**BEZPEČNOSTNÉ OPATRENIA**

ZÁSADY BEZPEČNOSTI PRE POVERENÉ OSOBY – POUŽÍVATEĽOV IS,

ZÁSADY BEZPEČNOSTI PRI SPRÁVE DATABÁZ A APLIKÁCIÍ IS,

ZÁSADY OCHRANY OSOBNÝCH ÚDAJOV V LISTINÁCH A DOKUMENTOCH PRI SPRACOVÁVANÍ OSOBNÝCH ÚDAJOV,

ZÁSADY BEZPEČNOSTI PRI PREVÁDZKE INFORMAČNÝCH A KOMUNIKAČNÝCH TECHNOLÓGIÍ NA PRACOVISKU IS,

INFORMAČNÁ POVINNOSŤ PREVÁDZKOVATEĽA DOTKNUTÝM OSOBÁM

Dokument: Bezpečnostné opatrenia

**Prevádzkovateľ:**

PETAN parket, s.r.o.

M.R.Štefánika 314

956 18 Bošany

IČO: 50 341 189

Kvetoslava Turčeková

Tel.č.: 0905 386 423

e-mail: petanparket@gmail.com

Obsah

[HLAVNÉ ZÁSADY OCHRANY OSOBNÝCH ÚDAJOV 3](#_Toc139620232)

[HLAVNÉ ZÁSADY GDPR 4](#_Toc139620233)

[ZÁSADY BEZPEČNOSTI PRE POVERENÉ OSOBY – POUŽÍVATEĽOV IS 4](#_Toc139620234)

[VŠEOBECNÉ USTANOVENIA 4](#_Toc139620235)

[MANIPULÁCIA S TECHNICKÝMI PROSTRIEDKAMI IS 5](#_Toc139620236)

[MANIPULÁCIA S DÁTOVÝMI NOSIČMI OSOBNÝCH ÚDAJOV (PAMÄŤOVÝMI MÉDIAMI IS) 5](#_Toc139620237)

[ZÁKLADNÉ ZÁSADY PRE MANIPULÁCIU S POROGRAMOVÝM VYBAVENÍM IS 6](#_Toc139620238)

[OCHRANA PRED NEOPRÁVNENÝM PRÍSTUPOM A RIADENIE PRÍSTUPU OPRÁVNENÝCH OSÔB 7](#_Toc139620239)

[MANIPULÁCIA S ÚDAJMI IS 7](#_Toc139620240)

[ANTIVÍRUSOVÉ OPATRENIA 8](#_Toc139620241)

[ZAZNAMENÁVANIE A HLÁSENIE PROBLÉMOV S PRACOVNOU STANICOU 8](#_Toc139620242)

[PRÍSTUP DO SIETE INTERNET 9](#_Toc139620243)

[MANIPULÁCIA S TECHNICKÝMI PROSTRIEDKAMI IS 10](#_Toc139620244)

[PRÍSTUPOVÉ HESLÁ 10](#_Toc139620245)

[MANIPULÁCIA S ÚDAJMI IS 11](#_Toc139620246)

[ZÁSADY BEZPEČNOSTI PRI SPRÁVE DATABÁZ A APLIKÁCIÍ IS 11](#_Toc139620247)

[VŠEOBECNÉ USTANOVENIA 11](#_Toc139620248)

[PODMIENKY ZAKLADANIA DATABÁZ OSOBNÝCH ÚDAJOV V IS 11](#_Toc139620249)

[ZÁKLADNÉ ZÁSADY BEZPEČNOSTI PRI SPRÁVE DATABÁZ A APLIKÁCIÍ 12](#_Toc139620250)

[ZÁDADY BEZPEČNOSTI PRI PREVÁDZKE INFORMAČNÝCH A KOMUNIKAČNÝCH TECHNOLÓGIÍ NA PRACOVISKU IS 13](#_Toc139620251)

[VŠEOBECNÉ USTANOVENIA 13](#_Toc139620252)

[KĽÚČOVÉ KOMPONENTY IS 14](#_Toc139620253)

[ZÁKLADNÉ ZÁSADY BEZPEČNEJ PREVÁDZKY IS 14](#_Toc139620254)

[ZÁLOHOVANIE 15](#_Toc139620255)

[ZÁSADY RIEŠENIA NEPREDVÍDANÝCH UDALOSTÍ S DOPADOM NA PREVÁDZKU IS 16](#_Toc139620256)

[ZÁSADY RIEŠENIA BEZPEČNOSTNÝCH INCIDENTOV 16](#_Toc139620257)

[PREVENCIA 16](#_Toc139620258)

[INFORMAČNÁ POVINOSŤ PREVÁDZKOVATEĽA DOTKNUTÝM OSOBÁM 17](#_Toc139620259)

[INFORMÁCIE, KTORÉ SA MAJÚ POSKYTOVAŤ PRI ZÍSKAVANÍ OSOBNÝCH ÚDAJOV OD DOTKNUTEJ OSOBY 17](#_Toc139620260)

[INFORMÁCIE, KTORÉ SA MAJÚ POSKYTNÚŤ, AK OSOBNÉ ÚDAJE NEBOLI ZÍSKANÉ OD DOTKNUTEJ OSOBY 18](#_Toc139620261)

[PRÁVO DOTKNUTEJ OSOBY NA PRÍSTUP K ÚDAJOM 18](#_Toc139620262)

[SPÔSOB POSKYTOVANIA ŽIADOSTI DOTKNUTEJ OSOBY 19](#_Toc139620263)

[PODMIENKY VYJADRENIA SÚHLASU SO SPRACOVANÍM OSOBNÝCH ÚDAJOV 20](#_Toc139620264)

[OSOBITNÉ KATEGÓRIE OSOBNÝCH ÚDAJOV 21](#_Toc139620265)

[KOPÍROVANIE, SKENOVANIE A ZAZNAMENÁVANIE ÚRADNÝCH DOKLADOV VŠEOBECNE 21](#_Toc139620266)

[SPRÁVNOSŤ A AKTUÁLNOSŤ OSOBNÝCH ÚDAJOV 22](#_Toc139620267)

[LIKVIDÁCIA OSOBNÝCH ÚDAJOV 22](#_Toc139620268)

[ČO JE OSOBNÝ ÚDAJ 23](#_Toc139620269)

# HLAVNÉ ZÁSADY OCHRANY OSOBNÝCH ÚDAJOV

1. Spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe („zákonnosť, spravodlivosť a transparentnosť“)
2. Získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi; ďalšie spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či štatistické účely sa v súlade s čl. 89 ods. 1 nepovažuje za nezlučiteľné s pôvodnými účelmi („obmedzenie účelu“)
3. Primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú („minimalizácia údajov“).
4. Správne a podľa potreby aktualizované; musia sa prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia („správnosť“).
5. Smernica Európskeho parlamentu a Rady EÚ 2015/1535 z 9. Septembra 2015, ktorou sa stanovuje postup pri poskytovaní informácií v oblasti technických predpisov a pravidiel vzťahujúcich sa na služby informačnej spoločnosti (ú. V. Eú I 241, 17.9. 2015, s. 1).
6. Uchovávanie vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú.
7. Osobné údaje sa môžu uchovávať dlhšie, pokiaľ sa budú spracúvať výlučne na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu, či na štatistické účely v súlade s čl. 89 ods. 1 za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných týmto nariadením na ochranu práv a slobôd dotknutých osôb („minimalizácia uchovávania“).
8. Spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení („integrita a dôvernosť“).

# HLAVNÉ ZÁSADY GDPR

1. **Zákonnosť, spravodlivosť a transparentnosť**: osobné údaje môže prevádzkovateľ spracúvať len v prípade, ak disponuje primeraným právnym základom, napr. súhlasom alebo na základe osobitného právneho predpisu, či na účel plnenia zmluvy. Na transparentné spracúvanie osobných údajov sa vyžaduje, aby dotknutá osoba bola informovaná o rozsahu a spôsoboch spracúvania jej údajov.
2. **Obmedzenie účelu spracovania**: získavať osobné údaje dotknutých osôb je prípustné len na výslovne uvedené a legitímne účely a môžu byť ďalej spracúvané len na účel, na ktorý boli získané. Získané osobné údaje sa nesmú ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s účelom, na ktoré boli tieto osobné údaje získané (okrem výnimiek ustanovených v GDPR, napr. v prípade kompatibilného účelu). Je neprípustné získavať osobné údaje pod zámienkou iného účelu spracúvania alebo inej činnosti.
3. **Minimalizácia údajov (nevyhnutnosť):** rozsah spracúvaných osobných údajov dotknutých osôb má byť primeraný (obmedzený) vzhľadom na účel, na ktorý sa spracúvajú, tzn. na určený účel sa majú spracúvať len osobné údaje, ktoré sú na naplnenie daného účelu nevyhnutné.
4. **Správnosť osobných údajov**: prevádzkovateľ má povinnosť zabezpečiť, aby sa osobné údaje dotknutých osôb, ktoré sú nesprávne bezodkladne vymazali alebo opravili.
5. **Minimalizácia uchovávania osobných údajov (likvidácia)**: osobné údaje majú byť uchovávané najviac do doby potrebnej na naplnenie účelov, na ktoré sú údaje spracúvané. Uchovávanie osobných údajov na dlhšiu dobu je možné výlučne v prípadoch špecifikovaných v GDPR. Okrem toho je potrebné zabezpečiť, aby boli uchovávané len nevyhnutné údaje.
6. **Integrita a dôvernosť (bezpečnosť)**: osobné údaje majú byť spracúvané výlučne takým spôsobom, aby sa zabezpečila primeraná bezpečnosť pri ich spracúvaní, ako aj pred ich nezákonným spracúvaním, náhodnou stratou, zničením alebo poškodením. Zabezpečenie ochrany osobných údajov má byť realizované prostredníctvom primeraných technických alebo organizačných opatrení.
7. **Zodpovednosť**: prevádzkovateľ a rovnako aj sprostredkovateľ musia vedieť preukázať, že splnili požiadavky GDPR počas celej doby spracúvania osobných údajov.

# ZÁSADY BEZPEČNOSTI PRE POVERENÉ OSOBY – POUŽÍVATEĽOV IS

# VŠEOBECNÉ USTANOVENIA

Táto časť dokumentu upravuje základné pravidlá pre zaistenie bezpečnej a spoľahlivej prevádzky pracovných staníc, na ktorých sú prevádzkované IS.

Poverenými osobami – používateľmi IS sú poverené osoby, ktoré na základe pracovnej náplne a na základe oprávnenia, prostredníctvom technických prostriedkov (pracovnej stanice, počítača) využívajú služby IS, teda spracovávajú osobné údaje uložené v IS, alebo majú k nim prístup za účelom plnenia svojich pracovných povinností.

V podmienkach prevádzkovateľa sa poverené osoby – používatelia IS riadia nasledovnými článkami tejto časti smernice.

# MANIPULÁCIA S TECHNICKÝMI PROSTRIEDKAMI IS

1. Pracovné stanice musia byť v rámci chráneného priestoru umiestnené tak, aby vplyvom okolia nedošlo k neúmyselnému poškodeniu alebo poruche zariadenia (pádom, teplou vodou, elektromagnetickým žiarením, priamym slnečným svetlom, ...).
2. Používateľ IS môže manipulovať s pracovnými stanicami (zapínať, používať, vypínať) len v súlade s inštrukciami výrobcu, resp. dodávateľa zariadenia alebo dodávateľa príslušného programového vybavenia.
3. Používateľ IS nesmie znižovať životnosť pracovných staníc zlým zaobchádzaním a ich znečisťovaním.
4. V blízkosti technických zariadení IS prevádzkovateľa je zakázané jesť, piť a fajčiť, ale aj vykonávať iné činnosti hroziace znečistením technických zariadení, resp. znížením ich životnosti alebo spoľahlivosti (vibrácie, vystavovanie nadmernej prašnosti, vysávanie v blízkosti zapnutého zariadenia a podobne).
5. Používateľ IS nemôže bez súhlasu zodpovednej osoby, resp. štatutára prevádzkovateľa:
6. robiť zásahy do pracovných staníc,
7. pripájať k pracovným staniciam ďalšie technické zariadenia,
8. odpájať technické zariadenia pracovnej stanice,
9. premiestňovať pracovné stanice,
10. manipulovať s ovládacími prvkami pracovnej stanice okrem tých, ktoré sú umiestnené na vonkajšej strane skrinky pracovnej stanice, tlačiarne a krytu monitora (zapínanie, vypínanie a resetovanie počítača a tlačiarne, vkladanie a vyberanie USB kľúčov a CD/DVD mechaník, výmena tonera bez oboznámenia sa so spôsobom výmeny).
11. Opravy a úpravy pracovnej stanice môže vykonávať len prizvaný kvalifikovaný externý špecialita. Externý špecialista pritom môže zasahovať do pracovnej stanice iba s preukázateľným súhlasom zodpovednej osoby, resp. štatutára prevádzkovateľa. Používateľ IS je povinný odmietnuť prístup k pracovnej stanici osobe, ktorá sa nepreukáže takýmto súhlasom.
12. Čistenie povrchu technických zariadení pracovnej stanice od prachu je v kompetencii používateľa IS. Vnútorné čistenie zariadení IS prevádzkovateľa môže vykonávať len kvalifikovaný externý špecialista pri dodržaní podmienok bodu 6.

# MANIPULÁCIA S DÁTOVÝMI NOSIČMI OSOBNÝCH ÚDAJOV (PAMÄŤOVÝMI MÉDIAMI IS)

Na dátové nosiče osobných údajov je možné ukladať záložné kópie dát s osobnými údajmi iba šifrovaným spôsobom, čo musí zabezpečiť buď softwarový komponent IS (aplikačný program automatizovaného alebo poloautomatizovaného spracovávania osobných údajov v IS) alebo špeciálny zálohovací software obsahujúci šifrovaciu funkcionalitu.

1. Pamäťové médiá IS prevádzkovateľa sú pevné disky, USB kľúče a ostatné média používané na uchovávanie dát v elektronickej forme.
2. Pamäťové médiá musia byť uložené tak, aby nedošlo k poškodeniu záznamu, predovšetkým nesmú byť vystavované pôsobeniu silného elektromagnetického poľa, teplotným extrémom, vlhkosti a prašnosti.
3. Do mechaník prenosných pamäťových médií nesmú byť vkladané znečistené alebo poškodené médiá.
4. Pamäťové médiá obsahujúce citlivé údaje musia byť skladované na bezpečnom mieste (uzamykateľný stôl, trezor a pod.).

# ZÁKLADNÉ ZÁSADY PRE MANIPULÁCIU S POROGRAMOVÝM VYBAVENÍM IS

1. Používateľ IS môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované externým špecialistom, resp. nainštalované s preukázateľným súhlasom zodpovednej osoby, resp. štatutára prevádzkovateľa. Používateľ IS nemôže na pracovnej stanici inštalovať ani odinštalovať žiadne programové vybavenie a tiež nemôže meniť konfiguráciu programového vybavenia s výnimkou zmien, s ktorými bol riade oboznámený na školení o používaní príslušného programového vybavenia.
2. Používateľ IS nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.
3. Je zakázaný akýkoľvek zásah do nastavení CMOS pracovnej stanice. Povolený zásah sa netýka prípadnej odôvodnenej zmeny počiatočného štartovacieho hesla.
4. Používatelia IS pred opustením pracoviska sú povinní ukončiť prácu s programovým vybavením a pracovnú stanicu vypnúť.
5. Pri krátkodobej neprítomnosti môže používateľ IS, pokiaľ mu to používané programové vybavenie umožňuje, nahradiť vypnutie pracovnej stanice spustením šetriča obrazovky s heslom pre jeho ukončenie.
6. Používatelia IS sú povinní vykonávať základnú údržbu pracovnej stanice – okrem vyčistenia povrchu pracovnej stanice (monitor, klávesnica) aspoň raz mesačne čistenie (odstraňovanie nepotrebných súborov) svojich dátových adresárov a pomocných adresárov operačného systému (vrátane adresára Kôš), prípadne spusteniu profylaktických programov (podľa použitého operačného programu – napr. scandisk, defragmentácia disku a pod.). so spôsobom vykonávania základnej údržby systému sa oboznámia na školení.
7. Používatelia IS sú povinní po inštalácii novej verzie programového vybavenia po dobu minimálne jedného týždňa venovať zvýšenú pozornosť činnosti systému a kontrolovať správnosť výsledkov jeho práce. Prípadné odchýlky od požadovaného stavu sú povinní čo najúplnejšie zdokumentovať a bezodkladne ohlásiť zodpovednej osobe.

# OCHRANA PRED NEOPRÁVNENÝM PRÍSTUPOM A RIADENIE PRÍSTUPU OPRÁVNENÝCH OSÔB

Na fyzické dátové stanice osobných údajov je možné ukladať záložné kópie dát s osobnými údajmi iba šifrovaným spôsobom, čo musí zabezpečiť softwarový komponent IS (aplikačný program automatizovaného alebo poloautomatizovaného spracovávania osobných údajov v IS) alebo špeciálny zálohovací software obsahujúci šifrovaciu funkcionalitu.

Prístup tretích strán k IS musí byť zamedzený v najväčšej možnej miere a pre odôvodnenú potrebu takéhoto prístupu musia byť jasne stanovené, prehľadné a kontrolovateľné pravidlá.

Oprávnené osoby pre prístup k IS, resp. k spracovávaniu osobných údajov v IS musia mať pred samotným prístupom k IS zabezpečenú:

1. **identifikáciu** – jednoznačné identifikovanie oprávnenej osoby pomocou identifikátora (napr. identifikačného kľúča zvereného oprávnenej osobe, resp. uloženého na GRID karte alebo elektronickom zariadení – „token“)
2. **autentizáciu** – overenie identity jedinečným príznakom, osobné heslo, osobný certifikát vystavený na konkrétnu osobu

Softwarový komponent IS musí zaznamenávať všetky vstupy (log in) a ukončenia vstupov (log out) poverenej osoby do IS a do záznamu doplniť časový údaj.

1. Používateľ je povinný svoje prístupové heslá meniť najmenej jedenkrát za rok, prípadne aj na pokyn zodpovednej osoby, resp. štatutára prevádzkovateľa.
2. Prístupové heslá používateľa IS musia mať aspoň 8 znakov (prístupové heslo šetriča obrazovky aspoň 4 znaky). Používateľ IS nesmie ako heslo použiť takú kombináciu znakov, ktorú by bolo možné priradiť k jeho osobe, akými sú napr. meno používateľa a jeho rodinných príslušníkov napísané spredu či odzadu, telefónne číslo domov alebo na pracovisko.
3. Používateľ IS musí svoje prístupové heslo používať tak, aby sa ho nemohla dozvedieť iná osoba (vrátane iných používateľov). Musí si byť vedomý svojej zodpovednosti za aktivity v IS, ktoré sa vykonajú pod jeho menom a heslom.
4. V prípade podozrenia, že iná osoba pozná heslo používateľa IS, je tento povinný príslušné heslo okamžite zmeniť a svoje podozrenie ohlásiť zodpovednej osobe.
5. Používateľ IS sa prihlasuje do aplikácie pod svojím menom a svojím heslom aj v prípade, že pracuje na pracovnej stanici pridelenej inému používateľovi.

# MANIPULÁCIA S ÚDAJMI IS

1. Súbory údajov na lokálnom disku pracovnej stanice, ktoré používateľ IS vytvára a používa pri svojej práci, je povinný si zálohovať minimálne raz mesačne, s prihliadnutím na rozsah údajov i dvakrát mesačne. So spôsobom zálohovania sa oboznámi na školení. Používateľ IS tieto údaje zálohuje na USB kľúč alebo na CD/DVD a uskladňuje v zamknutej zásuvke stola alebo v zamknutej skrinke – kľúče od zásuvky, resp. skrinky nesmú zostať voľne prístupné.
2. Používateľ IS môže vytvárať z aplikácie tlačové výstupy len v rozsahu určenom jeho pracovnou náplňou. V prípade výstupov obsahujúcich údaje dôverného charakteru (osobné údaje) musí zabezpečiť, aby k príslušnej tlačiarni nemala počas tlačenia výstupov nekontrolovateľný prístup neoprávnená osoba. Vytlačené výstupy obsahujúce údaje dôverného charakteru musia byť skladované alebo zlikvidované tak, aby nedošlo k narušeniu ich dôvernosti.
3. Používateľ IS môže poskytovať údaje IS externým subjektom len v rozsahu určenom jeho pracovnou náplňou a ďalšími predpismi. Výnimku tvoria údaje už zverejnené alebo určené na zverejnenie.

# ANTIVÍRUSOVÉ OPATRENIA

1. V prípade, že sa na pracovnej ploche používateľa IS zobrazí varovanie, že sa na disku alebo vloženom USB kľúči nachádza vírus, nesmie toto varovanie ignorovať. V prípade, že zavírený USB kľúč patrí inému subjektu, viditeľne a výrazne ho označí ako zavírený a vráti ju danému subjektu. V prípade zavírenia pevného disku alebo USB kľúča, používateľ túto skutočnosť bezodkladne oznámi zodpovednej osobe, prípadne po konzultácii s ňou vykoná antivírovú „dezinfekciu“ príslušného pamäťového média. So spôsobom vykonania antivírovej kontroly a dezinfekcie sa oboznámi na školeníV prípade objavenia vírusu v prijatej elektronickej pošte používateľa IS, bezodkladne o tejto udalosti upovedomí zodpovednú osobu, ako aj odosielateľa predmetnej elektronickej pošty. V žiadnom prípade zavírenú elektronickú poštu neposiela inému adresátovi a na svojej pracovnej stanici ju zmaže – odstráni a priečinok „Odstránená pošta“ vyprázdni.

# ZAZNAMENÁVANIE A HLÁSENIE PROBLÉMOV S PRACOVNOU STANICOU

1. Používateľ IS používajúci pracovnú stanicu zaznamená a zodpovednej osobe bezodkladne ohlási každú vnímateľnú odchýlku od bežnej činnosti pracovnej stanice, predovšetkým však nasledovné udalosti:
2. hlásenia chýb operačného systému a aplikácií, s ktorými používateľ pracuje (presný prepis chybového hlásenia) spolu so stručným popisom situácie (vykonávaných akcií), počas ktorej sa toto hlásenie vyskytlo, problémy s technickými zariadeniami pracovnej stanice spolu s popisom situácie, počas ktorej k problémom došlo (popis akcií, zadávaných údajov a/alebo viditeľných javov, ktoré predchádzali, resp. nasledovali výskyt problému).
3. Používateľ IS používajúci pracovnú stanicu zaznamená svojmu nadriadenému následne zodpovednej osobe bezodkladne každú udalosť, ktorá by mohla indikovať porušenie bezpečnosti IS, predovšetkým však nasledovné udalosti:
4. výskyt vírusu (prepis varovného hlásenia)
5. únik údajov s informáciou, aké informácie unikli, kam a ako
6. odcudzenie médií s údajmi z pracovnej stanice
7. odcudzenie technických zariadení pracovnej stanice,
8. neoprávnený zásah do technických zariadení pracovnej stanice,
9. neoprávnený zásah do programového vybavenia pracovnej stanice (vrátane výskytu nových súborov alebo adresárov na disku pracovnej stanice) alebo do nastavenia jeho parametrov (napr. nastavené zdieľanie disku alebo adresárov pracovnej stanice)
10. Vyššie uvedené zásady platia aj v prípade, že používateľ IS dočasne používa pracovnú stanicu pridelenú inému používateľovi. V takom prípade naviac informuje aj používateľa, ktorému bola pracovná stanica pridelená. V prípade podozrenia z poškodenia alebo neoprávnenej manipulácie s osobnými údajmi a nemožnosti postupu podľa tejto smernice postupuje podľa Havarijného plánu pracovísk IS.
11. Používateľ IS informuje zodpovednú osobu a svojho nadriadeného aj v prípade, keď má podozrenie, že súčasný stav umožňuje narušenie bezpečnosti alebo funkčnosti IS
12. Používatelia IS sú povinní spolupracovať so zodpovednou osobou a ňou prizvaným externým špecialistom pri objasňovaní príčin výskytu bezpečnostných problémov, aby mohli byť následne vykonané opatrenia, ktoré by zabránili výskytu podobnej situácie.

# PRÍSTUP DO SIETE INTERNET

1. Každý používateľ IS, ktorému bol umožnený prístup do siete internet, je povinný rešpektovať nasledovné zásady:
2. prístup do siete internet využívať predovšetkým v súlade so svojou pracovnou náplňou
3. svojou činnosťou v sieti internet reprezentuje nielen seba, ale aj pracovisko prevádzkovateľa, ktoré mu prístup do siete umožnilo. Je preto povinný rešpektovať etické zásady platné v internete a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena pracoviska alebo k iným škodám
4. komunikácia v internete (napr. elektronická pošta) spravidla nie je chránená pred „odpočúvaním“. V prípade potreby prenosu dôverných údajov sieťou internet, je nevyhnutné tieto riadne zabezpečiť ich zašifrovaním
5. internet je bohatým zdrojom nie len informácií, ale aj rôznych programov. Pre získavanie programového vybavenia a jeho použitie na počítačových systémoch pracoviska platia rovnaké pravidlá ako pre ostatné programové vybavenie (Základné zásady pre manipuláciu s programovým vybavením IS).

# MANIPULÁCIA S TECHNICKÝMI PROSTRIEDKAMI IS

1. Oprávnení používatelia kamerového systému s jednotlivými kamerami nemanipulujú, nepremiestňujú ich, ani nemenia ich uhol snímania obrazového obsahu bez predošlého súhlasu štatutára prevádzkovateľa a nového riadneho vyznačenia monitorovaného priestoru. Týmito úkonmi môže štatutár poveriť evidovaného externého špecialistu.
2. Technické prostriedky musia byť umiestnené tak, aby vplyvom okolia nedošlo k ich neúmyselnému poškodeniu alebo poruche (pádom, teplom, vodou, elektromagnetickým žiarením, priamym slnečným svetlom, ...)
3. Používateľ IS môže manipulovať so záznamový zariadením (nastavovať časovú slučku automatického mazania, vyberať záujmový obrazový obsah a robiť jeho kópiu) len v súlade s inštrukciami výrobcu, resp. dodávateľa zariadenia alebo dodávateľ príslušného programového vybavenia a len s vedomím štatutára a poverenej zodpovednej osoby.
4. Používateľ IS nesmie znižovať životnosť technických prostriedkov kamerového systému zlým zaobchádzaním a ich znečisťovaním.
5. V blízkosti záznamového zariadenia IS kamerového systému je zakázané jesť, piť a fajčiť, ale aj vykonávať iné činnosti hroziace znečistením, resp. znížením jeho životnosti, alebo spoľahlivosti (vibrácie, vystavovanie nadmernej prašnosti, vysávanie v blízkosti zapnutého zariadenia a pod.)
6. Používateľ IS nemôže bez súhlasu zodpovednej osoby:
7. robiť zásahy do záznamového zariadenia kamerového systému,
8. pripájať ku kamerovému systému ďalšie technické zariadenia,
9. odpájať už pripojené technické zariadenia ku kamerovému systému,
10. premiestňovať záznamové zariadenie,
11. manipulovať s ovládacími prvkami záznamového zariadenia okrem tých, ktoré sú umiestnené na vonkajšej strane krytu (zapínanie, vypínanie, vkladanie a vyberanie USB kľúčov a CD/DVD z mechaník)
12. Opravy a úpravy záznamového zariadenia kamerového systému alebo jednotlivých kamier, môže vykonávať len prizvaný kvalifikovaný externý špecialista. Externý špecialista pritom môže zasahovať do nahrávacieho zariadenia iba s preukázateľným súhlasom štatutára prevádzkovateľa. Používateľ IS je povinný odmietnuť prístup k záznamovému zariadeniu osobe, ktorá sa nepreukáže takýmto súhlasom.
13. Čistenie povrchu technických zariadení kamerového systému od prachu je v kompetencii používateľa IS. Vnútorné čistenie môže vykonávať len kvalifikovaný externý špecialista pri dodržaní podmienok bodu 6

# PRÍSTUPOVÉ HESLÁ

1. Používateľ IS je povinný svoje prístupové heslá meniť najmenej jedenkrát za rok, prípadne aj na pokyn štatutára prevádzkovateľa.
2. Prístupové heslá používateľa IS musia mať aspoň 8 znakov. Používateľ IS nesmie ako heslo použiť takú kombináciu znakov, ktorú by bolo možné priradiť k jeho osobe, akými sú napr. meno používateľa a jeho rodinných príslušníkov napísané spredu alebo odzadu, telefónne číslo domov alebo na pracovisko.
3. Používateľ IS musí svoje prístupové heslo používať tak, aby sa ho nemohla dozvedieť iná osoba (vrátane iných používateľov). Musí si byť vedomý svojej zodpovednosti za aktivity v IS, ktoré sa vykonávajú pod jeho menom a heslom.
4. V prípade podozrenia, že iná osoba pozná heslo používateľa IS, je tento povinný príslušné heslo okamžite zmeniť a svoje podozrenie ohlásiť zodpovednej osobe.

# MANIPULÁCIA S ÚDAJMI IS

1. Používateľ IS kamerový systém s údajmi v záznamovom zariadení nijako nemanipuluje. Tieto údaje sú automaticky premazávané v nastavenej 7-dňovej slučke. V prípade poverenia štatutárom prevádzkovateľa alebo poverenou zodpovednou osobou vyberá na prenosné pamäťové médium iba ukladá kópiu časovo ohraničeného záujmového obrazového obsahu.
2. Obrazový obsah, ktorý je špecifikovaný ako záujmový pre účely prejednania prípadného priestupku, sa vymazáva po prejednaní, pričom neprejednaný materiál sa archivuje najviac po dobu 2 rokov. Po prejednaní priestupku sa rovnako skartuje všetok príslušný materiál.
3. Obrazový materiál, ktorý je špecifikovaný ako záujmový pre účely poskytnutia oprávnenému subjektu (štátna polícia, prokuratúra, ...) na ďalšie konanie, sa archivuje dvojmo. Jedna kópia sa poskytuje, druhá archivuje zákonnú dobu 1 rok. Archivácia sa vykonáva priamo na pracovisku kamerového okruhu, špeciálnym archivačným postupom na DVD (prípadná možnosť USB).
4. Používateľ IS nesmie poskytovať údaje IS externým subjektom, mimo tých, ktorí sú vymedzení zákonom.

# ZÁSADY BEZPEČNOSTI PRI SPRÁVE DATABÁZ A APLIKÁCIÍ IS

# VŠEOBECNÉ USTANOVENIA

1. Táto časť smernice upravuje základné pravidlá pre zaistenie bezpečnosti databáz IS a aplikácií informačných systémov na pracovisku prevádzkovateľa.
2. Bezpečnosť databáz IS a aplikácií IS prevádzkovateľa zabezpečujú samotní používatelia IS v spolupráci so zodpovednou osobou.

# PODMIENKY ZAKLADANIA DATABÁZ OSOBNÝCH ÚDAJOV V IS

1. Zoznam databáz IS osobných údajov, ktoré sa spracúvajú u prevádzkovateľa, a vymedzenie účelu ich spracovania tvorí samostatnú časť: Záznamy o spracovateľských činnostiach, ktoré sú uschované u zodpovednej osoby.
2. Vznik novej databázy IS podlieha súhlasu štatutára prevádzkovateľa.
3. Databáza IS môže vzniknúť na základe splnomocňujúcich ustanovení zákona alebo potreby plniť úlohy prevádzkovateľa, riadiacich aktov. V prípade, že na spracovanie osobných údajov nejestvuje splnomocňujúce ustanovenie zákona, musí byť k tomuto spracovaniu zabezpečený súhlas dotknutých osôb v súlade s príslušným predpisom a v prípade ich nespôsobilosti na právne úkony, súhlas ich zákonných zástupcov.
4. Povinnosti podľa ods. 3 nepodliehajú:
5. databázy IS pozostávajúce z titulu, mena, priezviska a adresy dotknutej osoby na účely poštového styku,
6. údaje na štatistické účely, ak sa zabezpečí ich anonymizovanie,
7. údaje na historické alebo vedecké účely spracovávané prevádzkovateľom,
8. už zverejnené osobné údaje, ak sú náležite označené a ich spracovateľ dokáže preukázať ich zverejnenie,
9. osobné údaje, ktoré sú súčasťou platnej zmluvy, kde dotknutá osoba je jednou zo zmluvných strán a jej podpis sa považuje za súhlas na spracovávanie osobných údajov.
10. O vzniku databázy IS jej používateľ informuje zodpovednú osobu, ktorá zaeviduje databázu IS do zoznamu spracovateľských činností prevádzkovateľa a preverí bezpečnosť systému, ktorý má databázu spracovávať ešte pred začatím spracovávania databázy. Zodpovedná osoba v prípade nedostatkov vykoná opatrenia na zabezpečenie informačnej bezpečnosti spracovávaných údajov. Vstupnú kontrolu systému zapíše do prevádzkového denníka príslušného IS.

# ZÁKLADNÉ ZÁSADY BEZPEČNOSTI PRI SPRÁVE DATABÁZ A APLIKÁCIÍ

1. Používatelia vedú prevádzkový denník príslušného IS, resp. aplikácie, do ktorého zaznamenávajú podstatné udalosti súvisiace s databázou IS, resp. aplikáciou a jej bezpečnosťou. Do prevádzkového denníka sa zaznamenávajú predovšetkým nasledovné udalosti:
2. zistené chyby a odchýlky od správnej alebo požadovanej činnosti databázy IS alebo aplikácie
3. opravy a úpravy databázy IS alebo aplikácie, vrátane inštalácie novej verzie príslušného programového vybavenia
4. zmenu prístupového hesla používateľa
5. bezpečnostné incidenty
6. previerka (vyhodnotenie záznamov) prevádzkového denníka

Do prevádzkového denníka sa zapisujú minimálne nasledovné údaje:

* dátum a čas výskytu zaznamenávanej udalosti
* stručný, výstižný a zrozumiteľný popis zaznamenávanej udalosti
* popis postupu (riešenia), resp. prijatých opatrení
* jednoznačná identifikácia osoby, ktorá vykonala záznam
1. Používatelia v spolupráci so zodpovednou osobou zabezpečujú systematické zálohovanie údajov databázy IS, resp. aplikácie. V odôvodnených prípadoch realizujú zálohovanie nad rámec obvyklého systematického zálohovania.
2. Používatelia môžu realizovať zálohovanie údajov a lokálny disk pracovnej stanice iba ako núdzové riešenie a jedine za predpokladu dostatočného zabezpečenia predmetnej pracovnej stanice.
3. Používatelia vedú prehľadnú evidenciu pridelených, zmenených a odňatých prístupových práv k predmetnej databáze IS, resp. aplikácie.
4. Používatelia sú povinní pri svojej práci rešpektovať zásadu, podľa ktorej sa vyššie privilégiá pre prácu s databázou IS, resp. aplikáciou využívajú iba na výkon činností, ,ktoré nie je možné vykonať s nižšími právami.
5. Používateľ je povinný pri dlhodobom opustení miestnosti, v ktorej je uložená jemu pridelená pracovná stanica, odhlásiť sa zo systému. V prípade krátkodobého opustenia miestnosti musí aspoň aktivovať šetrič obrazovky s heslom na jeho odblokovanie.
6. V prípade akokoľvek dlhého opustenia miestnosti zabezpečí uzamknutím dvere miestnosti, v prípade, že v miestnosti neostal iný pracovník. V prípade, že pracovník opúšťa miestnosť na prízemí a v miestnosti neostáva iný pracovník, zabezpečí zatvorenie okna.
7. V prípade zistenia výskytu bezpečnostného incidentu súvisiaceho s príslušnou databázou alebo aplikáciou používatelia IS bezodkladne informujú zodpovednú osobu, s ktorou tiež konzultujú postup riešenia incidentu a taktiež spolupracujú pri zdokumentovaní incidentu a jeho riešenia.
8. Používatelia IS sú povinní po inštalácii novej verzie programového vybavenia príslušnej databázy IS alebo aplikácie IS po dobu minimálne dvoch týždňov venovať zvýšenú pozornosť činnosti databázy IS, resp. aplikácie IS a vykonávať kontroly správnosti. Prípadné odchýlky od požadovaného stavu sú povinní čo najúplnejšie zdokumentovať a bezodkladne ohlásiť zodpovednej osobe.

# ZÁDADY BEZPEČNOSTI PRI PREVÁDZKE INFORMAČNÝCH A KOMUNIKAČNÝCH TECHNOLÓGIÍ NA PRACOVISKU IS

# VŠEOBECNÉ USTANOVENIA

1. Táto smernica upravuje základné pravidlá pre zaistenie bezpečnej a spoľahlivej prevádzky informačných a komunikačných technológií informačných systémov na pracovisku prevádzkovateľa.
2. Prevádzku informačných a komunikačných technológií IS na pracovisku prevádzkovateľa zabezpečuje zodpovedná osoba, resp. štatutár prevádzkovateľa prostredníctvom poverenej osoby.

# KĽÚČOVÉ KOMPONENTY IS

1. Pre účely tejto smernice kľúčové komponenty IS prevádzkovateľa sú tie technické a programové prostriedky a dokumenty, ktorých poškodenie, zlyhanie alebo neoprávnená manipulácia nimi môže mať za následok ohrozenie spoľahlivej a bezpečnej prevádzky IS. Medzi kľúčové komponenty patria systémové a aplikačné programové vybavenia používané v rámci IS prevádzkovateľa, pamäťové médiá obsahujúce záložné kópie údajov IS, inštalačné médiá pre základné a aplikačné programové vybavenie IS, zoznam prístupových hesiel pre použitie v prípade neprítomnosti príslušných používateľov IS a podobne.
2. Prístup ku kľúčovým komponentom IS prevádzkovateľa má len zodpovedná osoba, resp. štatutár prevádzkovateľa, resp. štatutárom poverená osoba.
3. Upratovanie a podobné práce v miestnostiach, kde sú uložené kľúčové komponenty IS, sa podľa možnosti vykonávanú s ohľadom na tieto komponenty. Osoby vykonávajúce zmienené práce musia byť vopred riadne poučené o zákaze akokoľvek manipulovať s elektronickými zariadeniami bez predchádzajúceho súhlasu zodpovednej osoby, resp. štatutára, resp. štatutárom poverenej a oprávnenej osoby.

# ZÁKLADNÉ ZÁSADY BEZPEČNEJ PREVÁDZKY IS

1. Opravy a úpravy a akýkoľvek zásah na všetkých komponentoch IS môžu vykonávať len kvalifikované osoby – externí špecialisti konajúci na základe platného, vopred daného poverenia. Všetky opravy a úpravy musia byť primerane zdokumentované.
2. Pri odstraňovaní porúch kľúčových komponentov IS je zodpovedná osoba, resp. štatutárom poverená oprávnená osoba na základe požiadavky externého špecialistu oprávnená vyhlásiť technickú prestávku na nevyhnutný čas potrebný pre odstránenie poruchy.
3. Na staniciach PC s IS je zakázané inštalovať a prevádzkovať programové vybavenie získané nelegálnym spôsobom, resp. porušujúce platné licenčné podmienky.
4. Zodpovedná osoba, resp. štatutárom poverená oprávnená osoba vedie prevádzkový denník IS, do ktorého sa zaznamenávajú podstatné udalosti súvisiace so systémom, jeho prevádzkou a bezpečnosťou. Do prevádzkového denníka sa zaznamenávajú predovšetkým nasledovné udalosti:
5. poruchy na kľúčových komponentoch IS (vrátane komunikácie v sieti a porúch v dodávke elektrickej energie na pracovisko)
6. opravy, úpravy a zásahy do kľúčových komponentov IS
7. zmeny prístupových hesiel privilegovaných používateľov (napr. správca systémov)
8. vykonanie preventívnej prehliadky a testovania systému alebo jeho komponentov (vrátane kontroly čitateľnosti médií so záložnými kópiami IS pracoviska)
9. inštalovanie novej verzie základného alebo aplikačného programového vybavenia
10. bezpečnostné incidenty (vrátane výskytu počítačového vírusu)
11. previerka (vyhodnotenie záznamov) prevádzkového denníka.

Do prevádzkového denníka sa zapisujú minimálne nasledovné údaje:

* dátum a čas výskytu zaznamenávanej udalosti
* stručný, výstižný a zrozumiteľný popis zaznamenávanej udalosti
* popis postupu (riešenia), resp. prijatých opatrení
* jednoznačná identifikácia osoby, ktorá vykonala záznam
1. Prístupové práva používateľov IS prideľuje, mení a odníma iba zodpovedná osoba, štatutár, resp. štatutárom poverená oprávnená osoba.
2. Zodpovedná osoba, štatutár, resp. štatutárom poverená oprávnená osoba sú povinní pri svojej práci rešpektovať zásadu, podľa ktorej sa vyššie privilégiá pre prácu so systémom využívajú iba na výkon činností, ktoré nie je možné vykonať s nižšími právami.
3. Prístupové heslá, ktoré boli v oprávnených prípadoch (predvádzanie funkcií systému, servisné zásahy a pod. ) dočasne prepožičané externým subjektom, je potrebné po ukončení dôvodu ich prepožičania bezodkladne zmeniť tak, aby externé subjekty neboli oboznámené s novými prístupovými heslami.
4. V prípade vyraďovania PC systémov a médií z pracoviska sú používatelia IS v spolupráci s externým špecialistom povinní zabezpečiť dôkladnú likvidáciu údajov IS na vyraďovaných zariadeniach a médiách.

# ZÁLOHOVANIE

1. Kompletný systém samostatne používaných pracovných staníc (počítačov) je potrebné zálohovať tak, aby bolo možné v prípade potreby rýchlo obnoviť základné a aplikačné programové vybavenie, konfiguračné súbory, štruktúru súborového systému a všetky podstatné parametre systému potrebné pre rutinnú prevádzku.
2. Všetky médiá so záložnými kópiami údajov a programového vybavenia musia byť označené tak, aby označenie jednoznačne určovalo aktuálny obsah média a taktiež, aby bolo možné určiť dátum vytvorenia záložnej kópie na predmetnom médiu.
3. Zodpovedná osoba, resp. štatutárom poverené oprávnená osoba v spolupráci s externými špecialistami je povinná aspoň dvakrát ročne overiť bezporuchovosť (schopnosť zapisovať a korektne prečítať zapísané údaje) zálohovacieho zariadenia a aspoň tretiny médií používaných pre záložné kópie údajov a v prípade zistenej zníženej spoľahlivosti bezodkladne overiť všetky médiá a vykonať nápravné opatrenia (kvalitná oprava alebo náhrada zálohovacieho zariadenia, náhrada médií).
4. Pokiaľ je to technicky možné, médiá so záložnými kópiami údajov a programového vybavenia sa skladajú zásadne v stave zabraňujúcom zapisovanie na médium.

# ZÁSADY RIEŠENIA NEPREDVÍDANÝCH UDALOSTÍ S DOPADOM NA PREVÁDZKU IS

1. V prípade nepredvídateľnej situácie ohrozujúcej prevádzku IS alebo údaje IS prevádzkovateľa sú zodpovedná osoba, resp. štatutárom poverená oprávnená osoba a ňou poverení externí špecialisti povinní pri riešení súvisiacich problémov zaistiť primeranú ochranu všetkých komponentov systému obsahujúcich citlivé údaje IS pracoviska pred prístupom neoprávnených osôb.
2. V prípade nepredvídanej situácie je zodpovedná osoba, resp. štatutár, resp. štatutárom poverená oprávnená osoba vyhlásiť technickú prestávku na nevyhnutný čas potrebný pre riešenie udalosti.
3. Externí špecialisti na základe žiadosti zodpovednej osoby, resp. štatutárom poverenej oprávnenej osoby organizujú priebežné testovanie a aktualizáciu plánu postupu pre prípad nepredvídaných udalostí.

# ZÁSADY RIEŠENIA BEZPEČNOSTNÝCH INCIDENTOV

1. V prípade výskytu bezpečnostného incidentu zodpovedná osoba, resp. štatutárom poverená oprávnená osoba bezodkladne informuje štatutára a kontaktuje príslušného externého špecialistu.
2. Riešenie každého bezpečnostného incidentu musí byť primerane zdokumentované.
3. Zodpovedná osoba a privolaný externý špecialista sa pri riešení bezpečnostného incidentu riadia nasledovnými prioritami:
4. bezodkladné obnovenie bežnej prevádzky IS aspoň v redukovanom režime, zabezpečenie ochrany údajov IS pracoviska, zachovanie dôkazového materiálu nevyhnutného na ďalšiu analýzu príčin vzniku bezpečnostného incidentu
5. zistenie príčin, ktoré viedli k vzniku bezpečnostného incidentu
6. určenie zodpovednosti za vznik bezpečnostného incidentu a vyvodenie dôsledkov
7. zovšeobecnenie zistených skutočností a návrh opatrení na zabránenie opakovanému výskytu bezpečnostného incidentu.

# PREVENCIA

Zodpovedná osoba resp. štatutárom poverená oprávnená osoba v spolupráci s externým špecialistom je povinná:

1. Každý mesiac vykonať základnú preventívnu kontrolu kľúčových komponentov IS (testovanie systému, odstránenie nepotrebných súborov, posúdenie rýchlosti zapĺňania pamäťovej kapacity, množstvo a vek životnosti médií používaných na zálohovanie, previerka na výskyt nových programov v systéme, vyčistenie komponentov systému a pod.).
2. Pravidelne, minimálne raz za štvrťrok vykonať základnú preventívnu kontrolu zameranú na preverenie funkčnosti komponentov nevyhnutných pre riešenie nepredvídaných situácií (zariadenie pre zálohovanie a obnovu údajov, médiá so záložnými kópiami údajov a programov, aktuálnosť zálohovaných prístupových hesiel).
3. Pomáhať používateľom IS riešiť problémy, ktoré sa objavia pri práci so systémom. V prípade opakovaného výskytu problémov z dôvodu nedostatočnej kvalifikácie alebo schopnosti používateľa pracovať s IS, upozorniť priamo nadriadeného príslušného používateľa na zistené nedostatky a potrebu nápravy.

# INFORMAČNÁ POVINOSŤ PREVÁDZKOVATEĽA DOTKNUTÝM OSOBÁM

# INFORMÁCIE, KTORÉ SA MAJÚ POSKYTOVAŤ PRI ZÍSKAVANÍ OSOBNÝCH ÚDAJOV OD DOTKNUTEJ OSOBY

1. V prípadoch, keď sa od dotknutej osoby získavajú osobné údaje, ktoré sa jej týkajú, poskytne prevádzkovateľ pri získavaní osobných údajov dotknutej osobe všetky tieto informácie:
2. kontaktné údaje prípadnej zodpovednej osoby,
3. právny základ spracúvania, a ak sa spracúvanie zakladá na čl. 6 ods. 1 písm. f) nariadenia aj oprávnené záujmy prevádzkovateľa alebo tretej strany
4. o dobe uchovávania osobných údajov alebo ak to nie je možné, tak kritériá na jej určenie
5. konkretizácia práv dotknutej osoby, a to:
* práva na ich opravu
* práva na vymazanie
* právo na obmedzenie spracovania
* právo na prenos osobných údajov
* právo namietať proti spracovaniu
* existencia automatizovaného rozhodovania vrátane profilovania
1. ak je spracúvanie založené na súhlase, existencia práva kedykoľvek svoj súhlas odvolať
2. právo podať sťažnosť na úrad
3. informácia o tom, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou, alebo požiadavkou ktorá je potrebná na uzavretie zmluvy, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj možné následky neposkytnutia takýchto údajov
4. Ak má prevádzkovateľ v úmysle ďalej spracovávať osobné údaje na iný účel ako ten, na ktorý boli získané, poskytne dotknutej osobe pred takýmto ďalším spracúvaním informácie o tomto inom účele a ďalšie relevantné informácie uvedené v odseku 1.

# INFORMÁCIE, KTORÉ SA MAJÚ POSKYTNÚŤ, AK OSOBNÉ ÚDAJE NEBOLI ZÍSKANÉ OD DOTKNUTEJ OSOBY

1. Ak osobné údaje neboli získané od dotknutej osoby, prevádzkovateľ poskytne dotknutej osobe tieto informácie:
2. kategórie dotknutých osobných údajov
3. kontaktné údaje prípadnej zodpovednej osoby
4. právny základ spracúvania, a ak sa spracúvanie zakladá na čl. 6 ods. 1 písm. f) nariadenia aj oprávnené záujmy prevádzkovateľa alebo tretej strany
5. doba uchovávania osobných údajov alebo ak to nie je možné, kritériá na jej určenie
6. konkretizácia práv dotknutej osoby, a to:
* práva na ich opravu
* práva na vymazanie
* právo na obmedzenie spracovania
* právo na prenos osobných údajov
* právo namietať proti spracovaniu
* existencia automatizovaného rozhodovania vrátane profilovania
1. ak je spracúvanie založené na súhlase, existencia práva kedykoľvek súhlas odvolať
2. právo podať sťažnosť na úrad
3. z akého zdroja pochádzajú osobné údaje prípadne informácie o tom, či údaje pochádzajú z verejne prístupných zdrojov.
4. Ak má prevádzkovateľ v úmysle ďalej spracúvať osobné údaje na iný účel ako ten, na ktorý boli osobné údaje získané, poskytne dotknutej osobe pred takýmto ďalším spracúvaním informácie o tomto inom účele a akékoľvek ďalšie relevantné informácie uvedené v odseku 1.

# PRÁVO DOTKNUTEJ OSOBY NA PRÍSTUP K ÚDAJOM

1. Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak tomu tak je, má právo získať prístup k týmto osobným údajom a tieto informácie:
2. účely spracúvania
3. kategórie dotknutých osobných údajov
4. príjemcovia alebo kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, najmä príjemcovia v tretích krajinách alebo medzinárodné organizácie
5. ak je to možné, predpokladaná doba uchovávania osobných údajov alebo ak to nie je možné, kritériá na jej určenie
6. existencia práva požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby alebo ich vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti takémuto spracúvaniu
7. právo podať sťažnosť dozornému orgánu
8. ak sa osobné údaje nezískali od dotknutej osoby, akékoľvek dostupné informácie, pokiaľ ide o ich zdroj
9. existencia automatizovaného rozhodovania vrátane profilovania uvedeného v čl. 22 ods. 1 a 4 a v týchto prípadoch aspoň zmysluplné informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.
10. Ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii, dotknutá osoba má právo byť informovaná o primeraných zárukách podľa čl. 46 týkajúcich sa prenosu.
11. Prevádzkovateľ poskytne kópiu osobných údajov, ktoré sa spracúvajú. Za akékoľvek ďalšie kópie, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa poskytnú v bežne používanej elektronickej podobe, pokiaľ dotknutá osoba nepožiadala o iný spôsob.
12. Právo získať kópiu uvedenú v ods. 3 nesmie mať nepriaznivé dôsledky na práva a slobody iných.

# SPÔSOB POSKYTOVANIA ŽIADOSTI DOTKNUTEJ OSOBY

Prevádzkovateľ poskytovania informácii dotknutej osobe:

1. Musí byť v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho.
2. Písomne, elektronicky alebo inými prostriedkami alebo na požiadanie ústne (ak dotknutá osoba podala žiadosť elektronickými prostriedkami informácie sa podľa možnosti poskytnú elektronickými prostriedkami, pokiaľ dotknutá osoba nepožiadala o iný spôsob).
3. Poskytnutie oznámení o prijatých opatreniach bez zbytočného odkladu, nie neskôr ako do jedného mesiaca od doručenia žiadosti (v obzvlášť zložitých prípadoch možnosť predĺžiť o ďalšie dva mesiace, kedy sa informácia poskytne ešte za plynutia pôvodnej lehoty).
4. Ak prevádzkovateľ neprijme opatrenia na základe žiadosti dotknutej osoby, bezodkladne a najneskôr do jedného mesiaca od doručenia žiadosti informuje dotknutú osobu o dôvodoch nekonania a o možnosti podať sťažnosť na úrad a uplatniť súdny prostriedok nápravy.
5. Bezplatné poskytovanie informácií a oznámení, v osobitných prípadoch možnosť účtovať primeraný poplatok.
6. Oprávnenie prevádzkovateľa žiadať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby.
7. Prevádzkovateľ nemôže odmietnuť konať na základe žiadosti dotknutej osoby pri výkone jej práva, pokiaľ nepreukáže, že dotknutú osobu nie je schopný identifikovať.
8. Poskytnutie dotknutej osobe informácie o opatreniach bez zbytočného odkladu, nie neskôr ako do jedného mesiaca od doručenia žiadosti (v rámci lehoty je potrebné oznámiť prípadné predĺženie lehoty o ďalšie dva mesiace v prípade obzvlášť zložitých prípadoch), ak prevádzkovateľ neprijme opatrenia na základe žiadosti dotknutej osoby, bezodkladne a najneskôr do jedného mesiaca od doručenia žiadosti informuje dotknutú osobu o dôvodoch nekonania a o možnosti podať sťažnosť úradu a uplatniť súdny prostriedok nápravy.
9. Bezodplatné poskytnutie oznámení, s výnimkou neopodstatnených alebo neprimeraných, najmä opakujúcich žiadostí (právo požadovať náhradu administratívnych nákladov; prípadne nekonať).
10. Právo prevádzkovateľa požadovať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby.

# PODMIENKY VYJADRENIA SÚHLASU SO SPRACOVANÍM OSOBNÝCH ÚDAJOV

1. Ak je spracúvanie založené na súhlase, prevádzkovateľ musí vedieť preukázať, že dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov.
2. súhlas by sa mal poskytnúť jasným prejavom vôle, ktorý je slobodný, konkrétnym, informovaným a jednoznačným vyjadrením súhlasu dotknutej osoby so spracúvaním osobných údajov, ktoré sa jej týkajú (napr. prostredníctvom elektronických prostriedkov alebo ústnym vyhlásením alebo označenie políčka pri návšteve internetového webového sídla; v tejto súvislosti dávame do pozornosti, že políčko nesmie byť vopred označené)
3. súhlas sa má vzťahovať na všetky spracovateľské činnosti vykonávané na ten istý účel alebo účely
4. ak sa spracúvanie vykonáva na viaceré účely, súhlas sa má udeliť/má byť oddelený/uvedený oddelene na všetky tieto účely
5. udelenie súhlasu musí byť jasne odlíšiteľné od iných skutočností so súhlasom na spracúvanie osobných údajov nesúvisiacich
6. súhlas má byť formulovaný v zrozumiteľnej a ľahko dostupnej forme, jasne a jednoducho
7. informovanie o možnosti súhlas odvolať musí byť také jednoduché ,ako poskytnutie súhlasu
8. zákaz podmieňovať súhlas so spracúvaním osobných údajov, ktorý nie je na plnenie zmluvy, vrátane poskytnutia služby nevyhnutný

# OSOBITNÉ KATEGÓRIE OSOBNÝCH ÚDAJOV

1. Zakazuje sa spracúvanie osobných údajov, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie osoby.
2. Odsek 1 sa neuplatňuje, ak platí niektorá z týchto podmienok:
3. dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov na jeden alebo viacero určených účelov
4. spracúvanie je nevyhnutné na účely plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva a práva sociálneho zabezpečenia a sociálnej ochrany, pokiaľ je to povolené právom Únie alebo právom členského štátu alebo kolektívnou zmluvou podľa práva členského štátu poskytujúcimi primerané záruky ochrany základných práv a záujmov dotknutej osoby
5. spracúvanie je nevyhnutné na ochranu životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby v prípade, že dotknutá osoba nie je fyzicky alebo právne spôsobilá vyjadriť svoj súhlas
6. spracúvanie vykonáva v rámci svojej zákonnej činnosti s primeranými zárukami nadácia, združenie alebo akýkoľvek iný neziskový subjekt s politickým, filozofickým, náboženským alebo odborárskym zameraním a pod podmienkou že spracúvanie sa týka výlučne členov alebo bývalých členov subjektu alebo osôb, ktoré majú pravidelný kontakt s ním v súvislosti s jeho cieľmi, a že bez súhlasu dotknutej osoby sa osobné údaje neposkytnú mimo tohto subjektu
7. spracúvanie sa týka osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila
8. spracúvanie je nevyhnutné na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov, alebo kedykoľvek, keď súdy vykonávajú svoju súdnu právomoc
9. Pri spracúvaní osobných údajov možno využiť na účely určenia fyzickej osoby všeobecne použiteľný identifikátor (rodné číslo – nepatrí do osobitnej kategórie osobných údajov) ustanovený osobitným zákonom len vtedy, ak jeho použitie je nevyhnutné na dosiahnutie daného účelu spracúvania a zároveň dotknutá osoba dala písomný alebo inak hodnoverne preukázateľný súhlas na jeho spracúvanie; súhlas je neplatný, ak jeho poskytnutie vylučuje osobitný zákon, alebo ak spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa. Zverejňovať všeobecne použiteľný identifikátor (rodné číslo) sa zakazuje.

# KOPÍROVANIE, SKENOVANIE A ZAZNAMENÁVANIE ÚRADNÝCH DOKLADOV VŠEOBECNE

1. Poverené osoby prevádzkovateľa získavajú osobné údaje kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov len v nevyhnutnom rozsahu.
2. Jedná sa najmä o nasledovné úradné doklady:
3. cestovný pas
4. vodičský preukaz
5. rodný list
6. sobášny list
7. preukaz ZŤP občana
8. rozhodnutie o priznaní dôchodku a pod.
9. Je zakázané kopírovať, skenovať občiansky preukaz a kartičku poistenca dotknutej osoby.
10. Poskytnutím takéhoto dokladu sa prevádzkovateľovi môžu dostať do informačného systému aj osobné údaje, ktoré spravidla svojim rozsahom aj obsahom idú nad rámec daného účelu spracovania. Preto je oprávnená osoba povinná kopírovať iba tie údaje resp. tie časti osobného dokladu, ktoré nevyhnutne potrebuje na dosiahnutie daného účelu spracúvania (napr. prekrytím nepotrebných údajov, alebo začiarkať takéto údaje, aby neboli čitateľné).
11. Ak poverené osoby spracúvajú uvedené kópie úradných dokladov v informačnom systéme je k tomu nevyhnutný písomný súhlas dotknutej osoby. Iba v prípadoch kedy tento spôsob získavania osobných údajov oprávnenej osobe prevádzkovateľa vyslovene umožňuje osobitný zákon smie oprávnená osoba postupovať bez súhlasu dotknutej osoby.
12. Poverená osoba si súhlas nesmie vynucovať. V prípade, ak dotknutá osoba nesúhlasí s vyhotovením kópie jej úradného dokladu, oprávnená osoba vyhotoví odpis.

# SPRÁVNOSŤ A AKTUÁLNOSŤ OSOBNÝCH ÚDAJOV

1. Osobný údaj sa považuje za správny, kým sa nepreukáže opak.
2. Správnosť a aktuálnosť osobných údajov zabezpečuje prevádzkovateľ, a to:
3. zmluvným záväzkom osôb, ktoré osobné údaje do informačného systému poskytujú, že sú povinné v prípade akejkoľvek zmeny túto zmenu prevádzkovateľovi v primeranej lehote oznámiť

# LIKVIDÁCIA OSOBNÝCH ÚDAJOV

1. Oprávnená osoba po splnení účelu spracovávania osobných údajov zabezpečí bezodkladne likvidáciu tých osobných údajov, u ktorých bol účel ich spracovávania splnený.
2. Poverené osoby sú povinné pri likvidácií osobných údajov vykonať ich likvidáciu tak, aby tieto údaje sa stali nečitateľnými a nemohli byť zneužité inou neoprávnenou osobou. Pri automatizovanom spracovaní ich vymazaním z dát súboru informačného systému (subsystému), pri manuálnej podobe ich skartovaním.
3. Dokumenty s osobnými údajmi ktoré nie sú zaradené do registratúry, alebo po uplynutí doby uloženia (zákon č. 395/2002 Z. z.) sa likvidujú fyzickou likvidáciou.

# ČO JE OSOBNÝ ÚDAJ

1. Akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby.
2. Identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, ,alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.
3. Online identifikátory – IP adresa, cookies, MAC adresa, geolokalizačné údaje, logy a iné informácie získavané zo serverov.
4. Anonymizované údaje – ak sa nedá spätne určiť dotknutá osoba, nespadajú pod GDPR.
5. Pseudonymizované údaje – považujeme za osobný údaj, pretože umožňujú identifikáciu osoby, hoci s použitím kľúča 🡪 bezpečnostné opatrenie.

Vypracoval:

Schválil: