinárne opatrenie pri preukázanom porušení ustanovení tejto smernice • vyhodnotiť incident a splniť informačné povinnosti podľa ZoOOÚ
prístup neoprávnenej osoby	narušenie integrity, strata, alebo zneužitie osobných údajov	• zmeniť všetky prihlasovacie heslá do informačného systému, • vykonať poučenie osôb o ochrane a utajení hesiel, • vykonať disciplinárne opatrenie pri preukázanom porušení ustanovení tejto smernice • vyhodnotiť incident a splniť informačné povinnosti podľa ZoOOÚ
narušenie priestorov prevádzkovateľa	narušenie integrity, strata alebo zneužitie osobných údajov	• zabezpečenie priestorov • vykonať disciplinárne opatrenie pri preukázanom porušení ustanovení tejto smernice

		• vyhodnotiť incident a splniť informačné povinnosti podľa ZoOOÚ
krádež, strata kľúčov	neoprávnený vstup do priestorov prevádzkovateľa, narušenie integrity, strata alebo zneužitie osobných údajov	• výmena zámkov • vykonať disciplinárne opatrenie pri preukázanom porušení ustanovení tejto smernice • vyhodnotiť incident a splniť informačné povinnosti podľa ZoOOÚ
strata, odcudzenie záložných médií, zmazanie dát v systéme, zásah do integrity dát,	strata alebo zneužitie osobných údajov, ak neboli dostatočne chránené šifrovaním s bezpečným heslom,	• zabezpečiť obnovenie dát • vykonať disciplinárne opatrenie pri preukázanom porušení ustanovení tejto smernice • vyhodnotiť incident a splniť informačné povinnosti podľa ZoOOÚ • zabezpečiť obnovenie dát zo zálohy osobných údajov v zašifrovanom kontajneri s bezpečným heslom • zabezpečiť priebežné zálohovanie dát - osobných údajov v zašifrovanom kontajneri s bezpečným heslom
napadnutie vírusom	narušenie integrity, strata, odcudzenie alebo zneužitie osobných údajov	• aktualizovať antivírovú ochranu, • nová inštalácia operačného systému tzv., „čistý disk“, • obnova údajov zo záložných médií, • neinštalovať software z neoverených zdrojov, • nepripájať neoverené zariadenia (USB disky, DVD/CD nosiče), • neotvárať nevyžiadané e-mailové prílohy, • sledovanie sieťovej aktivity na lokálnej sieti • vyhodnotiť incident a splniť informačné povinnosti podľa ZoOOÚ
neautorizovaný vstup z vonkajšej siete	narušenie integrity, strata, odcudzenie alebo zneužitie osobných údajov	• analyzovať logy o prevádzke firewallu, routerov, • aktualizácia antivírového programu, • obnova údajov zo záložných médií, • skontrolovať a prehodnotiť nastavenia firewallu • zmena hesla administrátorského prístupu k routerom a firewallom
neautorizovaný prístup cez Wifi do vnútornej siete	narušenie integrity, strata, odcudzenie alebo zneužitie osobných údajov	• zmena hesla pre prístup cez Wifi, • nastavenie filtrácie prístupu podľa MAC adries, • obnovenie konfigurácie Wifi routra,

		• kontrola záznamov prístupu na Wifi routri

8. Likvidácia osobných údajov

Likvidácia osobných údajov je postup zrušenia osobných údajov najmä ich vymazaním, fyzickým zničením hmotných nosičov (médií, listín), spoľahlivo zabezpečujúce neobnoviteľnosť, nereprodukovateľnosť osobných údajov.

Likvidáciu osobných údajov, ktoré sú zachytené na nepotrebných listinách (bez archivačnej hodnoty), vykoná oprávnená osoba fyzickým zničením listiny, najmä skartáciou.

Osobné údaje z pamäťových médií (USB disky, CD, DVD nosiče, pamäťové karty a pod.) sa likvidujú bezpečným vymazaním, naformátovaním nosiča a následným úplným zaplnením kapacity nosiča napr. náhodnými údajmi alebo verejne publikovanými súbormi neobsahujúce osobné údaje, tak aby sa z nich zmazané súbory s osobnými údajmi nedali reprodukovať.

Bezpečné vymazanie osobných údajov z dátových nosičov sa vykoná týmto postupom:

1. otvorí sa súbor elektronického dokumentu (napr. editorom),
2. prepíše sa obsah dokumentu náhodným textom,
3. dokument sa uloží pod rovnakým menom pod akým bol otvorený,
4. vymaže sa súbor z adresára.

Pre fyzickú likvidáciu dátových nosičov osobných údajov (USB, CD a DVD médiá a pod.) sa použije skartovacie zariadenie určené na drvenie hmotných nosičov.

Za dodržiavanie postupu likvidácie osobných údajov zodpovedá oprávnená osoba, kontrolu dodržiavania postupu likvidácie osobných údajov zabezpečuje štatutár prevádzkovateľa v rámci pravidelnej a náhodnej kontroly.

Opatrenia na likvidáciu osobných údajov uložené na technológiách elektronickej platformy služieb dostupných na portáli https://zoznamtesa.sk/ vykonáva poverený sprostredkovateľ

9. Implementácia a riadenie opatrení, kontrolná činnosť

9.1 Implementácia a riadenie opatrení na ochranu osobných údajov

Prevádzkovateľ konajúc štatutárnym orgánom:

- rozhoduje o schvaľovaní tejto smernice,
- určuje rozsah technických, organizačných a bezpečnostných opatrení,
- zabezpečenie súladu spracúvania osobných údajov s nariadením GDPR a ZoOOÚ,
- prijíma opatrenia na návrh zodpovednej osoby na základe vyhodnotenia incidentov

Zodpovedná osoba prevádzkovateľa:

- poskytuje odborné poradenstvo štatutárnemu orgánu,
- kontroluje súlad spracovania osobných údajov s GDPR a ZoOOÚ,

Táto smernica je záväzná pre zamestnancov prevádzkovateľa, ktorí sú povinní:

- riadiť sa jej ustanoveniami a dodržiavať smernicou uložené povinnosti,
- vykonávať spracovanie osobných údajov rozsahu poverenia alebo pokynov prevádzkovateľa,
- vykonávať uložené opatrenia,
- zúčastniť sa školení o ochrane osobných údajov.

9.2 Kontrolná činnosť

Kontrolnú činnosť vykonáva štatutár prevádzkovateľa, zodpovedná osoba, poverený členovia komisie alebo poverený zamestnanec prevádzkovateľa, ktorá je zameraná na dodržiavanie zásad spracúvania osobných údajov, dodržiavania technických, organizačných a bezpečnostných opatrení spracúvania osobných údajov.

Kontrolnú činnosť prevádzkovateľ vykonáva:

- pravidelne, minimálne raz polročne,
- náhodne, kedykoľvek,
- následnú kontrolu po zistení porušenia zásad alebo porušenia technických, organizačných a bezpečnostných opatrení spracúvania osobných údajov.

Kontrolná činnosť prevádzkovateľa sa zameriava najmä na dodržiavanie:

- účelu a rozsahu spracovávaných osobných údajov, zákonnosť spracovávania osobných údajov,
- spôsobu vykonávaných spracovateľských operácií, najmä dodržiavanie mlčanlivosti,
- spôsob a lehotu vybavenia o žiadostí dotknutých osôb,
- dodržiavania opatrení tejto smernice.

O priebehu a výsledku vykonanej kontroly spíše prevádzkovateľ protokol, ktorý obsahuje najmä:

- miesto, dátum a čas kontroly,
- rozsah kontroly,
- opis zistených nedostatkov,
- opis prijatých opatrení,
- zoznam osôb zodpovedných za vykonanie opatrení a určenie termínu vykonania opatrení,
- dátum kontroly splnenia opatrení,
- meno a priezvisko, podpis kontrolujúcej osoby.

príloha č. 1 – Záznam o poučení oprávnenej osoby

Záznam o poučení oprávnenej osoby

Prevádzkovateľ:

Mária Hudáková, Ag. Rosa, IČO 37 163 256, miesto podnikania 93021 Dunajský Klátov 41, vedená v registri Okresné úradu Dunajská Streda, číslo živnostenského registra 201-13735.

Rozsah poučenia:

- technické, organizačné a bezpečnostné opatreniach spracovania osobných údajov:
  - postup pri získavaní osobných údajov
  - povinnosť zachovávať diskrétnosť pri získavaní osobných údajov a mlčanlivosť o osobných údajoch
  - manipulácia a uchovávanie listín s osobnými údajmi
- zásady ochrany osobných údajov:
  - účely spracovávania osobných údajov
  - právny základ spracovávania osobných údajov
  - rozsah spracovávania osobných údajov prevádzkovateľom
- politika ochrany osobných údajov
- povinnosti vyplývajúce zo zákona č. 18/2018 Z. z. a nariadenia GDPR a o zodpovednosti za ich porušenie

Dole podpísaní sa týmto zaväzujeme dodržiavať mlčanlivosť o osobných údajoch, s ktorými prídeme do styku pri činnostiach pre prevádzkovateľa to aj po skončení vzťahu k prevádzkovateľovi.

Poučené osoby:

p.č.	titul, meno a priezvisko	pracovné zaradenie	podpis poučenej osoby	dátum ukončenia činnosti

Poučenie vykonala dňa:.....

.....

Mária Hudáková, Ag. Rosa

IČO 37 163 256

miesto podnikania
93021 Dunajský Klátov 41

príloha č. 2 - Záznam o bezpečnostnom incidente

Záznam o bezpečnostnom incidente

Prevádzkovateľ:

Mária Hudáková, Ag. Rosa, IČO 37 163 256, miesto podnikania 93021 Dunajský Klátov 41, vedená v registri Okresné úradu Dunajská Streda, číslo živnostenského registra 201-13735.

Miesto, dátum a čas zistenia incidentu: .....
Opis spôsobu, ako bol incident zistený: (uvedie sa najmä meno osoby, ktorá incident ohlásila):

.....

.....
Opis priebehu incidentu, jeho začiatku a skončenia, hrozby, ktoré incident vyvolal:

.....

.....
Opis prijatých opatrení:

.....

.....
Návrh na prijatie opatrení pre zabránenie opakovania incidentu:

.....

.....
Opis porušených opatrení, ktoré zapríčinili, že incident nastal:

.....

.....

Meno priezvisko a podpis: .....

príloha č. 3 - Záznam o kontrole

Záznam o kontrole

dodržiavania zásad a technických, organizačných a bezpečnostných opatrení

spracúvania osobných údajov

Prevádzkovateľ:

Mária Hudáková, Ag. Rosa, IČO 37 163 256, miesto podnikania 93021 Dunajský Klátov 41, vedená v registri Okresné úradu Dunajská Streda, číslo živnostenského registra 201-13735.

Miesto, dátum a čas kontroly: .....

Rozsah kontroly:

.....

.....

Opis zistených nedostatkov:

.....

.....

Opis prijatých opatrení:

.....

.....

Osoby zodpovedné za vykonanie opatrení a termín vykonania opatrení:

.....

.....

Dátum kontroly splnenia opatrení: .....

Meno priezvisko a podpis kontrolujúcej osoby: .....

príloha č. 4 – Záznam o poučení servisného technika

Záznam o poučení servisného technika

Prevádzkovateľ:

Mária Hudáková, Ag. Rosa, IČO 37 163 256, miesto podnikania 93021 Dunajský Klátov 41, vedená v registri Okresné úradu Dunajská Streda, číslo živnostenského registra 201-13735.

Rozsah poučenia o:

- povinnosti zachovávať mlčanlivosť o osobných údajoch o ktorých sa servisný technik dozvedel pri výkone servisnej činnosti,
- zákaze oboznamovať sa s osobnými údajmi, s ktorými príde do styku,
- právnej zodpovednosti za porušenie zásad ochrany osobných údajov,
- povinnostiach vyplývajúcich zo zákona č. 18/2018 Z. z. a nariadenia GDPR a o zodpovednosti za ich porušenie a zo smernice o technických, organizačných a bezpečnostných opatreniach spracovania osobných údajov,

Dole podpísaní sa týmto zaväzujeme dodržiavať mlčanlivosť o osobných údajoch, s ktorými prídeme do styku pri činnostiach pre prevádzkovateľa a to aj po skončení vzťahu k prevádzkovateľovi a zaväzujeme sa neoboznamovať sa s osobnými údajmi, s ktorými prídeme do styku.

Poučené osoby:

p.č.	titul, meno a priezvisko	vykonávaný servis	podpis poučenej osoby

Poučenie vykonala dňa:.....

.....

Mária Hudáková, Ag. Rosa
IČO 37 163 256
miesto podnikania
93021 Dunajský Klátov 41